

Věnováno památce Nielse Henrika Abela

Obsah

Úvodní slovo	9
<i>M. Křížek, L. Somer</i>	
1. První Abelovu cenu získal Jean-Pierre Serre v roce 2003	17
<i>M. Křížek, M. Markl</i>	
2. Atiyah a Singer získali Abelovu cenu za rok 2004	26
<i>M. Křížek</i>	
3. Abelovu cenu v roce 2005 získal Peter Lax	37
<i>M. Křížek</i>	
4. Abelovu cenu za rok 2006 získal Lennart Carleson	48
<i>M. Křížek, I. Vrkoč</i>	
5. Abelovu cenu za matematiku získal v roce 2007 Šrínivása Varadhan	57
<i>M. Křížek, L. Somer</i>	
6. Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup	70
<i>O. Kowalski, M. Křížek</i>	
7. Abelova cena v roce 2009 udělena Michailu Gromovovi	87
<i>M. Křížek, L. Somer</i>	
8. John Tate získal Abelovu cenu za rok 2010	101
<i>M. Křížek, M. Markl</i>	
9. Abelovu cenu za rok 2011 získal John Milnor	113
<i>M. Křížek, P. Pudlák, L. Somer</i>	
10. Maďarský matematik Endre Szemerédi získal Abelovu cenu za rok 2012	126

<i>M. Křížek, M. Markl, L. Somer</i>	
11. V roce 2013 získal Abelovovu cenu Pierre Deligne za fundamentální práce svazující algebru a geometrii	138
<i>M. Křížek</i>	
12. Abelovu cenu za matematiku získal v roce 2014 Jakov G. Sinaj	150
<i>M. Křížek</i>	
13. Abelovu cenu za matematiku získali v roce 2015 John F. Nash a Louis Nirenberg	162
<i>M. Křížek, L. Somer</i>	
14. Abelova cena v roce 2016 udělena za důkaz Velké Fermatovy věty	172
<i>M. Křížek</i>	
15. Abelova cena v roce 2017 udělena za teorii waveletů	200
The Abel Prize — the Highest Achievement in Mathematics	
213	
Jmenný rejstřík	215

Úvodní slovo

Matematika bývá nazývána královnou věd již od antického Řecka. V současnosti se bez ní neobejde prakticky žádná moderní disciplína. Proto by si jistě již dávno zasloužila uznání srovnatelné s Nobelovou cenou co do významu, finanční odměny i způsobu předávání. Přesto si matematika musela počkat až do počátku 3. tisíciletí na svoje vlastní prestižní ocenění — Abelovu cenu.

V letech 2004–2017 časopis Pokroky matematiky, fyziky a astronomie (dále jen PMFA) pravidelně přinášel zprávy o laureátech Abelovy ceny za matematiku. Předkládaná publikace M. Křížek, L. Somer, M. Markl, O. Kowalski, P. Pudlák, I. Vrkoč: *Abelova cena — nejvyšší*



NIELS HENRIK ABEL (zdroj Wikipedia)

ocenění za matematiku vznikla úpravou, doplněním a rozšířením této série článků (viz www.dml.cz). V roce 2002 byl v PMFA uveřejněn na str. 7–8 článek M. T. Becka *Proč se neuděluje Nobelova cena za matematiku?* Jeho autor vyjadřuje přesvědčení, že to bylo pravděpodobně v důsledku neshod Alfreda Nobela s významným švédským matematikem Göstou Mittaglem-Lefflerem (1846–1927), žákem Weierstrassovým a zakladatelem časopisu Acta Mathematica. Existuje však mnohem přijatelnější vysvětlení. Alfred Nobel¹ nezřídil Nobelovu cenu za matematiku údajně proto, že matematiku na počátku 20. století vnímal jen jako málo praktickou disciplínu (srov. obr. 3.3).

Nejprestižnějším oceněním v matematice byla dříve Fieldsova medaile [11], která se uděluje od roku 1936 (kromě delší přestávky během 2. světové války). Seznam nositelů Fieldsovy medaile je uveden v [7]. Pro matematiky ale existuje celá řada dalších ocenění, např. Fermatova cena,² Kleinova cena, Lagrangeova cena, Gaussova cena a Wienerova cena za aplikovanou matematiku, ceny společnosti SIAM, Nevanlinnova cena za matematické práce v informatice, Pólyaova cena, Steeľova cena, Wolfova cena a Wolfskehlůva cena [2]. Některé ceny se udělují jen jednorázově, jako např. cena za vyřešení Bealovy domněnky (viz [6]). Připomeňme též vyhlášení sedmi problémů pro 3. tisíciletí „Millennium Prize Problems“ (viz [3]), kde bude vyplacen milion dolarů za každý vyřešený problém.

Mezi Nobelovou cenou a Fieldsovou medailí jsou ovšem dosti podstatné rozdíly. Zatímco Nobelova cena za fyziku se udílí každoročně od roku 1901 (kromě období 1940–1942), Fieldsova medaile se předává jen jednou za čtyři roky na mezinárodním kongresu matematiků a kandidáti se podle nepsaného pravidla vybírají tak, aby jejich věk nepřesáhl 40 let. Finanční ocenění při udělení Fieldsovy medaile činí přibližně 15 000 kanadských dolarů ($\approx 11\,000$ USD), což je o dva řády menší suma než u Nobelovy ceny. Proto se Norská akademie věd rozhodla zřídit Abelovu cenu (viz www.abelprize.no) na počest

¹A. 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. A tak po Nobelově smrti vznikla Nobelova cena za fyziku, chemii, fyziologii nebo lékařství, literaturu a Nobelova cena míru.

²Fermatovu cenu vyhlašuje každé dva roky Univerzita Paula Sabatiera v Toulouse. Mezi oceněnými byl i Andrew Wiles (1995) a Richard Taylor (2001) za důkaz Velké Fermatovy věty.



Abelova cena (zdroj <http://www.abelprize.no/>)

geniálního norského matematika Nielse Henrika Abela (1802–1829). Abelova cena se uděluje každoročně za vynikající vědecké výsledky v oblasti matematiky. Její finanční ohodnocení 6 000 000 norských korun je srovnatelné s Nobelovou cenou. Předává se v norském Oslu podobně jako Nobelova cena míru.

Zřízení Abelovy ceny navrhl další slavný norský matematik Sophus Lie (1842–1899) již na konci 19. století, jakmile se dozvěděl, že Alfred Nobel nezahrnul cenu za matematiku mezi navrhaných pět cen. V roce 1901 byla udělena první Nobelova cena za fyziku Wilhelmu Conradu Röntgenovi. Možnost udělit Abelovu cenu za matematiku v následujícím roce 1902 při příležitosti 100. výročí Abela narození

však byla promarněna, i když ji chtěl tehdejší norský král Oscar II. finančně podporovat. Ještě nenastal ten správný čas. Uplynulo celé století, než byla Abelova cena uvedena v život.

Právo nominovat kandidáta na Abelovu cenu má kdokoliv kromě sebe samého. Výběrová komise je složena z pěti mezinárodně uznávaných matematiků. Každý člen komise je volen na 2 roky počínaje sudým rokem s výjimkou předsedy, který je volen na 4 roky. Podle statutu Abelovy ceny musí být předseda norským matematikem a stanoví ho Norská akademie věd. Evropská matematická společnost EMS (European Mathematical Society) nominuje dva členy, z nichž je vybrán jeden, a zbývající tři členy volí Mezinárodní matematická unie IMU (International Mathematical Union).

Předložená kniha zachycuje portréty výjimečných osobností dosavadních laureátů Abelovy ceny. Seznamuje čtenáře s tématy jejich vědeckého bádání, s vynikajícími výsledky, za které byla cena udělena, i s možnostmi jejich uplatnění v praxi. Přiblížit laikům výsledky vrcholné matematiky je nelehký úkol, jenž se neobejde bez použití složitého matematického aparátu, odborných termínů a matematických vzorců. Některé části proto mohou být běžnému čtenáři obtížně srozumitelné. Přesto mohou vytvořit představu o složitosti a hloubce vědecké práce předních matematiků současnosti a o problémech, kterými se moderní matematika zabývá.

Připomeňme si ještě několik základních údajů o samotném Abelovi. Niels Henrik Abel se narodil 5. srpna 1802 v nemajetné rodině evangelického pastora jako druhý ze sedmi synů. Na podzim roku 1815 byl poslán do katedrální školy v Kristianii (v dnešním Oslu). Své nadání prokázal již v 16 letech, kdy zobecnil binomickou větu pro libovolný reálný exponent (viz [1], srov. též [8, s. 624]). Rozšířil tak Eulerův výsledek, který podobnou větu vyslovil jen pro racionální exponent. Abel v 19 letech dokázal, že neexistuje obecné algebraické řešení rovnice pátého stupně. Podařilo se mu to v době, kdy již studoval na univerzitě v Kristianii (1821). Na jaře roku 1823 o tom publikoval svůj první článek v norském časopise pro přírodní vědy *Magazin for Naturvidenskaberne*. Následující rok si z vlastních peněz zaplatil publikování článku o algebraických rovnicích pátého stupně, který vyšel francouzsky na pouhých šesti stránkách v poněkud obtížně srozumitelném matematickém stylu vyjadřování. Finančně jej později podporoval B. M. Holmboe (1795–1850).



Alternující grupu A_5 přímých symetrií velké Keplerovy hvězdy (též pravidelného dvanáctistěnu či dvacetistěnu) Abel implicitně použil k důkazu tvrzení, že neexistuje obecné algebraické řešení rovnice 5. stupně (foto M. Krížek).

Roku 1825 Abel obdržel stipendium od norské vlády ke studijnímu pobytu ve Francii a Německu. Cestoval přes Kodaň, Altonu, Freiberg, Drážďany, Vídeň, s delší zastávkou přes Benátky do Paříže. Při svém putování Evropou navštívil také Prahu, ale bohužel zde nenašel nikoho, s kým by mohl spolupracovat a diskutovat o svých matematických problémech. V Berlíně se pak spřátelil se stavebním inženýrem Augustem Crellem (1780–1855), který později založil proslulý matematický časopis *Journal für die reine und angewandte Mathematik*. Crelle zůstal Abelovi otcovským přítelem. Bez nadsázky lze říci, že jej zachránil pro světovou matematiku. Rozšířenou verzi Abelova článku uveřejnil Crelle v prvním čísle svého časopisu. Abel v něm podrobně dokázal, že kořeny algebraické rovnice pátého řádu obecně nelze vyjádřit v radikálech, tj. vyčíslit je pomocí konečného počtu odmocnin a čtyř základních aritmetických operací. Tento Abelův výsledek je považován za jeden z historických milníků matematiky. Pomocí teorie grup byl později nezávisle zobecněn Évaristou Galoisem (1811–1832) na kořeny polynomů libovolného stupně většího než čtyři [5]. Právem jsou proto Abel i Galois považováni za zakladatele teorie grup.



Ulice pojmenovaná po N. H. Abelovi se nachází v blízkosti univerzity v Oslu (foto M. Křížek).

V roce 1828 Abel publikoval důležité pojednání o eliptických funkcích v časopise *Astronomische Nachrichten*. Teorii eliptických funkcí později rozvinul Carl G. J. Jacobi (1804–1851). V roce 1797 Carl Friedrich Gauss (1777–1855) popsal konstrukci, jak rozdělit pomocí kružítka a pravítka Bernoulliho lemniskátu na pět stejně dlouhých částí (tj. jak zkonstruovat příslušné dělicí body, je-li lemniskáta zadána). Připomeňme, že lemniskáta je křivka, jejíž body mají konstantní součin vzdáleností od dvou pevných bodů. Abel zobecnil Gaussův postup na n stejně dlouhých částí, kde n je součin mocniny dvou vzájemně různých Fermatových prvočísel (viz [4]). Zde Abel podstatně využil toho, že explicitně vyjádřil délku lemniskáty pomocí eliptických integrálů (viz [9]). V Crellově časopise vyšla též osmdesátistránková stať věnovaná Abelovu výzkumu v oblasti eliptických křivek. Další Abelovy matematické práce lze nalézt v sebraných spisech [10].

Abel strávil spoustu času zajišťováním prostředků na svou obživu. Za jeho života se mu nedostalo uznání. Zemřel 6. dubna 1829 v chudobě na plicní tuberkulózu ve věku nedožitých 27 let. Jmenování profesorem matematiky v Berlíně, o něž se postaral A. Crelle, ho již nedostihlo. Dnes je Abelovo jméno spojováno k jeho počtě s mnoha mate-

matickými termíny: Abelovy (komutativní) grupy, Abelovy integrály, Abelovy identity, Abelovy funkce, abelovská kategorie, abelovský diferenciál, abelovské rozšíření, Abelovo kritérium pro konvergenci řad aj. Kráter Abel o průměru 114 km najdeme na jihovýchodním okraji přivrácené strany Měsíce nedaleko impaktního kráteru Legendre. V norském Gjerstadu, v němž Abel strávil dětství, vzniklo Abelovo centrum podporující svým programem učitele matematiky. Abelova cena je dalším krokem k tomu, aby dílo mladého génia nebylo nikdy zapomenuto.

Na závěr úvodní části bych rád poděkoval za celý autorský kolektiv Marku Brandnerovi, Lubomíře Dvořákové, Janě Grünerové, Jaroslavu Hančlovi, Karlu Horákovi, Radimu Hoškovi, Janě Jurečkové, Františku Katrnoškovi, Martinu Klazarovi, Stanislavu Koukalovi, Filipu a Pavlu Křížkovi, Lei Křížkové, Bohdanu Maslowskému, Šárce Nečasové, Ivanu Netukovi, Pavle Pavlíkové, Vojtěchu Pravdovi, Aleši Pultrovi, Jiřímu Rákosníkovi, Ivanu Saxlovi, Karlu Segethovi, Antonínu Slavíkovi, Jakubu Šístkovi, Jiřímu Vanžurovi, Tomáši Vejchodskému, Václavu Vopravilovi a Janě Ždárské za cenné připomínky k jednotlivým kapitolám. Můj vřelý dík též patří Hance Bílkové za pečlivé technické zpracování celého textu a nakreslení některých obrázků. Obrázky, u nichž není uveden autor, jsou staženy z internetu. Publikace vznikla v rámci grantů GA ČR P201/12/G028, GA ČR P101/14-02067S a RVO 67985840 Matematického ústavu Akademie věd ČR. Mnohokrát také děkuji Ediční radě Akademie věd ČR za finanční podporu a Brigitě Dusiové, Janě Halaškové, Kateřině Indrové, Evě Leinerové a Michaela Procházkové z Nakladatelství Academia za významnou pomoc při závěrečné úpravě knížky.

21. 3. 2018

Michal Křížek

L i t e r a t u r a

- [1] ABEL, N. H.: *Beweis eines Ausdrucks, von welchem die Binomial-Formel ein einzelner ist*. J. reine angew. Math. 1 (1926), 159–160; reprinted in [10], 102–103.
- [2] BARNER, K.: *Paul Wolfskehl and the Wolfskehl Prize*. Notices Amer. Math. Soc. 44 (1997), 1294–1303.

- [3] DEVLIN, K. J.: *The millennium problems: The seven greatest unsolved mathematical puzzles of our time*. Basic Books, New York 2002; český překlad, nakl. Dokořán, Praha 2005.
- [4] KRÍŽEK, M., LUCA, F., SOMER, L.: *17 lectures on Fermat numbers: From number theory to geometry*. Springer-Verlag, New York 2001, 2011.
- [5] KRÍŽEK, M., SOMER, L.: *Why quintic polynomial equations are not solvable in radicals*. Proc. Conf. Appl. Math. (Eds J. Brandts et al.), Inst. of Math., Prague 2015, 125–131.
- [6] MAULDIN, R. D.: *Zobecnění Velké Fermatovy věty: Bealova domněnka a problém o cenu*. PMFA 43 (1998), 104–107.
- [7] NETUKA, I.: *Mezinárodní matematické kongresy a Fieldsovy medaile*. PMFA 40 (1995), 124–129.
- [8] REKTORYS, K.: *Přehled užití matematiky I*. Prometheus, Praha 1995.
- [9] ROSEN, M.: *Abel's theorem on the lemniscate*. Amer. Math. Monthly 88 (1981), 387–395.
- [10] SYLOW, L., LIE, S. (eds): *Œuvres complètes de Niels Henrik Abel*, vol. I, II, Nouvelle Edition, Oslo 1881, 621 + 341 pp.
- [11] TROPP, H. S.: *The origins and history of the Fields medal*. Historia Math. 3 (1976), 167–181.

1. První Abelovu cenu získal Jean-Pierre Serre v roce 2003

Michal Křížek, Lawrence Somer

1.1 Prolog

Abelova cena je 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.

V červnu r. 2003 převzal Abelovu cenu za matematiku z rukou norského krále Haralda V. francouzský matematik Jean-Pierre Serre.



JEAN-PIERRE SERRE

Tento první laureát Abelovy ceny byl oceněn již v roce 1954 Fieldsovou medailí (viz [1]) za práce týkající se homotopických grup sfér a teorie svazků. Tehdy mu bylo pouhých 28 let. Tato medaile doposud nebyla udělena nikomu mladšímu. Serre získal Abelovu cenu za celoživotní klíčovou roli při formování mnoha částí moderní matematiky, zahrnujících topologii, algebraickou geometrii a teorii čísel.

1.2 Stručný životopis

Jean-Pierre Serre se narodil v roce 1926 v Bages na jihu Francie. Oba jeho rodiče byli farmaceuti. Matka měla v oblibě matematiku. Mladý Jean-Pierre rád četl různé matematické knížky, které mu matka pečlivě vybírala. Na gymnáziu v Nîmes jej starší děti šikanovaly. Aby si je usmířil, dělal jim domácí úkoly z matematiky (viz [6]). V posledním ročníku středoškolských studií 1943/44 vyhrál celostátní matematickou soutěž „Concours général“.

V letech 1945–1948 navštěvoval École normale supérieure v Paříži. V dizertační práci se zabýval homotopickými grupami. Již v r. 1951 získal vědeckou hodnost D.Sc. na pařížské Sorbonně. Pak pracoval v Centre national de la recherche scientifique (CNRS), což je obdoba naší Akademie věd. Od roku 1956 byl profesorem algebry na Collège de France v Paříži (v současnosti emeritním). Profesor Serre měl zvanou přednášku na Mezinárodním matematickém kongresu ve Stockholmu v roce 1962. Všeobecně je pokládán za skvělého přednášejícího, jak ostatně bylo patrné i z jeho abelovské přednášky (viz [8]). V rozhovoru pro časopis Mathematical Intelligencer 8 (1986) uvedl (srov. též [6, s. 243]):

Často v noci pracuji v polospánku bez nutnosti cokoliv zapisovat, což mé mysli dává mnohem větší koncentraci a též svobodu měnit témata.

Jean-Pierre Serre byl zvolen do národních akademií Francie, Nizozemska, Ruska, Švédska, USA a London Royal Society. Čestný doktorát (doctor honoris causa) získal na univerzitách v Oxfordu, Harvardu, Oslu, Aténách, Stockholmu a dalších. Je držitelem mnoha medailí, např. medaile Émila Picarda (1971), Zlaté medaile CNRS (1987). V r. 1995 získal Steelovu cenu Americké matematické společnosti a v r. 2000 prestižní Wolfovu cenu za matematiku [5].

J.-P. Serre je jedním z největších matematiků naší doby. Více než půl století publikoval zásadní články přispívající ke všeobecnému pokroku matematiky. Databáze Mathematical Reviews a Zentralblatt für Mathematik registrují přes 250 jeho prací. V roce 1968 J.-P. Serre publikoval v *Annals of Mathematics* průlomový článek [13] z algebraické geometrie s Johnem Tatem, který získal Abelovu cenu v roce 2010 (viz kap. 8). Prof. Serre je autorem více než patnácti monografií.

1.3 Hlavní vědecké výsledky

Prof. Serre vyvinul nové algebraické metody pro studium topologických objektů. Zejména se zabýval zobrazeními mezi sférami ve vyšších dimenzích. Tato problematika úzce souvisí se známou Poincarého hypotézou (viz [14], [15, s. 276]). Byl jedním z průkopníků algebraické geometrie. V mnoha ohledech tak rozšířil i Abelovy matematické ideje, zejména analytické metody pro studium algebraických rovnic ve dvou proměnných. Svými revolučními nápady sehrál klíčovou roli při formování mnoha odvětví moderní matematiky.

Jean-Pierre Serre například částečně přispěl k důkazu Velké Fermatovy věty, kterou dokázal Andrew Wiles společně s Richardem Taylorem [16] v roce 1995 (viz též [7]). Velká Fermatova věta tvrdí, že pro celé $n \geq 3$ neexistuje řešení rovnice¹

$$a^n + b^n = c^n \tag{1.1}$$

v přirozených číslech, tj. celých kladných. Koncem šedesátých let Yves Hellegouarch ve své doktorské dizertační práci přišel s myšlenkou přiřadit případným řešením (a, b, c) rovnice (1.1) zcela jiné objekty, a sice *eliptické křivky*. Pokud je p liché prvočíslo a a, b, c jsou přirozená čísla taková, že

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

pak odpovídající *Freyova křivka* je daná rovnicí

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

¹Pierre Fermat však uměl dokázat neexistenci řešení rovnice (1.1) jen pro $n = 4, 8, 16, 32, \dots$



Obr. 1.1 Jean-Pierre Serre během své přednášky o eliptických křivkách (zdroj Wikipedia).

Tato algebraická křivka se nazývá *eliptická křivka* (viz obr. 1.1 vlevo) a uvažuje se jen nad racionálními čísly $\mathbb{Q}$. Více podrobností o eliptických křivkách uvádíme v kapitolách 8.4 a 14.4.

V roce 1982 Gerhard Frey věnoval pozornost neobvyklým vlastnostem těchto křivek, které nemusí být modulární. Podle Tanijamovy–Šimurovy domněnky je ale každá racionální eliptická křivka modulární (podrobnosti viz kap. 14.5, [7] a [9]). Proto se Frey domníval, že Tanijamova–Šimurova domněnka implikuje Velkou Fermatovu větu. Jeho argumentace však nebyla úplná.

J.-P. Serre se usilovně zabýval modulárními formami a Galoisovými reprezentacemi na konečných tělesech [12]. V roce 1985 se pokusil dokázat, že Freyova křivka nemusí být modulární, ale předložil jen částečný důkaz tohoto tvrzení. Přesněji řečeno, ukázal, že tzv. semi-stabilní případ Tanijamovy–Šimurovy domněnky by mohl implikovat Velkou Fermatovu větu. To, co Serrovi scházelo k úplnému důkazu, se dnes nazývá ε -domněnka.

V létě roku 1986 Ken Ribet dokázal ε -domněnku v celé obecnosti, a tak nyní víme, že Tanijamova–Šimurova domněnka implikuje Velkou

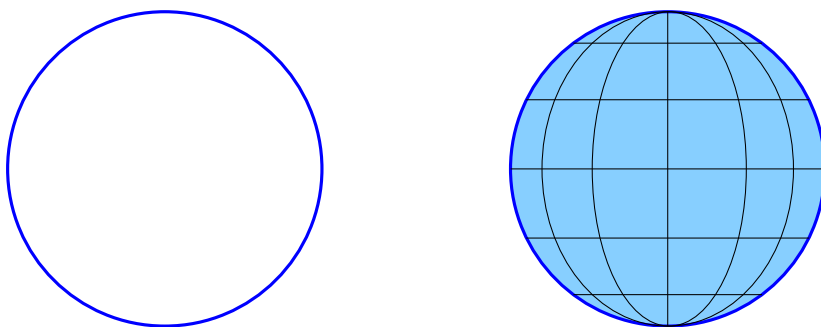
Fermatovu větu. To pak již umožnilo Wilesovi a Taylorovi dokázat Velkou Fermatovu větu v roce 1995 (viz kap. 14.6).

Již od studentských let se J.-P. Serre intenzivně zabýval teorií grup (viz kap. 6.2). Zde jenom připomeneme, že *grupa* G je množina, na které je definována asociativní binární operace $\circ : G \times G \rightarrow G$ s neutrálním prvkem e a v níž ke každému prvku $g \in G$ existuje prvek inverzní $g^{-1} \in G$ tak, že

$$g \circ g^{-1} = g^{-1} \circ g = e. \quad (1.2)$$

J.-P. Serre napsal pojednání o otevřených podgrupách profinitních grup. Je to jedna z jeho nejobtížnějších prací v tomto oboru. Nejvíce si však cení své práce o tenzorovém součinu grup reprezentací nad tělesem charakteristiky p . Napsal ji až po šedesátce a věnoval Émilu Borelovi (srov. [8]).

Jean-Pierre Serre také podstatným způsobem obohatil algebraickou topologii právě pomocí teorie grup. Připomeňme nejprve, že *jednotková sféra* $\mathbb{S}^n$ je množina bodů v $(n+1)$ -rozměrném eukleidovském prostoru $\mathbb{E}^{n+1}$, které mají jednotkovou vzdálenost od počátku (viz obr. 1.2). Symbolem $\pi_i(\mathbb{S}^n)$ označíme *i-tou homotopickou grupu* spojitých zobrazení sféry $\mathbb{S}^i$ do sféry $\mathbb{S}^n$, přičemž dvě zobrazení se pokládají za ekvivalentní, pokud jedno lze spojitě deformovat na druhé. Uveďme si to na jednoduchém příkladu grupy $\pi_1(\mathbb{S}^1)$. Existuje nekonečně mnoho tříd ekvivalentních zobrazení kružnice na sebe. Můžeme si např. představit gumičku, kterou lze příslušně nataženou ovinout



Obr. 1.2 Jednotková kružnice vlevo je sféra $\mathbb{S}^1 = \{(x, y) \in \mathbb{E}^2; x^2 + y^2 = 1\}$. Povrch jednotkové koule vpravo je sféra $\mathbb{S}^2 = \{(x, y, z) \in \mathbb{E}^3; x^2 + y^2 + z^2 = 1\}$ (nakreslil P. Křížek).

kolem kružnice jednou, dvakrát, třikrát atd. Navíjení však může probíhat i v opačném směru. Proto je příslušná grupa $\pi_1(\mathbb{S}^1)$ izomorfní s množinou celých čísel $\mathbb{Z}$.

Během studií se J.-P. Serre zabýval Lerayovou teorií fibrovaných prostorů.² Napadlo jej, že může použít spektrální posloupnost ke studiu homotopických grup sfér $\mathbb{S}^n$, a takto dokázal, že většina těchto grup je konečná (viz [10]):

Věta. Homotopická grupa $\pi_i(\mathbb{S}^n)$ je konečná kromě dvou případů:

- (1) $\pi_n(\mathbb{S}^n) \cong \mathbb{Z}$ pro $n \geq 1$,
- (2) $\pi_{4n-1}(\mathbb{S}^{2n})$ pro $n \geq 1$, která je modulo torze izomorfní se $\mathbb{Z}$.

Poznamenejme, že homotopické grupy vícerozměrných sfér poprvé definoval český matematik Eduard Čech již v roce 1932 (viz [4]). Následující tabulka uvádí homotopické grupy, které jsou buď triviální 0, nebo celá čísla $\mathbb{Z}$, nebo cyklické grupy $\mathbb{Z}_k$ řádu k , nebo jsou direktním součinem takových grup.

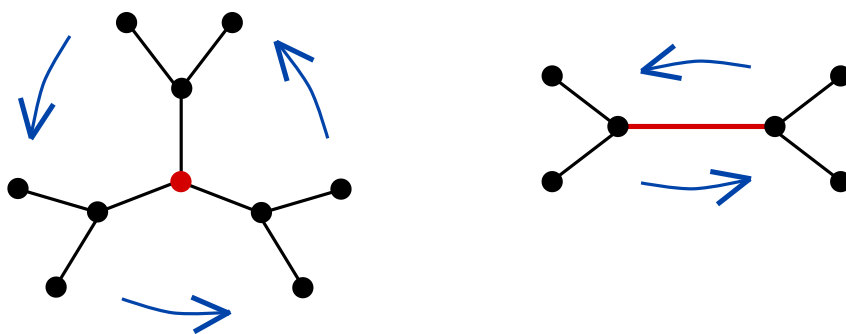
	π_1	π_2	π_3	π_4	π_5	π_6	π_7	π_8	π_9	π_{10}	π_{11}
$\mathbb{S}^1$	$\mathbb{Z}$	0	0	0	0	0	0	0	0	0	0
$\mathbb{S}^2$	0	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_{12}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_{15}$	$\mathbb{Z}_2$
$\mathbb{S}^3$	0	0	$\mathbb{Z}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_{12}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_{15}$	$\mathbb{Z}_2$
$\mathbb{S}^4$	0	0	0	$\mathbb{Z}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z} \times \mathbb{Z}_{12}$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_{24} \times \mathbb{Z}_3$	$\mathbb{Z}_{15}$
$\mathbb{S}^5$	0	0	0	0	$\mathbb{Z}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_{24}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
$\mathbb{S}^6$	0	0	0	0	0	$\mathbb{Z}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_{24}$	0	$\mathbb{Z}$

Tab. 1.1 Homotopické grupy $\pi_i(\mathbb{S}^n)$ pro $i \leq 11$ a $n \leq 6$

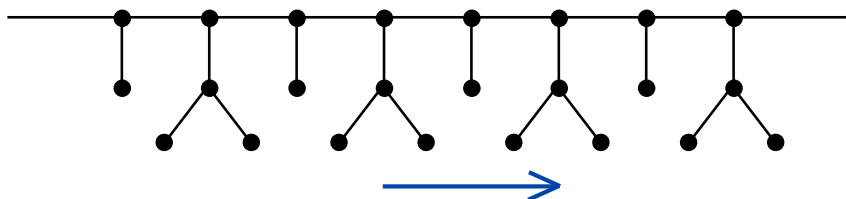
J.-P. Serre získal pozoruhodné výsledky také v teorii grafů. Připomeňme ve stručnosti, že *grafem* rozumíme trojici $\mathbf{G} = (V, E, \varepsilon)$, kde $V \neq \emptyset$ je množina vrcholů, E je množina hran a ε je zobrazení (vztah incidence), které každé hraně přiřadí dvouprvkovou množinu vrcholů. *Strom* je souvislý graf neobsahující kružnici (cyklus). Dva grafy $\mathbf{G} = (V, E, \varepsilon)$ a $\mathbf{G}' = (V', E', \varepsilon')$ jsou *izomorfní*, jestliže existují dvě vzájemně jednoznačná zobrazení $f : V \rightarrow V'$ a $g : E \rightarrow E'$ taková, že pro každou hranu $e \in E$ platí

$$\varepsilon(e) = \{v, w\} \Leftrightarrow \varepsilon'(g(e)) = \{f(v), f(w)\}.$$

²O fibrovaných varietách pojednávají články [2] a [8] uveřejněné v PMFA (viz též kap. 2.4 a 9.4).



Obr. 1.3 Příklady automorfismů (znázorněných šipkami) na Jordanovu větu. Červeně jsou označeny vrchol a hrana, které se zachovávají (nakreslila H. Bílková).



Obr. 1.4 Translace (znázorněna šipkou) na nekonečném stromu je příkladem automorfismu, jenž nezachovává ani jeden vrchol, ani jednu hranu (nakreslila H. Bílková).

Automorfismus je izomorfismus G do G . Snadno se lze přesvědčit, že množina automorfismů daného grafu G tvoří grupu s operací skládání zobrazení. Již v roce 1869 Camille Jordan zjistil, že grupa automorfismů konečného stromu musí zachovávat nějaký vrchol nebo hranu (viz obr. 1.3). Inspirován tímto výsledkem J.-P. Serre dokázal následující tvrzení (srov. obr. 1.4).

Věta. *Grupa automorfismů nekonečného stromu, které nezachovávají ani vrcholy, ani hrany, je volná³.*

Příslušné definice a důkaz lze nalézt v [3] a [11].

V algebraické geometrii J.-P. Serre přispěl k důkazu Weilových domněnek, které zformuloval André Weil v r. 1949. Tyto hypotézy se týkají generování funkcí získaných z počtu řešení systému poly-

³Grupa se nazývá *volná*, jestliže neexistuje žádný vztah mezi jejími generátory kromě definičního vztahu (1.2) mezi prvkem a jeho inverzí. Příkladem volné grupy je grupa $\mathbb{Z} \times \mathbb{Z}$.

nomiálních rovnic nad konečnými tělesy. V padesátých a šedesátých letech Serre úzce spolupracoval s Alexandrem Grothendieckem. Během této spolupráce si Serre uvědomil možnost konstrukce obecnějších kohomologických teorií k vyřešení Weilových domněnek nikoli pomocí existujících kohomologií. To působilo jako zdroj inspirace pro Grothendiecka k vývoji jisté kohomologie, což se později ukázalo jako klíčové pro důkaz Weilových domněnek Pierrem Delignem v r. 1944, viz kap. 11.5.

I když se Serre zabýval především čistou matematikou, některé jeho výsledky mají důležité aplikace. Vyvinul například efektivní samoopravující se kódy a věnoval se též kryptografii s veřejným šifrovacím klíčem. Tato problematika vyžadovala řešení algebraických rovnic nad konečnými tělesy. Jean-Pierre Serre patří mezi vědce, kteří zásadně ovlivnili matematiku minulého století a zcela změnili strukturu některých důležitých partií.

L i t e r a t u r a

- [1] BAYER, P.: *Jean-Pierre Serre, Medalla Fields*. La Gaceta 4 (2001), 211–247.
- [2] BERNSTEIN, H. J., PHILLIPS, A. J.: *Fibrovane variety a kvantová teorie*. PMFA 28 (1983), 121–147.
- [3] BIGGS, N. L.: *A proof of Serre's theorem*. Discrete Math. 78 (1989), 55–57.
- [4] ČECH, E.: *Höherdimensionale Homotopiegruppen*. Verhandlungen des Internationalen Mathematikerkongress, Zürich, Orell Füssli, 1932.
- [5] CHERN, S. S., HIRZEBRUCH, F. (Eds): *Jean-Pierre Serre*. In: *Wolf Prize in Mathematics*, Vol. II, World Sci. Publ. Co. 2001, 523–551.
- [6] CHONG, C. T., LEONG, Y. K.: *Rozhovor s Jeanem-Pierrem Serrem*. PMFA 33 (1988), 241–248.
- [7] NEKOVÁŘ, J.: *Modulární křivky a Fermatova věta*. Math. Bohem. 119 (1994), 79–96.
- [8] RAUSSEN, M., SKAU, C.: *Rozmluva s Jeanem-Pierrem Serrem, prvním nositelem Abelovy ceny*. PMFA 49 (2004), 114–121.

- [9] RIBENBOIM, P.: *Fermat's Last Theorem for amateurs*. Springer, New York, 1999.
- [10] SERRE, J.-P.: *Homologie singulière des espaces fibrés. Applications*. Ann. of Math. *54* (2) (1951), 425–505.
- [11] SERRE, J.-P.: *Trees*. Springer, Berlin, 1980.
- [12] SERRE, J.-P.: *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* . Duke Math. J. *54* (1987), 179–230.
- [13] SERRE, J.-P., TATE, J.: *Good reduction of abelian varieties*. Ann. of Math. *88* (1968), 492–517.
- [14] SMALE, S.: *Mathematical problems for the next century*. Math. Intelligencer *20* (2) (1998), 7–15.
- [15] STILLWELL, J.: *Příběh stodvacetistěnu v $\mathbb{R}^4$* . PMFA *46* (2001), 265–280.
- [16] TAYLOR, R., WILES, A.: *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. *141* (1995), 553–572.

2. Atiyah a Singer získali Abelovu cenu za rok 2004

Michal Křížek, Martin Markl

2.1 Prolog

Norská akademie věd se rozhodla udělit Abelovu cenu za rok 2004 siru Michaelu Francisi Atiyahovi z univerzity v Edinburghu a Isadoru M. Singerovi z Massachusettského technologického ústavu. Cenu získali „za objev a důkaz věty o indexu, která uvádí do souvislosti topologii, geometrii a analýzu, a za významnou roli při budování nových mostů mezi matematikou a teoretickou fyzikou“. V komisi pro výběr kandidátů na Abelovu cenu za rok 2004 byli David Mumford, Jacob Palis, Erling Størmer (předseda), Gilbert Strang a Don Zagier.

Atiyahova–Singerova věta o indexu je jedním z velkých mezníků matematiky dvacátého století, který významně ovlivnil pokrok v nejdůležitějších oblastech topologie, diferenciální geometrie a kvantové



SIR MICHAEL FRANCIS ATIYAH ISADORE MANUEL SINGER

teorie pole. Oběma autorům se podařilo společně i individuálně zaplnit mezeru mezi světem čisté matematiky a teoretickou částicovou fyzikou. Ve svých oborech se začali vzájemně obohacovat a jejich spolupráce se stala jednou z nejvíce fascinujících výzkumných činností několika posledních desetiletí. S formulací věty o indexu se seznámíme v kap. 2.4. Atiyah, Singer a Vijay K. Patodi zavedli v [2] invariant, kterému se dnes běžně říká Atiyahův–Patodiho–Singerův η -invariant.

Atiyah a Singer se původně zabývali různými oblastmi matematiky: Atiyah se věnoval algebraické geometrii a Singer matematické analýze. Jejich hlavní výsledky v těchto oborech jsou též vysoce ceněny. Jako příklad uveďme Atiyahovu ranou práci o meromorfních formách na algebraických varietách a jeho článek [1] o Thomových komplexech z roku 1961. Atiyahovo pionýrské dílo s Friedrichem Hirzebruchem o rozvoji topologické obdoby Grothendieckovy K-teorie¹ mělo řadu aplikací v klasických problémech topologie. Později se ukázalo, že je těsně spjato s větou o indexu.

Singer společně s Richardem V. Kadisonem inicioval výzkum v oblasti trojúhelníkových operátorových algeber (angl. triangular operator algebras). Jeho jméno je spojováno i s Ambroseovou–Singerovou větou o holonomii a Rayovým–Singerovým torzním invariantem. Společně s Henrym P. McKeanem upozornil Singer na důležitou geometrickou informaci ukrytou v tzv. tepelných jádrech² (angl. heat kernels). I tento objev měl velký dopad.

2.2 Stručná biografie Michaela F. Atiyaha

Michael Francis Atiyah³ se narodil v Londýně v roce 1929. Titul B.A. a později doktorát získal na Koleji Nejsvětější Trojice (Trinity College) v Cambridgi. Podstatnou část své akademické dráhy strávil také v Oxfordu. Zastával mnoho význačných funkcí, mezi jinými vysoce prestižní Savilian Chair of Geometry v Oxfordu a Master of Trinity College v Cambridgi. Byl také profesorem matematiky v Ústavu pro pokročilá studia v Princetonu.

¹K-teorie je moderní forma teorie reprezentací grup, viz PMFA 48 (2003), 177–192.

²Tato jádra jsou charakterizována fundamentálním řešením rovnice pro vedení tepla.

³S názory M. Atiyaha na matematiku ve 20. století je možno se seznámit v článcích PMFA 31 (1986), 154–168 a 48 (2003), 177–192.

V době svého působení v Oxfordu a Cambridgi se Atiyah stal představitelem nové generace mladých matematiků. Byl vedoucí osobností při budování Newtonova ústavu matematických věd v Cambridgi a též jeho prvním ředitelem. Je zároveň čestným profesorem na univerzitě v Edinburghu.

Během své kariéry obdržel Atiyah mnohá ocenění včetně Fieldsovy medaile (1966). Byl zvolen řádným členem Královské společnosti v Londýně v roce 1962, když mu bylo pouhých 32 let. Od této společnosti získal Královskou medaili v r. 1968 a Copleyho medaili v r. 1988. Prezidentem Královské společnosti byl v letech 1990–1995 a prezidentem Londýnské matematické společnosti v letech 1974–1976. Hrál též významnou roli při utváření dnešní Evropské matematické společnosti.

Atiyahovou zásluhou byla založena tzv. meziakademická panelová diskuse, která svedla dohromady řadu akademií věd z celého světa. Podnítil také utvoření Asociace evropských akademií (ALLEA). Byl prezidentem pugwashských konferencí (On Science and World Affairs).

Z mnoha cen, které mu byly uděleny, jmenujme Feltrinelliho cenu (Accademia Nazionale dei Lincei, 1981) a Mezinárodní cenu za vědu krále Fajsala (1987). V roce 1983 byl Atiyah pasován na rytíře a v roce 1992 získal britský řád Za zásluhy (angl. Order of Merit).

2.3 Stručná biografie Isadora M. Singera

Isadore Manuel Singer se narodil v roce 1924 v Detroitu a v roce 1944 ukončil studia na univerzitě v Michiganu. Po získání doktorátu (Ph.D.) na univerzitě v Chicagu v roce 1950 přešel na Massachusettský technologický ústav (MIT). Zde strávil většinu svého profesního života a v současné době je zde profesorem.

Singer je členem Americké akademie umění a věd, Americké filosofické společnosti a Národní akademie věd (NAS). Působil v radě NAS, v řídicím výboru Úřadu pro národní výzkum (Governing Board of the National Research Council) a ve vědecké radě Bílého domu (White House Science Council). V letech 1970–1972 byl viceprezidentem Americké matematické společnosti (viz *Notices AMS* 51 (2004), 649).

V roce 1992 získal Singer cenu Americké matematické společnosti Award for Distinguished Public Service. V odůvodnění se uznává

„vynikající příspěvek k jeho profesi, vědě v širším smyslu a veřejným věcem“.

Mezi další jeho ocenění patří Böcherova cena (1969) a Steelova cena (2000) za celoživotní úspěchy. Obě dostal od Americké matematické společnosti. Dále obdržel Wignerovu medaili (1988) a Národní medaili za vědu (1983).

V poděkování po získání Steelovy ceny (Notices AMS, April 2000) Singer prohlásil: „Školní třída je pro mě důležitý protějšek výzkumu. Moc se mi líbilo učit postgraduální studenty na všech stupních. Od mnohých z nich jsem se naučil více, než jsem je naučil já.“ Singerovými vynikajícími učebními texty byly inspirovány generace matematiků.

2.4 Atiyahova–Singerova věta o indexu

Věta o indexu pojednává o eliptických diferenciálních operátorech. Zopakujme nejdříve základní definice. *Diferenciální operátor* na prostoru $\mathcal{C}(U)$ hladkých komplexních funkcí na otevřené podmnožině U eukleidovského prostoru $\mathbb{R}^n$ se souřadnicemi $(x_1, \dots, x_n)$ je operátor tvaru

$$D = \sum_{i_1, \dots, i_n \geq 0} F_{i_1, \dots, i_n}(x_1, \dots, x_n) \frac{\partial^{i_1 + \dots + i_n}}{\partial x_1^{i_1} \dots \partial x_n^{i_n}}, \quad (2.1)$$

kde pouze konečně mnoho koeficientů $F_{i_1, \dots, i_n} \in \mathcal{C}(U)$ je nenulových. Jinými slovy, D náleží okruhu $\mathcal{C}(U)[\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}]$ polynomů v proměnných $\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}$ s koeficienty v $\mathcal{C}(U)$. *Řád operátoru* D je číslo

$$\text{rk}(D) := \max\{i_1 + \dots + i_n ; F_{i_1, \dots, i_n} \neq 0\}.$$

Symbol operátoru D řádu k je polynom $\sigma(D) \in \mathcal{C}(U)[t_1, \dots, t_n]$ definovaný předpisem

$$\sigma(D)(x_1, \dots, x_n, t_1, \dots, t_n) := \sum_{i_1 + \dots + i_n = k} F_{i_1, \dots, i_n}(x_1, \dots, x_n) t_1^{i_1} \dots t_n^{i_n}.$$

Operátor D je *eliptický*, jestliže $\sigma(D)(x_1, \dots, x_n, t_1, \dots, t_n) \neq 0$, kdykoliv $t_m \neq 0$ pro nějaké $m \in \{1, \dots, n\}$. Příkladem je laplacián

$$\Delta := \frac{\partial^2}{\partial x_1^2} + \dots + \frac{\partial^2}{\partial x_n^2}, \quad (2.2)$$

jehož symbol je $t_1^2 + \dots + t_n^2$. Naproti tomu vlnový operátor

$$\square := -\frac{\partial^2}{\partial x_1^2} + \dots + \frac{\partial^2}{\partial x_n^2} \quad (2.3)$$

eliptický není.

Věta o indexu se ovšem týká obecnějších diferenciálních operátorů působících na řezech hladkých vektorových fibrací.⁴ Opět připomeňme základní pojmy. *Komplexní vektorová fibrace* (krátce vektorová fibrace) je zobrazení topologických prostorů $\pi : E \rightarrow M$ takové, že $F_b := \pi^{-1}(b)$ (tzn. *fibr* nad bodem b) je pro každé $b \in M$ konečnorozměrný komplexní vektorový prostor. Dále požadujeme *lokální trivialitu*, tedy aby pro každý bod $b \in M$ existovalo otevřené okolí $U \ni b$, číslo k a homeomorfismus

$$\phi : U \times \mathbb{C}^k \rightarrow \pi^{-1}(U)$$

takový, že

- (i) $(\pi\phi)(x, v) = x$ pro každé $(x, v) \in U \times \mathbb{C}^k$ a
- (ii) pro každé $x \in U$ je zobrazení $v \mapsto \phi(x, v)$ izomorfismem komplexních vektorových prostorů $\mathbb{C}^k$ a F_x .

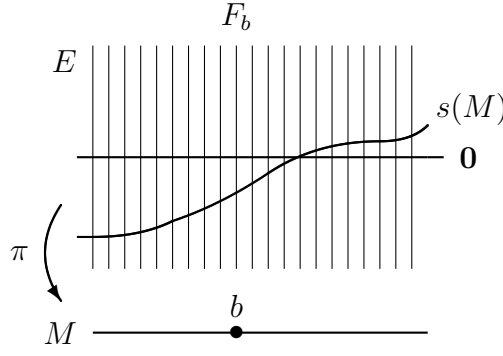
Podmínka (i) vyjadřuje komutativitu diagramu

$$\begin{array}{ccccc} U \times \mathbb{C}^k & \xrightarrow[\cong]{\phi} & \pi^{-1}(U) & \hookrightarrow & E \\ p_1 \downarrow & & \downarrow \pi & & \downarrow \pi \\ U & \xrightarrow{=} & U & \hookrightarrow & M \end{array} \quad (2.4)$$

V něm p_1 je projekce na první faktor. Prostory M , resp. E se nazývají *báze*, resp. *totální prostor* fibrace $\pi : E \rightarrow M$. Na zobrazení π se budeme odkazovat jako na *fibrující zobrazení*.

Volně řečeno, vektorová fibrace je rodina vektorových prostorů $\{F_b\}_{b \in M}$ spojitě parametrizovaná bází M , což schematicky vyjadřuje obrázek 2.1. Příklad fibrace je samozřejmě projekce $p_1 : U \times \mathbb{C}^k \rightarrow U$ na otevřenou podmnožinu $U \subset \mathbb{R}^n$. Tato tzv. *triviální fibrace* má bázi U a totální prostor $U \times \mathbb{C}^k$.

⁴Anglicky smooth vector bundle.



Obr. 2.1 Představa fibrace jako spojitě rodiny vektorových prostorů (nakreslil M. Markl).

Restrikce vektorové fibrace $\pi: E \rightarrow M$ na podmnožinu $U \subset M$ je vektorová fibrace $\pi|_U: E|_U \rightarrow U$ s bází U a totálním prostorem $E|_U := \pi^{-1}(U)$. Diagram (2.4) říká, že restrikce vektorové fibrace na dostatečně malé otevřené podmnožiny báze jsou triviální.

Vektorová fibrace $\pi: E \rightarrow M$ je *hladká*, jestliže π je hladké zobrazení hladkých variet.⁵ Dále budeme hladkost předpokládat automaticky. Řez fibrace $\pi: E \rightarrow M$ je pravá inverze fibrujícího zobrazení, tedy hladké zobrazení $s: M \rightarrow E$, pro něž πs je identita. Řez s je určen svým grafem $s(M)$ vloženým do totálního prostoru E , viz opět obrázek 2.1. Množina $\Gamma(E, M)$ všech řezů je komplexní vektorový prostor s nulovým elementem $\mathbf{0}$, což je řez, pro který $\mathbf{0}(b) := 0 \in F_b$ pro všechna $b \in M$. Součet $s' + s''$ řezů s' a s'' je definován „po fíbrech“, tedy vzorcem $(s' + s'')(b) := s'(b) + s''(b)$, $b \in M$.

Snadno ověříme, že prostor řezů $\Gamma(U \times \mathbb{C}^k, U)$ triviální fibrace tvoří k -tice $(f_1, \dots, f_k)$ funkcí z $\mathcal{C}(U)$. Speciálně tedy $\Gamma(U \times \mathbb{C}, U) = \mathcal{C}(U)$. Operátory Δ a $\square$ připomenuté v (2.2), resp. (2.3) můžeme nyní chápat jako lineární zobrazení $\Gamma(U \times \mathbb{C}, U) \rightarrow \Gamma(U \times \mathbb{C}, U)$.

Na vektorové fibrace lze „po fíbrech“ aplikovat stejné operace jako na vektorové prostory. Každá vektorová fibrace $E \rightarrow M$ má proto svůj *duál* $E^* \rightarrow M$, jehož fibr F_b^* nad $b \in M$ je lineární duál fibr F_b původní fibrace.⁶ Podobně můžeme utvořit *součet*

$$E' \oplus E'' \rightarrow B \quad (2.5)$$

fibrací $E' \rightarrow B$ a $E'' \rightarrow B$ se stejnou bází B . Fíbr $\mathbf{0}$ součtu (2.5) tvoří přímé součty $F_b' \oplus F_b''$ fibrů jednotlivých konstituentů.

⁵O hladkých varietách pojednáme též v kap. 9.3.

⁶Pokud není třeba, vynecháváme symbol pro fibrující zobrazení.

Ve formulaci věty o indexu upotřebíme i následující konstrukci. Pro hladké zobrazení $p: B \rightarrow M$ a fíbraci $\pi: E \rightarrow M$ definujeme *indukovanou* fíbraci⁷ $p^*E \rightarrow M$ fíbrace π podél zobrazení p jako fíbraci s totálním prostorem

$$p^*E := \{(b, e) \in B \times E ; p(b) = \pi(e)\}.$$

Fíbrující zobrazení $p^*E \rightarrow B$ je projekce na první faktor. Indukovaná fíbrace tvoří komutativní diagram

$$\begin{array}{ccc} p^*E & \longrightarrow & E \\ \downarrow & & \downarrow \pi \\ M & \xrightarrow{p} & B \end{array}$$

s obvyklou univerzální vlastností kategoriálních kartézských čtverců.

Vraťme se nyní k definici diferenciálních operátorů v potřebné obecnosti. Uvažujme vektorové fíbrace $\pi': E' \rightarrow M$ a $\pi'': E'' \rightarrow M$ nad stejnou bází. Diferenciální operátor je lineární zobrazení $D: \Gamma(E', M) \rightarrow \Gamma(E'', M)$ lokálně reprezentované maticí diferenciálních operátorů (2.1). Tím rozumíme toto. Víme, že vektorové fíbrace jsou lokálně modelovány triviálními fíbracemi. Restrikce prostorů řezů na dostatečně malé otevřené podmnožiny báze M jsou tedy tvořeny k -ticemi (resp. l -ticemi) hladkých komplexních funkcí z $\mathcal{C}(U)$ pro nějaká k a l . Vyžadujeme, aby na těchto restrikcích byl operátor D dán předpisem

$$D(f_1, \dots, f_k) = \left(\sum_{1 \leq i \leq k} D_1^i(f_i), \dots, \sum_{1 \leq i \leq k} D_l^i(f_i) \right),$$

kde D_j^i jsou „klasické“ diferenciální operátory jako v (2.1). Takový operátor D se nazývá eliptický, jestliže je příslušná matice symbolů

$$|\sigma(D_j^i)(x_1, \dots, x_n, t_1, \dots, t_n)|, \quad 1 \leq i \leq k, \quad 1 \leq j \leq l,$$

regulární, kdykoliv $(t_1, \dots, t_n) \neq (0, \dots, 0)$. Elipticita nutně implikuje $k = l$.

⁷Anglicky pullback.

Příklad 1. Pro $i = 0, 1, 2, \dots$ označme $\wedge_{\mathbb{C}}^i(M)$ komplexifikovanou i -tou vnější (Grassmannovu) mocninu kotečné fibrace T^*M variety M .⁸ Její řezy

$$\Omega^i(M) := \Gamma(\wedge_{\mathbb{C}}^i(M), M)$$

jsou (komplexní) *de Rhamovy formy* stupně i . Ty spolu s *de Rhamovým diferenciálem* $d^i: \Omega^i(M) \rightarrow \Omega^{i+1}(M)$ tvoří (komplexifikovaný) de Rhamův komplex $(\Omega(M), d)$ variety M . Jeho kohomologie $H(\Omega(M), d)$ jsou shodné s kohomologiemi $H(M; \mathbb{C})$ variety M s komplexními koeficienty. Pomocí Riemannovy metriky lze sestrojít operátor $d^{i*}: \Omega^{i+1}(M) \rightarrow \Omega^i(M)$ *sdužený* k operátoru d^i . Operátory d^i a d^{i*} jsou příklady diferenciálních operátorů na řezech fibrace $\wedge_{\mathbb{C}}^i(M)$ s hodnotami v řezech fibrace $\wedge_{\mathbb{C}}^{i+1}(M)$, resp. $\wedge_{\mathbb{C}}^{i-1}(M)$. Označme

$$E' := \bigoplus_{j \geq 0} \wedge_{\mathbb{C}}^{2j}(M), \quad \text{resp.} \quad E'' := \bigoplus_{j \geq 0} \wedge_{\mathbb{C}}^{2j+1}(M),$$

přímé součty sudých, resp. lichých vnějších mocnin kotečné fibrace. Operátory d^i a d^{i*} se skládají do operátorů

$$d := \sum_{j \geq 0} d^{2j}: \Gamma(E', M) \rightarrow \Gamma(E'', M)$$

a

$$d^* := \sum_{j \geq 0} d^{2j+1*}: \Gamma(E', M) \rightarrow \Gamma(E'', M),$$

jejichž součet $D := d + d^*: \Gamma(E', M) \rightarrow \Gamma(E'', M)$ je eliptický diferenciální operátor.

Dále se soustředíme na vektorové fibrace nad *kompaktními orientovanými uzavřenými* varietami.⁹ Ukazuje se, že eliptické operátory jsou *Fredholmovy*, tedy mají konečněrozměrná jádra i kojádra.¹⁰ Můžeme tedy definovat *analytický index* operátoru D jako

$$\text{Ind}_A(D) := \dim \text{Ker}(D) - \dim \text{coKer}(D), \quad (2.6)$$

kde $\text{Ker}(D)$, resp. $\text{coKer}(D)$ značí jádro, resp. kojádro lineárního zobrazení D .

⁸Velmi snadno se ověří, že $\wedge_{\mathbb{C}}^i(M) = 0$ pro $i > \dim(M)$.

⁹Význam těchto pojmů i nádherný úvod do charakteristických tříd čtenář nalezne v [3].

¹⁰Kojádro lineárního zobrazení $L: A \rightarrow B$ je podíl $B/L(A)$.

Druhým pojmem figurujícím ve větě o indexu je *topologický index* operátoru D definovaný vzorcem

$$\text{Ind}_T(D) := \text{ch}(D)\mathcal{T}(M)[M]. \quad (2.7)$$

Jeho úplné vysvětlení přesahuje možnosti této kapitoly, proto jenom naznačíme definice jednotlivých členů bez nároků na úplnou přesnost, na details odkazujeme čtenáře k [4]. Začneme s veličinou $\text{ch}(D)$.

Množina všech (nikoliv nutně hladkých) vektorových fibrací s danou bází B je komutativní pologrupa $\mathcal{E}(B)$ s asociativní operací $+$ danou součtem (2.5) a neutrálním prvkem 0 tvořeným identitou $B \rightarrow B$. Jako každou komutativní pologrupu lze $\mathcal{E}(B)$ zúplnit Grothendieckovou konstrukcí do komutativní grupy $K(X)$. Tím získáme (komplexní) K -grupu prostoru X .

Hladká varieta M má *tečnou fibraci* $TM \rightarrow M$ a duální *kotečnou fibraci* $p: T^*M \rightarrow M$. V totálním prostoru kotečné fibrace vezměme podprostor $B(M) \subset T^*M$ vektorů délky nepřesahující 1 a sestrojme indukované fibrace

$$\begin{array}{ccc} p^*E' & \longrightarrow & E' \\ \downarrow & & \downarrow \pi' \\ B(M) & \xrightarrow{p} & M \end{array} \quad \text{a} \quad \begin{array}{ccc} p^*E'' & \longrightarrow & E'' \\ \downarrow & & \downarrow \pi'' \\ B(M) & \xrightarrow{p} & M. \end{array}$$

Ukazuje se, že symbol $\sigma(D)$ operátoru D lze interpretovat jako zobrazení

$$\sigma(D): p^*E'|_{S(M)} \rightarrow p^*E''|_{S(M)} \quad (2.8)$$

restrikcí indukovaných fibrací p^*E' , resp. p^*E'' na podprostor $S(M) \subset B(M)$ vektorů délky 1. Operátor D je eliptický, právě když je toto zobrazení izomorfismus. Indukované fibrace p^*E' , resp. p^*E'' náležejí pologrupě $\mathcal{E}(B(M))$, můžeme proto vzít jejich rozdíl

$$p^*E' - p^*E'' \in K(B(M)).$$

Lze ukázat, že s použitím izomorfismu (2.8) určí prvek $p^*E' - p^*E''$ *rozdílový element* $d(D) \in K(B(M)/S(M))$ v K -grupě podílu $B(M)/S(M)$.

Uveďme následující posloupnost tvořenou standardními objekty algebraické topologie:

$$K(B(M)/S(M)) \xrightarrow{\text{ch}} H(B(M)/S(M); \mathbb{Q}) \xrightarrow{t} H(M; \mathbb{Q}). \quad (2.9)$$

První člen je již zmíněná K -grupa podílu $B(M)/S(M)$, druhý a třetí člen jsou racionální kohomologické okruhy podílu $B(M)/S(M)$, resp. variety M .

Zobrazení ch je *Chernův charakter*, což je určitý multiplikativní homomorfismus z komplexní K -teorie do racionálních kohomologií definovaný s použitím Chernových tříd komplexních vektorových fibrací. Zobrazení t je *Thomův izomorfismus* kotečné fibrace T^*M . Faktor $ch(D)$ v (2.7) je obraz prvku $d(D)$ kompozicí zobrazení v (2.9), tedy

$$ch(D) := t(ch(d(D))) \in H^*(M; \mathbb{Q}).$$

Symbol $\mathcal{T}(M)$ v (2.7) značí *Toddův rod* variety M , tedy mocninou řadu

$$\begin{aligned} \mathcal{T}(M) = & 1 + \frac{c_1}{2} + \frac{c_2 + c_1^2}{12} + \frac{c_1 c_2}{24} + \\ & + \frac{-c_1^4 + 4c_2 c_1^2 + 3c_2^2 + c_3 c_1 - c_4}{720} + \dots \in H(M; \mathbb{Q}), \end{aligned}$$

ve které $c_1, c_2, c_3, \dots \in H^*(M; \mathbb{Q})$ jsou Chernovy třídy komplexifikované tečné fibrace variety M . Topologický index (2.7) je racionální číslo dané evaluací součinu $ch(D)\mathcal{T}(M) \in H(M; \mathbb{Q})$ na fundamentální třídě $[M]$ variety M . Nyní již máme všechny potřebné definice.

Věta o indexu. *Analytický index eliptického diferenciálního operátoru na kompaktní hladké orientované uzavřené varietě je roven jeho topologickému indexu, tedy*

$$\text{Ind}_A(D) = \text{Ind}_T(D).$$

Hloubka věty je v porovnávání veličin rozdílného charakteru. Zatímco analytický index je celé číslo sestavené prostředky funkcionální analýzy, topologický index je geometrická veličina. Okamžitý důsledek je, že $\text{Ind}_T(D)$ je také celé číslo, zatímco jeho definice říká pouze, že je to číslo racionální – povšimněme si, že vzorec pro Toddův rod obsahuje racionální koeficienty!¹¹ To je samo o sobě velice silný výsledek.

Ani analytický, ani topologický index nemusí být definován, pokud operátor D není eliptický. V takovém případě nemusí být rozdíl (2.6)

¹¹Stejná poznámka platí i pro Chernův charakter, jenž je v podstatě exponenciální funkcí Chernových tříd.

definující $\text{Ind}_A(D)$ konečný, a protože (2.8) není izomorfismus, nelze sestavit ani rozdílový element $d(D)$, potřebný pro definici $\text{Ind}_T(D)$.

Příklad 2. Analytický index operátoru D z příkladu 1 je roven *Eulerově charakteristice* variety M , tedy

$$\text{Ind}_A(D) = \sum_{i \geq 0} (-1)^i \dim H^i(M, \mathbb{Q}).$$

Jeho topologický index získáme evaluací *Eulerovy třídy* $\chi(M)$ tečné fibrace variety M na její fundamentální třídě $[M]$,

$$\text{Ind}_T(D) = \chi(M)[M].$$

Věta o indexu pro operátor D vyjadřuje klasickou Gaussovu–Bonnetovu větu (viz kap. 7.3).

Příklad 3. Na varietě s komplexní strukturou můžeme místo operátoru D z předchozího příkladu vzít operátor $\bar{\partial} + \bar{\partial}^*$, působící na komplexních formách typu $(0, i)$. Věta o indexu v tomto případě vyústí v Riemannovu–Rochovu větu (viz [4, kap. XIX]).

L i t e r a t u r a

- [1] ATIYAH, M.: *Thom complexes*. Proc. London Math. Soc. 11 (1961), 291–310.
- [2] ATIYAH, M. F., PATODI, V. K., SINGER, I. M.: *Spectral asymmetry and Riemannian Geometry*. Bull. London Math. Soc. 5 (1973), 229–234.
- [3] MILNOR, J., STASHEFF, J.: *Characteristic classes*. Ann. of Math. Stud., vol. 76, Princeton Univ. Press, New Jersey, 1974.
- [4] PALAIS, R. S. (ed.): *Seminar on the Atiyah–Singer index theorem*. With contributions by M. F. Atiyah, A. Borel, E. E. Floyd, R. T. Seeley, W. Shih, and R. Solovay. Ann. of Math. Stud., vol. 57, Princeton Univ. Press, New Jersey, 1965 (ruský překlad Mir, Moskva, 1970).

3. Abelovu cenu v roce 2005 získal Peter Lax

Michal Křížek

3.1 Prolog

Norská akademie věd se rozhodla udělit Abelovu cenu za rok 2005 významnému numerickému matematikovi Peteru D. Laxovi za jeho fundamentální příspěvky k teorii a aplikacím parciálních diferenciálních rovnic a výpočtu jejich řešení. Tuto v pořadí již třetí Abelovu cenu získal P. Lax 18. května 2005 spolu s peněžitou odměnou 980 000 USD. Týž den pak proslovil Abelovu přednášku na půdě univerzity v Oslu.



PETER DAVID LAX

V 50. a 60. letech Peter Lax položil základy moderní teorie nelineárních hyperbolických systémů. Zkonstruoval jejich explicitní řešení a studoval, jak se tato řešení chovají na dlouhých časových intervalech. Jako průlomové lze označit jeho výsledky týkající se solitonů, entropie a rázových vln. Jeho jméno nese Laxovo–Milgramovo lemma, Laxovy páry, Laxova věta o ekvivalenci, Laxovo–Friedrichsovo schéma, Laxovo–Wendroffovo schéma, Laxova entropická podmínka, Laxova–Levemorova teorie či Laxova–Phillipsova teorie rozptylu.

3.2 Stručný životopis

Peter David Lax se narodil 1. května 1926 v Budapešti. V roce 1941 se s rodiči přestěhoval do New Yorku. V roce 1949 získal na Newyorské univerzitě titul Ph.D. pod vedením významného matematika Kurta O. Friedrichse. O rok později začal pracovat v Los Alamos jako konzultant. Od roku 1951 byl pak zaměstnán v Courantově ústavu matematických věd (University of New York), kde v letech 1972–1980 působil ve funkci ředitele. Ústav (viz obr. 3.1) je pojmenován po dalším vynikajícím matematikovi Richardu Courantovi, zakladateli metody konečných prvků. V roce 1958 P. Lax vyslovil domněnku týkající se maticové reprezentace různých hyperbolických polynomů, kterou se podařilo dokázat až v roce 2003. V období 1969–1971 byl viceprezidentem Americké matematické společnosti a později (1977–1980) se stal jejím prezidentem.

Během života Peter Lax získal řadu významných ocenění. Například v roce 1975 Cenu Norberta Wienera od Americké matematické společnosti a společnosti SIAM. V roce 1986 převzal v Bílém domě z rukou prezidenta Ronalda Reagana medaili za vědu (National Medal of Science). O rok později obdržel Wolfovu cenu a v roce 1992 Steelovu cenu Americké matematické společnosti. Celkem 9 univerzit mu udělilo čestný doktorát.

Podívejme se nyní stručně na některé Laxovy důležité výsledky (viz [10]).

3.3 Laxovo–Milgramovo lemma

Celá řada úloh z technické praxe vede na okrajové úlohy pro parciální (popř. obyčejné) diferenciální rovnice eliptického typu. Typickými



Obr. 3.1 Courantův ústav na Mercer street 251 v New Yorku (foto M. Křížek)

příklady jsou diferenciální rovnice popisující gravitační, elektrický či magnetický potenciál, rovnice proudění, rovnice lineární pružnosti, rovnice ustáleného vedení tepla apod. Klasické řešení těchto úloh většinou neexistuje, neboť případné materiálové konstanty mohou mít skoky, vyšetřovaná oblast nemusí být konvexní nebo nemá hladkou hranici. Potíže mohou nastat i v těch bodech hranice, kde jeden typ okrajové podmínky přechází v jiný typ a kdy se požaduje spojitost derivací až do hranice. To způsobuje, že nelze obecně zaručit globální hladkost řešení, tj. neexistují derivace vystupující v klasické formulaci.

Proto se většinou hledá tzv. slabé řešení těchto úloh, kdy výše uvedené obtíže nejsou na překážku, a pomocí Laxova–Milgramova lemmatu (viz [11]) lze dokázat existenci právě jednoho takového řešení.

Laxovo–Milgramovo lemma. *Nechť V je Hilbertův prostor nad reálnými čísly s normou $\|\cdot\|$, F je spojitý lineární funkcionál na V a nechť $a(\cdot, \cdot)$ je bilineární forma, která je spojitá, tj.*

$$\exists C > 0 \quad \forall v, w \in V \quad |a(v, w)| \leq C\|v\|\|w\|, \quad (3.1)$$

a V -eliptická, tj.

$$\exists c > 0 \quad \forall v \in V \quad a(v, v) \geq c\|v\|^2. \quad (3.2)$$

Pak problém najít $u \in V$ takové, že

$$a(u, v) = F(v) \quad \forall v \in V, \quad (3.3)$$

má právě jedno řešení.

Ukažme si použití Laxova–Milgramova lemmatu na jednoduchém příkladě. Nechť $\Omega \subset \mathbb{R}^d$ ($d \in \{1, 2, 3, \dots\}$) je omezená oblast, jejíž hranice $\partial\Omega$ je lipschitzovsky spojitá (viz [14]). Klasické řešení Poissonovy rovnice s Dirichletovou okrajovou podmínkou

$$-\Delta u = f \quad \text{v } \Omega, \quad (3.4)$$

$$u = 0 \quad \text{na } \partial\Omega, \quad (3.5)$$

kde $\Delta = \partial^2/\partial x_1^2 + \dots + \partial^2/\partial x_d^2$ je Laplaceův operátor a f patří do Lebesgueova prostoru $L^2(\Omega)$, se obvykle hledá v prostoru $C^2(\Omega)$. Je-li funkce f např. po částech spojitá, což je z praktického hlediska dosti častý případ, klasické řešení nemusí existovat. Proto si nyní stručně naznačíme, jak se klasická úloha převede na slabou formulaci.

Zavedme prostor testovacích funkcí

$$V = \left\{ v \in L^2(\Omega); \frac{\partial v}{\partial x_i} \in L^2(\Omega), i = 1, \dots, d, v = 0 \text{ na } \partial\Omega \right\}, \quad (3.6)$$

kde parciální derivace chápeme ve smyslu distribucí a rovnici $v = 0$ na hranici $\partial\Omega$ ve smyslu stop (viz [1] nebo [14]). Předpokládejme, že nějaké řešení $u \in V \cap C^2(\Omega)$ splňuje (3.4)–(3.5). Vynásobíme-li rovnici (3.4) testovací funkcí $v \in V$, pak integrací přes Ω dostaneme

$$-\int_{\Omega} (\Delta u)v \, dx = \int_{\Omega} f v \, dx.$$

Greenova věta (integrace per partes) aplikovaná na levou stranu rovnice dává

$$\int_{\Omega} \nabla u \cdot \nabla v \, dx = \int_{\Omega} f v \, dx \quad \forall v \in V; \quad (3.7)$$

příslušný povrchový integrál přes $\partial\Omega$ je roven nule, neboť testovací funkce v je nulová na $\partial\Omega$. Úloha najít $u \in V$ splňující rovnost (3.7)

se nazývá *slabá formulace* klasické úlohy a její řešení $u \in V$ se nazývá *slabé řešení*. Navíc vidíme, že pokud klasické řešení úlohy (3.4)–(3.5) existuje v prostoru $V \cap C^2(\Omega)$, pak je také slabým řešením.

Označíme-li $a(u, v)$ levou stranu rovnice (3.7) a $F(v)$ její pravou stranu, pak (3.7) je tvaru (3.3). Snadno se lze přesvědčit, že prostor (3.6) se skalárním součinem

$$(v, w)_V = \int_{\Omega} vw \, dx + \sum_{i=1}^d \int_{\Omega} \frac{\partial v}{\partial x_i} \frac{\partial w}{\partial x_i} \, dx, \quad v, w \in V,$$

je Hilbertův, že F je lineární spojitý funkcional na V a že $a(\cdot, \cdot)$ je bilineární spojitá forma. Její V -eliptičnost (3.2) plyne z Friedrichsovy nerovnosti (viz [14]). Z Laxova–Milgramova lemmatu plyne existence právě jednoho $u \in V$, které splňuje (3.7) pro $f \in L^2(\Omega)$ (např. pro f po částech spojitou).

Přibližné řešení u_h úlohy (3.7) se většinou hledá metodou konečných prvků v nějakém konečněrozměrném neprázdném podprostoru $V_h \subset V$, kde h charakterizuje míru diskretizace. Podprostor $V_h \subset V$ se konstruuje následovně [6]. Vytvoří se *triangulace* uzávěru vyšetřované oblasti na jednodušší uzavřené podoblasti. Ty se nazývají *prvky* a mohou to být úsečky, trojúhelníky, čtyřúhelníky, čtyřstěny, pětistěny, kvádry apod. *Prostor konečných prvků* V_h se zpravidla volí tak, že každá funkce $v_h \in V_h$ je spojitá na celé oblasti a je polynomem na každém prvku. Přibližné řešení $u_h \in V_h$ splňuje rovnici

$$a(u_h, v_h) = F(v_h) \quad \forall v_h \in V_h.$$

Existence a jednoznačnost takového $u_h \in V_h$ je pak opět zaručena Laxovým–Milgramovým lemmatem.

Hledáme-li $u_h \in V_h$ ve tvaru lineární kombinace báзовých funkcí $\{v^i\} \subset V_h$, pak dostaneme soustavu lineárních algebraických rovnic s regulární maticí $(a(v^i, v^j))$, $i, j = 1, 2, \dots, \dim V_h$. Podle (3.7) bude tato matice řídká (tj. s mnoha nulovými prvky), jestliže zvolíme báзовé funkce tak, aby měly malý nosič v porovnání s mírou Ω . To pak umožní podstatně zkrátit výpočetní čas a šetřit paměť počítače.

Laxovo–Milgramovo lemma vlastně zobecňuje známou Rieszovu větu o reprezentaci lineárních spojitých funkcionalů pomocí skalárního součinu.

Rieszova věta. *Nechť V je Hilbertův prostor se skalárním součinem $(\cdot, \cdot)_V$. Pak pro každý lineární spojitý funkcionál F definovaný na V existuje právě jeden prvek $u \in V$ tak, že $F(v) = (v, u)_V$ pro všechna $v \in V$.*

Forma $a(\cdot, \cdot)$ v Laxově–Milgramově lemmatu ale není skalárním součinem, pokud není symetrická. S nesymetrickými formami je zapotřebí pracovat v úlohách proudění [1] nebo při výpočtu elektromagnetického pole [7]. Například pro okrajovou úlohu

$$\begin{aligned} -u'' + u' + u &= f \quad \text{v } (0, 1), \\ u(0) &= u(1) = 0 \end{aligned}$$

je příslušná bilineární forma

$$a(v, w) = \int_0^1 (v'w' + v'w + vw)dx, \quad v, w \in V$$

nesymetrická, kde V je dáno (3.6) pro $d = 1$. Hilbertův prostor V vystupující v Laxově–Milgramově lemmatu může být i nad komplexními čísly [5]. Pak je ale třeba dát levou stranu nerovnosti (3.2) do absolutní hodnoty.

3.4 Konvergence numerických schémat

Nechť A je lineární diferenciální operátor eliptického typu v prostorových proměnných $x = (x_1, \dots, x_d)$, který každé dostatečně hladké skalární funkci $u = u(t, x)$ přiřazuje skalární funkci Au . Uvažujme parabolickou úlohu

$$\frac{\partial u}{\partial t} = Au \quad \text{pro } t \in [0, T], \quad (3.8)$$

$$u(0) = u_0, \quad (3.9)$$

kde $T > 0$ a u_0 představuje počáteční podmínku pro u v čase 0.

Peter Lax se zabýval numerickou metodou konečných diferencí pro řešení této počáteční úlohy. K jeho hlavním výsledkům patří věta, podle níž je metoda konvergentní právě tehdy, když je stabilní a konzistentní (pro příslušné definice viz např. přehledový článek [12]). Tato nutná a postačující podmínka je známá jako Laxův princip ekvivalence. Později ji Lax společně s Wendroffem zobecnil na jistou třídu

nelineárních hyperbolických rovnic. Laxova–Wendroffova věta zhruba říká, že pokud diskrétní řešení jsou stejnoměrně omezená a konvergují, pak jejich limita je řešením původního hyperbolického problému (viz [1]).

Jako ilustrační příklad uvažujme funkci $u = u(x, t)$, $x \in \mathbb{R}^1$, $t > 0$, jež je řešením lineární advekční rovnice s konstantním koeficientem $k \in \mathbb{R}^1$,

$$\frac{\partial u}{\partial t} + k \frac{\partial u}{\partial x} = 0, \quad (3.10)$$

kde $u(x, 0) = u_0(x)$ a $u_0 = u_0(x)$ je zadaná počáteční podmínka. Přímký $x = kt + c$ se nazývají *charakteristiky* a funkce $\bar{u}(x, t) := u_0(x - kt)$ je na nich konstantní. Rovnice (3.10) popisuje například unášení látky o koncentraci u jednorozměrným kanálem rychlostí k ve směru osy x .

Peter Lax studoval numerická řešení hyperbolické soustavy partiálních diferenciálních rovnic 1. řádu (viz [8], [9], [13])

$$\frac{\partial \mathbf{u}}{\partial t} + \frac{\partial f(\mathbf{u})}{\partial x} = 0, \quad (3.11)$$

kde $\mathbf{u} = (u_1, \dots, u_m)$ je neznámá vektorová funkce a f závisí obecně nelineárně na $x, t, \mathbf{u}$. Slabá řešení (3.11) ale nejsou určena jednoznačně počáteční podmínkou. Přitom entropická podmínka umožňuje získat fyzikálně relevantní řešení.

Peter Lax společně s Amiramem Hartenem a dalšími kolegy (viz [2], [3]) navrhl několik explicitních a implicitních schémat metody konečných diferencí aproximujících slabá řešení soustavy (3.11). Jde zejména o monotónní schémata 2. řádu. Přehledový článek [4] pojednává o tzv. upwindových (upstreamových) schématech pro numerické řešení rovnice (3.11) s počáteční podmínkou. V práci [9] je publikována konzervativní metoda konečných diferencí, dnes nazývaná Laxova–Friedrichsova. Je založena na centrálních diferencích a součet všech numerických toků je na každé časové vrstvě nulový.

P. Lax také studoval rázové vlny, které vznikají např. při nadzvukových rychlostech letadel nebo při explozích. Vyvinul nové matematické postupy, které nám umožňují pochopit a též simulovat na počítači tento důležitý jev, kdy dochází skokem ke změně hustoty a tlaku. V roce 1957 přišel s entropickou podmínkou, jež dovoluje z mnoha nespojitých a singulárních řešení vybrat to, které má dobrý

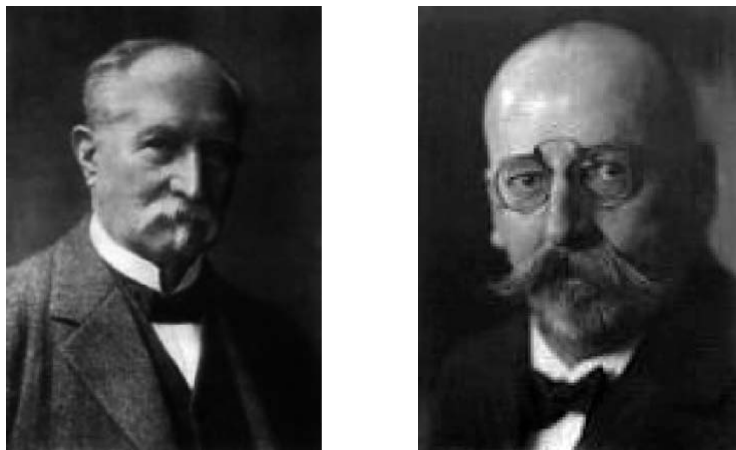
fyzikální smysl. Poznamenejme ještě, že entropickou podmínkou se u nás zabýval též prof. Jindřich Nečas.

3.5 Laxův přínos k teorii solitonů

V roce 1834 si skotský inženýr John Scott Russell povšiml, že když se na vodním kanálu zastaví loď tažená koňmi, vznikne izolovaná vlna, která se šíří dále po kanálu až do vzdálenosti několika kilometrů. Později nizozemský matematik Diederik Johannes Korteweg a jeho student Gustav de Vries (viz obr. 3.2) odvodili evoluční parciální diferenciální rovnici, která tento jev popisuje:

$$\frac{\partial u}{\partial t} = 6u \frac{\partial u}{\partial x} - \frac{\partial^3 u}{\partial x^3}, \quad (3.12)$$

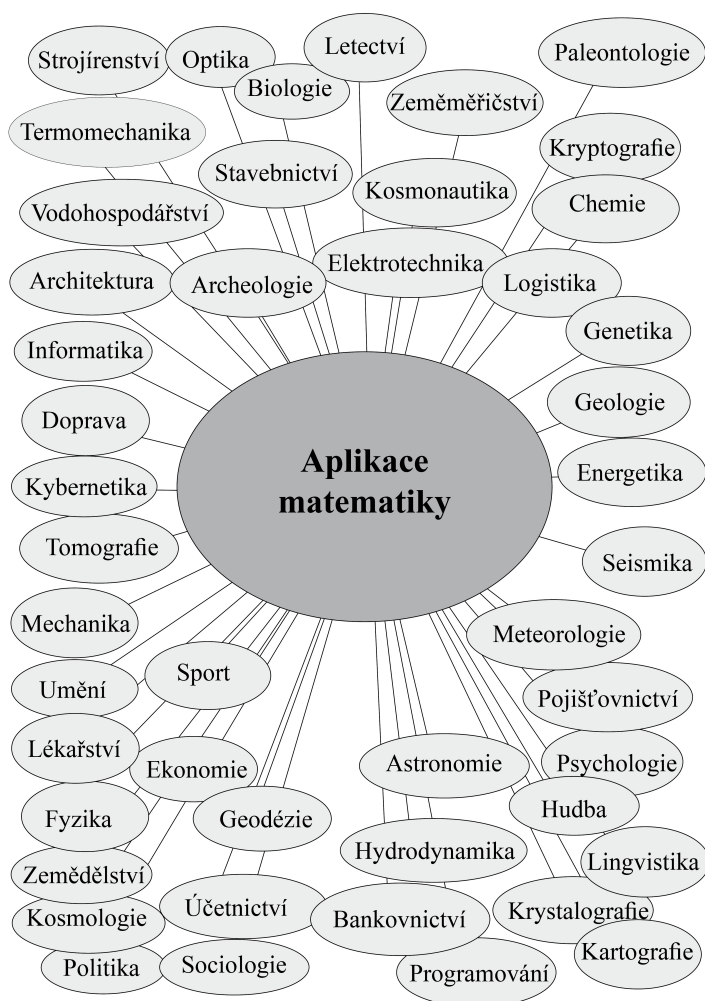
kde $u = u(t, x)$ označuje výšku vlny v čase t a bodě x . Tak vznikla matematická teorie solitonů. P. Laxovi se v roce 1968 podařilo pomocí Lieovy teorie grup rozložit nelineární diferenciální operátor třetího řádu na pravé straně rovnice (3.12) na operátory nižšího řádu. To pak umožnilo snadněji řešit Kortewegovu–de Vriesovu rovnici analyticky i numericky. Dnes má teorie solitonů řadu aplikací v kvantové teorii pole, při přenosu informace ve světlovodičích, při modelování biologických systémů a dokonce i při modelování vln cunami (viz [15]).



Obr. 3.2 Diederik J. Korteweg a Gustav de Vries (zdroj Wikipedia)

3.6 Aplikace matematiky z pohledu P. Laxe

Na počátku 20. století matematika neměla příliš mnoho praktických aplikací. Dnes bychom však asi jen obtížně hledali obor lidské činnosti, kde matematika dosud nenašla uplatnění. Její aplikace jsou skutečně rozsáhlé. Některé praktické oblasti jejího použití jsou schematicky znázorněny na obr. 3.3, ale zdaleka to nejsou všechny. Jen těžko si lze představit, že bychom žili bez rozhlasu, televize, kopírek,



Obr. 3.3 Schematické znázornění aplikací matematiky v nejružnějších oblastech lidské činnosti (nakreslil V. Pravda)

digitálních fotoaparátů a kamer, mobilních telefonů, GPS, telekomunikačních družic, laserů, rentgenu, mikročipů, počítačových tomografií a samotných počítačů včetně špičkového softwaru (GOOGLE, MATLAB, AUTOCAD, LINUX, HTML, ...). Tyto moderní výdobytky civilizace by bez matematicko-fyzikálních věd nevznikly a aplikovaná matematika sehrála při jejich vzniku nezastupitelnou roli.

Peter Lax sám sebe považuje za čistého i aplikovaného matematika. Významně se zasloužil o řešení problémů matematické fyziky popsaných nelineárními diferenciálními rovnicemi. Bohužel neexistuje obecná numerická metoda, která by umožňovala řešit jakýkoliv nelineární problém. A tak se každá třída nelineárních problémů musí vyšetřovat zvlášť. P. Lax se kromě již výše uvedených problémů zabýval řešením Eulerových rovnic proudění plynů. Studoval také matematické modely porézních materiálů, které umožňují simulovat pohyb uhlovodíků v přírodních nalezištích. Je spoluautorem známé teorie rozptylu (angl. Lax–Phillips scattering theory). Další jeho objevy jsou obsaženy ve vybraných spisech [10].

Peter Lax je velký příznivec využití počítačů v matematice. Tvrdí, že jejich úloha je srovnatelná s významem dalekohledů v astronomii či mikroskopů v biologii. Mladým studentům doporučuje, aby si trénovali matematické dovednosti na řešení konkrétního problému aplikované matematiky.

L i t e r a t u r a

- [1] FEISTAUER, M.: *Mathematical methods in fluid dynamics*. Longman, Harlow 1993.
- [2] HARTEN, A.: *On a class of a high resolution total-variation-stable finite-difference schemes* (with Appendix by P.D. Lax). SIAM J. Numer. Anal. 21 (1984), 1–23.
- [3] HARTEN, A., HYMAN, J. M., LAX, P. D.: *On finite-difference approximations and entropy conditions for shocks*. Comm. Pure Appl. Math. 29 (1976), 297–322.
- [4] HARTEN, A., LAX, P. D., VAN LEER, B.: *On upstream differencing and Godunov-type schemes for hyperbolic conservation laws*. SIAM Rev. 25 (1983), 35–61.

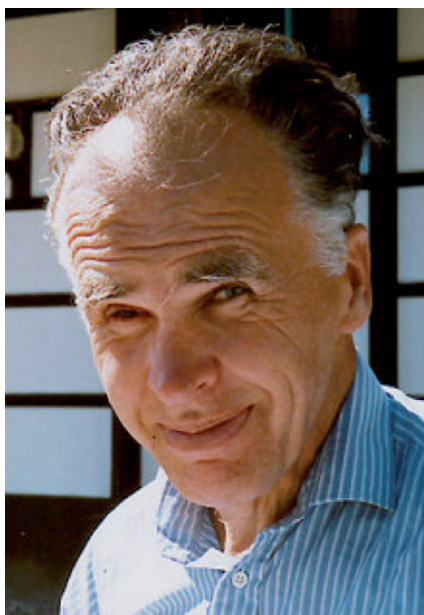
- [5] KOUKAL, S., KŘÍŽEK, M., POTŮČEK, R.: *Fourierovy trigonometrické řady a metoda konečných prvků v komplexním oboru*. Academia, Praha, 2002.
- [6] KŘÍŽEK, M., NEITTAANMÄKI, P.: *Finite element approximation of variational problems and applications*. Pitman Monographs and Surveys in Pure and Applied Mathematics vol. 50, Longman Scientific & Technical Harlow; copublished in the United States with John Wiley & Sons, New York, 1990.
- [7] KŘÍŽEK, M., NEITTAANMÄKI, P.: *Mathematical and numerical modelling in electrical engineering: theory and applications*. Kluwer Academic Publishers, Dordrecht, 1996.
- [8] LAX, P. D.: *Nonlinear partial differential equations and computing*. SIAM Rev. 11 (1969), 7–19.
- [9] LAX, P. D.: *Weak solutions of nonlinear hyperbolic equations and their numerical computation*. Comm. Pure Appl. Math. 7 (1954), 159–193.
- [10] LAX, P. D.: *Selected papers, volume I and II*. Eds. A. J. Majda and P. Sarnak, Springer, New York 2005.
- [11] LAX, P. D., MILGRAM, A. N.: *Parabolic equations. Contribution to the theory of partial differential equations*. Ann. Math. Stud. 33 (1954), 167–190.
- [12] LAX, P. D., RICHTMYER, R. D.: *Survey of the stability of linear finite difference equations*. Comm. Pure Appl. Math. 9 (1956), 267–293.
- [13] LAX, P. D., WENDROFF, B.: *Systems of conservation laws*. Comm. Pure Appl. Math. 13 (1960), 217–237.
- [14] NEČAS, J., HLAVÁČEK, I.: *Mathematical theory of elastic and elastoplastic bodies: an introduction*. Elsevier, Amsterdam 1981.
- [15] ŠVADLENKA, K.: *Matematické modely a numerická simulace vln tsunami*. PMFA 57 (2012), 177–185.

4. Abelovu cenu za rok 2006 získal Lennart Carleson

Michal Křížek

4.1 Prolog

V úterý 23. května 2006 obdržel profesor Lennart Carleson Abelovu cenu za rok 2006 z rukou Jeho Veličenstva norského krále Haralda V. na univerzitě v Oslu. Podle vyjádření komise pro výběr kandidátů do-



LENNART CARLESON

stal tuto cenu za *své fundamentální příspěvky k harmonické analýze a k teorii hladkých dynamických systémů*. Pod tímto stručným vyjádřením se skrývá zejména Carlesonův důkaz konvergence Fourierových řad funkcí integrovatelných s kvadrátem a důkaz existence podivných atraktorů Hénonova zobrazení. Podrobněji o tom pojednáme v kapitolách 4.3 a 4.4.

4.2 Kdo je Lennart Carleson?

Lennart Axel Edvard Carleson se narodil 18. března 1928 ve Stockholmu. Studoval na univerzitě v Uppsale, kde získal doktorát pod vedením známého švédského matematika Arne Beurlinga. V období 1950–1951 Carleson působil na Harvardově univerzitě jako postdoktorand. V pouhých 26 letech se stal profesorem na univerzitě ve Stockholmu. O rok později byl jmenován profesorem v Uppsale a následně byl též profesorem na Kalifornské univerzitě v Los Angeles a v Královském technologickém institutu ve Stockholmu (viz [16]).

V období 1968–1984 byl ředitelem Mittag-Lefflerova institutu v Djursholmu na severním okraji Stockholmu. Významný švédský matematik Gösta Mittag-Leffler (1846–1927) nechal postavit tuto majestátní budovu na konci 19. století jako rezidenci, knihovnu a místo, kde se mohla scházet kulturní a akademická elita. Carleson záhy objevil duchovní potenciál tohoto místa a zorganizoval financování a založení Mittag-Lefflerova institutu tak, jak jej dnes zná mezinárodní matematická komunita, tj. jako matematického centra, kde se setkávají specialisté z celého světa na kratší či střednědobé pobyty.

Od roku 1956 Carleson působil 23 let ve funkci vedoucího redaktora časopisu *Acta Mathematica*, který má dlouholetou historii spojenou s Mittag-Lefflerovým institutem. Velmi se věnoval popularizaci matematiky ve Švédsku a vyučování matematice. Je autorem knihy *Mathematics of Our Time*. Vychoval 26 Ph.D. studentů, z nichž mnozí jsou dnes již profesory. V letech 1978–1982 byl prezidentem Mezinárodní matematické unie. Tvrdě pracoval na tom, aby také Čína byla zastoupena v unii, což bylo v tehdejší době politicky dosti obtížné.

Carleson byl třikrát pozván jako hostující přednášející na mezinárodní matematický kongres, z čehož jednou měl plenární přednášku, což se považuje za jedno z nejvyšších ocenění v mezinárodní matematické komunitě. Obdržel čestný doktorát na několika univerzi-

tách a byl zvolen členem korespondentem řady akademií a učených společností (mj. Norwegian Academy of Science and Letters, Royal Norwegian Society of Sciences and Letters). Během svého života získal celou řadu významných ocenění za svou práci, např. v roce 1984 Steellovu cenu Americké matematické společnosti, v roce 1994 Wolfovu cenu, v roce 2002 Lomonosovovu zlatou medaili Ruské akademie věd a v roce 2003 Sylvestrovu medaili Královské společnosti v Londýně.

Podívejme se nyní stručně na matematickou formulaci dvou nejdůležitějších Carlesonových výsledků.

4.3 Konvergence Fourierových řad

Problém, který Carleson vyřešil, spadá do oblasti harmonické analýzy, jejíž základy položil francouzský matematik Jean Baptiste Joseph Fourier (1768–1830) kolem r. 1807. Jde o to, zda libovolnou periodickou funkci s periodou 2π lze vyjádřit jako nekonečnou sumu funkcí $\sin mx$ a $\cos mx$ s vhodnými koeficienty, kde m jsou nezáporná čísla. Fourier byl však ve svých formulacích dosti vágní. Kolem roku 1915 (viz [6, odst. 10.4.5]) domněnku přesně zformuloval ruský matematik Nikolaj N. Luzin (1883–1950), ale nebyl schopen ji dokázat. Po něm byla nazvána *Luzinovou domněnkou*. Více o její historii lze najít v PMFA v článku F. Štěpánka [14, s. 126–127]. V roce 1966 Luzinovu domněnku kladně vyřešil L. Carleson – viz níže uvedenou větu.

Nejprve si zavedeme některé pojmy. Nechť f je reálná lebesgueovsky integrovatelná funkce definovaná na uzavřeném intervalu $[0, 2\pi]$ a m je celé číslo. Pak m -tý Fourierův koeficient $\hat{f}(m)$ funkce $f = f(x)$ a n -tý částečný součet s_n Fourierovy řady funkce f (vzhledem k ortonormálnímu systému $\{e^{inx}\}_{n=-\infty}^{\infty}$) jsou definovány takto:

$$\hat{f}(m) = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-imt} dt, \quad s_n(x) = \sum_{m=-n}^n \hat{f}(m) e^{imx}.$$

Označíme-li

$$a_m = 2\operatorname{Re}\hat{f}(m) = \frac{1}{\pi} \int_0^{2\pi} f(t) \cos mt \, dt,$$

$$b_m = 2\operatorname{Im}\hat{f}(m) = \frac{1}{\pi} \int_0^{2\pi} f(t) \sin mt \, dt,$$

pak $\hat{f}(m) = (a_m - ib_m)/2$ a částečný součet $s_n(x)$ můžeme zapsat v reálném tvaru

$$s_n(x) = \frac{a_0}{2} + \sum_{m=1}^n (a_m \cos mx + b_m \sin mx).$$

Luzinovu domněnku dokázal Carleson v práci [5]:

Věta. *Nechť f je reálná funkce na intervalu $[0, 2\pi]$, která je lebesgueovsky integrovatelná s kvadrátem. Pak s_n konverguje k f pro $n \rightarrow \infty$ skoro všude.*

Tato věta byla později zobecněna Richardem A. Hunttem na funkce integrovatelné s p -tou mocninou pro $p > 1$ – tzv. Carlesonova–Hunttova věta (viz [14, s. 127]).

Fourierovy trigonometrické řady patří k základům matematické analýzy. O historii těchto řad je stručně pojednáno v [6]. Od svého objevu jsou využívány při studiu a popisu periodických dějů, např. kmitání v mechanice a elektrotechnice. Používají se ale i při řešení úloh, ve kterých a priori nejde o periodické jevy. Tak je tomu např. v [15] při rozpoznávání tvarů předmětů pomocí tzv. Fourierových deskriptorů. V [12, kap. 11] je zase řešení trojrozměrné okrajové eliptické úlohy na osově symetrické oblasti převedeno fourierovskou metodou konečných prvků na řešení posloupnosti dvojrozměrných úloh, které se pak řeší standardní metodou konečných prvků.

Na závěr této kapitoly ještě připomeňme, že bez Fourierovy analýzy bychom dnes neměli např. moderní automobily, televizi, výškové budovy, formáty JPG a MP3 používané v digitálních fotoaparátech, hudebních přehrávačích a v řadě softwarových produktů.

4.4 Existence podivného atraktoru Hénonova zobrazení

V roce 1960 se americký meteorolog Edward Lorenz z Massachusettského technologického ústavu (MIT) pokoušel předpovídat počasí pomocí primitivního počítače. Svůj diskrétní dynamický model omezil jen na tři parametry (viz [13]). Jednou musel v polovině výpočtu běh programu přerušit. Hodnoty tří mezivýsledků si pečlivě zapsal a druhý den ve výpočtu pokračoval. Pro jistotu pak celý výpočet zopakoval a překvapivě zjistil, že dostal úplně jiné výsledné hodnoty, než kdyby výpočet nepřerušil. Jak se to mohlo stát? Vždyť rovnice byly stejné

a počítač i program se nezměnily. Důkladnou analýzou odhalil, že při zapisování mezivýsledků v desítkové soustavě došlo k zaokrouhlování s relativní chybou menší než 0.00001 %. Tato nepatrná změna v jednom kroku však způsobila obrovské změny ve výsledném řešení. Lorenz tak objevil jev, kterému se dnes v meteorologii říká *efekt motýlího křídla*, tj. nepatrné mávnutí křídlů motýla v březnu někde v Pekingu může způsobit v srpnu změnu směru hurikánu v Atlantském oceánu. Nesmírně malá odchylka, která je v každém kroku mírně zvětšována, může tedy vést po mnoha krocích k naprosto nepředvídatelnému stavu.

V roce 1976 francouzský astronom Michel Hénon zjednodušil Lorenzův diskrétní systém jen na dva parametry. Přitom jeho systém měl podobné podivné chování jako systém Lorenzův. Hénon definoval zobrazení T roviny do sebe velice jednoduchým vztahem (viz [10])

$$T(x, y) = (1 + y - 1.4x^2, 0.3x).$$

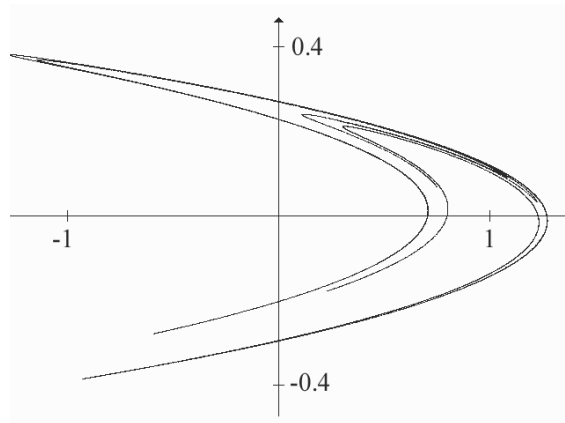
Vidíme, že první složka funkční hodnoty T je kvadratická funkce, kdežto druhá složka je dokonce lineární. Odpovídající diskrétní dynamický systém pro $n = 0, 1, 2, \dots$ je pak dán rovnicemi

$$\begin{aligned}x_{n+1} &= 1 + y_n - ax_n^2, \\y_{n+1} &= bx_n,\end{aligned}$$

kde $a = 1.4$ a $b = 0.3$ jsou hodnoty parametrů, které Hénon původně navrhl.

Bod $(0, 0)$ se pomocí T zobrazí na bod $(1, 0)$, bod $(1, 0)$ se zobrazí na bod $(-0.4, 0.3)$, jenž se dále zobrazí na bod $(1.076, -0.12)$ atd. Příslušné iterace se budou hromadit poblíž tzv. *podivného atraktoru*, tj. množiny, která je znázorněna na obr. 4.1. Budou sice postupně chaoticky „skákat“ na všechny strany (zdánlivě velice nesystematicky), ale stále se budou přibližovat k této množině. Jestliže začneme z bodu $(0, 0.2918)$, dostaneme překvapivě též atraktor. Pokud ale vystartujeme z bodu $(0, 0.2919)$, odpovídající iterace půjdou velice rychle do nekonečna. Vidíme tedy, že chování i poměrně jednoduchého nelineárního dynamického systému může být značně komplikované.

Pro libovolné reálné parametry a a b nazveme funkci T definovanou vztahem $T(x, y) = (1 + y - ax^2, bx)$ *Hénonovým zobrazením*. Snadno



Obr. 4.1 Hénonův podivný atraktor zobrazení T v oblasti $(-1.3, 1.3) \times (-0.4, 0.4)$, (nakreslil M. Křížek).

lze ověřit, že T má pro $a \neq 0$ dva pevné body:

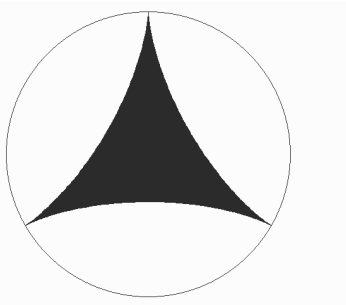
$$x_n = \frac{1}{2a} \left(b - 1 \pm \sqrt{(1 - b)^2 + 4a} \right),$$

$$y_n = bx_n,$$

tj. body, pro něž $x_{n+1} = x_n$ a současně $y_{n+1} = y_n$. Pro $a = 1.4$ a $b = 0.3$ má jeden z těchto pevných bodů souřadnice $x_n \doteq 0.63135$ a $y_n \doteq 0.18941$ a druhý $x_n \doteq -1.13135$ a $y_n \doteq -0.33941$. Oba pevné body jsou ale nestabilní, neboť libovolně malá perturbace odkloní příslušné iterace k podivnému atraktoru.¹

Carleson společně se svým krajanem Benedicksem jako první dokázali existenci podivného atraktoru pro Hénonovo zobrazení a jeho fraktální charakter (viz [1]). Tento atraktor má napříč „trajektorií“ z obr. 4.1“ strukturu jako Cantorova množina. Numerické testy ukazují, že jeho Hausdorffova dimenze je 1.26 ± 0.003 . S populárním výkladem o neceločíselné dimenzi se může čtenář seznámit v článku Jiřího Fialy [9].

¹Již před 100 lety se francouzský matematik Pierre Fatou [7] zabýval hledáním pevných bodů zobrazení T (viz též [8]). Složky tohoto zobrazení mohly být dokonce racionální funkce. Také Gaston Julia [11] studoval množiny všech počátečních podmínek, pro něž je posloupnost (x_n, y_n) omezená. Tehdy ale nebyly k dispozici žádné elektronické počítače, které by umožňovaly nakreslit příslušné fraktální množiny.



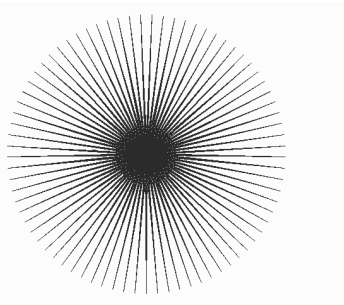
Obr. 4.2 Černě je obarvena oblast ohraničená Steinerovou hypocykloidou uvnitř kružnice o poloměru $3/4$ (nakreslil M. Křížek).

4.5 Další Carlesonovy výsledky

Lennart Carleson též přispěl k řešení několika záludných problémů. V roce 1917 japonský matematik Sóiči Kakeja zformuloval následující úlohu. Namočme jehlu do inkoustu a položme ji na list papíru. Jehlu je třeba otočit o 180° , aniž bychom ji nadzvedli. Přitom jí můžeme jakkoliv posunovat dopředu i dozadu tak, jako když se snažíme zaparkovat auto. Navíc předpokládáme, že jehla má nulovou tloušťku. Otázka zní: *Jak velká je obarvená plocha a jaký je nejlepší dolní odhad velikosti této plochy?*

Můžeme si rovněž klást otázky: *Jak posunovat a otáčet jehlou tak, aby obarvená plocha byla minimální? Existuje vůbec taková plocha o minimálním obsahu?* Uvidíme, že na poslední dvě otázky existuje negativní odpověď.

Bez újmy na obecnosti můžeme předpokládat, že jehla má délku 1. Pokud bychom jehlu otočili o 180° kolem její špičky, měla by obarvená plocha zřejmě velikost $\pi/2 \doteq 1.57$. Pokud bychom jí rotovali kolem jejího středu, získáme plochu o poloviční velikosti $\pi/4 \doteq 0.78$. To ovšem jistě není nejmenší plocha, protože jehlu můžeme také posouvat a otáčet o 180° uvnitř rovnostranného trojúhelníka s jednotkovou výškou a plochou $1/\sqrt{3} \doteq 0.58$. Ještě menší plochu dostaneme, když se s jehlou budeme pohybovat uvnitř Steinerovy hypocykloidy, tj. křivky, kterou opisuje bod na kružnici o poloměru $1/4$, jež se kotálí zevnitř po obvodu kružnice o poloměru $3/4$. Tímto způsobem lze získat plochu o obsahu přibližně 0.39, o které se Kakeja domníval, že je minimální (viz obr. 4.2). V roce 1928 ale ruský matematik



Obr. 4.3 Plocha složená z mnoha dlouhých a úzkých trojúhelníků (nakreslil M. Křížek).

Abram S. Besikovič (1891–1970) překvapivě dokázal, že obarvenou plochu můžeme udělat libovolně malou (viz [2], [3]). Jeho plocha se skládá z velkého množství úzkých trojúhelníků podobných jehličkám na vánočním stroměčku (viz obr. 4.3).

Carleson a jeho student Per Sjölin se zabývali zobecněním této úlohy, což později použili v teorii Fourierových multiplikátorů jako standardní prostředek.

Další japonský matematik Šizuo Kakutani na počátku 40. let minulého století zformuloval tzv. problém koróny (angl. corona problem), který se týká jisté třídy omezených analytických funkcí definovaných na jednotkovém kruhu v komplexní rovině. Otázka zní, co lze říci o chování těchto funkcí na hranici, jestliže víme, jak se chovají uvnitř kruhu. Jde tedy o čistě matematický problém, i když slovo koróna běžně označuje prstenec světla, který je vidět kolem Slunce při jeho úplném zatmění. Carleson problém koróny vyřešil v článku [4] z roku 1962. Zavádí zde speciální míru, která byla po něm později nazvána *Carlesonova míra*. Dnes se běžně používá v komplexní i harmonické analýze.

Komise pro výběr kandidátů na Abelovu cenu tedy právem ocenila Carlesonovy zásluhy o rozvoj matematiky, jeho široký záběr i organizační schopnosti. Z jejích závěrů citujme alespoň tuto větu: *Lennart Carleson is a brilliant scientist with a broad vision for mathematics and for the role of mathematics in the global community.*

L i t e r a t u r a

- [1] BENEDICKS, M., CARLESON, L.: *The dynamics of the Hénon map*. Ann. of Math. 133 (1991), 73–169.
- [2] BESICOVITCH, A. S.: *On Kakeya's problem and a similar one*. Math. Z. 27 (1927), 312–320.
- [3] BESICOVITCH, A. S.: *The Kakeya problem*. Amer. Math. Monthly 70 (1963), 697–706.
- [4] CARLESON, L.: *Interpolations by bounded analytic functions and the corona problem*. Ann. of Math. 76 (1962), 547–559.
- [5] CARLESON, L.: *On convergence and growth of partial sums of Fourier series*. Acta Math. 116 (1966), 135–157.
- [6] EDWARDS, R. E.: *Fourier series. A modern introduction, vol. 1*. Springer-Verlag, New York 1979.
- [7] FATOU, P.: *Sur les solutions uniformes de certaines équations fonctionnelles*. C. R. Acad. Sci. Paris 143 (1906), 546–548.
- [8] FATOU, P.: *Sur les équations fonctionnelles*. Bull. Soc. Math. France 47 (1919), 161–271, 48 (1920), 33–94, 208–314.
- [9] FIALA, J.: *Jedenapůlrozměrný prostor*. Vesmír 84 (2005), 734–739.
- [10] HÉNON, M.: *A two dimensional mapping with a strange attractor*. Comm. Math. Phys. 50 (1976), 69–77.
- [11] JULIA, G.: *Mémoire sur l'itération des fonctions rationnelles*. J. Math. Pures Appl. 4 (7), (1918), 47–245.
- [12] KOUKAL, S., KŘÍŽEK, M., POTŮČEK, R.: *Fourierovy trigonometrické řady a metoda konečných prvků v komplexním oboru*. Academia, Praha 2002.
- [13] LORENZ, E. N.: *Deterministic non-periodic flow*. J. Atmos. Sci. 20 (1963), 130–141.
- [14] ŠTĚPÁNEK, F.: *130 let divergentních trigonometrických řad (2. část)*. PMFA 49 (2004), 122–128.
- [15] ZAHN, C. T., ROSKIES, R. Z.: *Fourier description for plane closed curves*. IEEE Trans. Comput. C-21 (1972), 269–281.
- [16] *Carleson receives 2006 Abel Prize*. Notices Amer. Math. Soc. 53 (2006), 679–680.

5. Abelovu cenu za matematiku získal v roce 2007 Šrínivása Varadhan

Michal Křížek, Ivo Vrkoč

5.1 Prolog

Dne 22. května 2007 obdržel Abelovu cenu profesor Šrínivása S. R. Varadhan z Courantova ústavu matematických věd v New Yorku. V krátké historii Abelových cen, které se pravidelně udělují od roku 2003, je to již druhá cena, jež směřuje do tohoto ústavu. Připomeňme, že



ŠRÍNIVÁSA S. R. VARADHAN



Obr. 5.1 Vlevo Šrínivása S.R. Varadhan, vpravo norský král Harald V. (foto Terje Bendiksby/Scanpix)

v roce 2005 získal Abelovu cenu matematik maďarského původu Peter Lax, který pracoval v Courantově ústavu již od svých 25 let.

Podle vyjádření výběrové komise dostal Š. Varadhan Abelovu cenu *ze své fundamentální příspěvky k teorii pravděpodobnosti, zejména za vytvoření sjednocené teorie velkých odchylek.*

Komisi předsedal Kristian Seip. Abelovu cenu udělila Norská akademie věd a osobně ji předal norský král Harald V. (viz obr. 5.1). Slavnostnímu aktu v aule univerzity v Oslu byli přítomni Její Veličenstvo královna Sonja a norský ministr pro vzdělávání a výzkum Øystein Djupedal. Poté měl profesor Varadhan audienci v královském paláci, setkal se s mladými studenty matematiky, proslovil dvě odborné přednášky na univerzitách v Oslu a Trondheimu a zúčastnil se matematického cirkusu organizovaného pro děti.

5.2 Proslov prof. Varadhana při udělení Abelovy ceny

Vaše veličenstvo, vzácní členové Norské akademie věd, drazí přátelé.

Chci začít poděkováním norské vládě a lidem, kteří se zasloužili o zřízení Abelovy nadace, jež podporuje tuto cenu. Abel ve svém velice krátkém životě významně přispěl k „Matematice“ a já se cítím velice poctěn cenou, která byla zřízena na jeho památku.

Jen těžko mohu vyjádřit své emoce v tento den. Cítím se polichocen slovy, která zde o mně a o mé práci zazněla. Jsem skutečně potěšen, že jsem za tuto práci oceněn. Matematika je rozsáhlá disciplína, v níž pracuje mnoho vynikajících kolegů, kteří učinili fundamentální objevy ve svých oborech. Měl jsem štěstí, že komise letos ocenila teorii pravděpodobnosti a moje výsledky v ní.

Teorie pravděpodobnosti má dlouhou historii. I když různé hry opírající se o náhodu se hrají již tisíciletí, teprve nedávno se tento předmět stal součástí matematiky. Teorie pravděpodobnosti má dnes mnoho rolí. Jako součást matematiky je perspektivní a slouží také jako užitečný nástroj v ostatních oblastech čisté a aplikované matematiky. Stochastické modelování je důležitou součástí mnoha odvětví přírodních a sociálních věd. Žijeme ve světě plném nejistoty, a tak se stalo nezbytným tuto nejistotu modelovat, studovat a případně ji i řídit. Jsem skutečně velice šťasten, že teorie pravděpodobnosti získala letos uznání.

Na mém osobním i profesním formování se podílelo mnoho osobností. Můj otec byl učitelem a později ředitelem na střední škole. Vzdelání u nás doma mělo vždy vysokou prioritu a já jsem v tomto směru měl trvalou podporu obou rodičů.

Na střední škole jsem měl výborného profesora matematiky, který ve mně vzbudil pocit, že matematika může být i zábava jako ostatní hry. Moji učitelé v prezidentské koleji v Chennai mně poskytli solidní matematické vzdělání. Během studií v Indickém statistickém ústavu v Kalkatě mě školil Dr. C. R. Rao, který mě trvale podporoval. Můj zájem o matematiku tehdy výrazně vzrostl díky spolupráci s kolegy z ústavu. Zejména se o to zasloužil již zmíněný Ranga Rao a dále Varadarajan a Partasarathy.

Když jsem se v roce 1963 přestěhoval do New Yorku, Courantův ústav se podílel na množství aktivit v řadě oblastí. V analýze jsem hodně získal v diskusích s Moserem, Nirenbergem, Laxem, Johnem

a mnoha dalšími. Donsker, s nímž jsem po léta úzce spolupracoval, byl mým skvělým kolegou a věrným rádcem. Také Kac a McKean byli trvalými zdroji inspirace.

Vždy jsem si cenil úzké spolupráce s ostatními a hodně jsem se od nich naučil. Zejména bych rád zmínil některé z nich. Byli to má kolegové Stroock, Papanicolaou a H. T. Yau v různých obdobích a dále Kipnis, Olla a Landim, kteří dlouhodobě pobývali v našem ústavu. Během těch let jsem měl kolem třiceti studentů. Spolupráce s nimi byla velice povzbuzující a byli to oni, kdo přispěli a obohatili můj profesní život.

Newyorská univerzita a především Courantův ústav jsou báječné instituce v tom smyslu, že získávají studenty k vědeckému bádání a umožňují jim plný odborný růst.

Nakonec bych rád poděkoval své ženě Vasu za podporu, kterou mi poskytovala, a za porozumění, jehož se mi během let dostávalo. Jsem rád, že je zde s naším synem Ashokem, aby se mnou společně sdíleli radost. Lituji, že tu není Gopal¹ a že nemůže se mnou prožívat tento okamžik.

Na závěr bych rád poděkoval Norské akademii věd, Abelově nadaci a výběrové komisi za dnešní ocenění a přeji každému dobrý den.

5.3 Stručný životopis

Šrínivása S. R. Varadhan se narodil 2. ledna 1940 v Chennai (tj. Madrasu) na jihozápadním pobřeží Indie. Titul bakaláře získal na Presidency College v Chennai v roce 1959 a Ph.D. v Indickém statistickém ústavu v Kalkatě v roce 1963. Jeho školitelem byl světoznámý indický statistik C. R. Rao. Mladý Varadhan musel během obhajoby své doktorské dizertace čelit řadě zasvěcených dotazů od hosta pro něj do té doby neznámého. Později se ukázalo, že se jednalo o špičkového ruského matematika A. N. Kolmogorova.² Profesor Rao věděl, že přijede do Indie, a tak načasoval Varadhanovu obhajobu tak, aby mohl Kol-

¹Gopal je Varadhanův prvorozený syn, který tragicky zahynul 11. září 2001 při teroristickém útoku v New Yorku (srov. obr. 5.2).

²Andrej Nikolajevič Kolmogorov (1903–1987) v roce 1933 axiomatizoval teorii pravděpodobnosti. Zavedl pravděpodobnost jako pravděpodobnostní míru s hodnotami v intervalu $[0, 1]$ definovanou na σ -algebře a splňující jisté podmínky. Jeho standardní model (viz např. [12]) se dodnes používá. Opírá se o práce E. Borela (1871–1956) z teorie míry.



Obr. 5.2 Jméno Varadhanova syna Gopalakrishnana lze nalézt na Národním památníku World Trade Center v New Yorku (foto M. Křížek).

mogorovovi představit svého vynikajícího studenta. A nutno dodat, že Kolmogorov nebyl zklamán.

Š. Varadhan začal svoji akademickou kariéru v Courantově ústavu v New Yorku již jako postdoc (1963–1967). V letech 1966–1968 zde působil jako asistent a poté jako docent (angl. Associate Professor). V roce 1972 byl jmenován profesorem a ještě v téže roce odcestoval do švédského Mittag-Lefflerova ústavu na delší studijní pobyt. V období 1976–1977 přijal nabídku pracovat na Standfordské univerzitě. V letech 1980–1984 vystřídal ve funkci ředitele Courantova ústavu P. Laxe. Později (1991–1992) byl také zaměstnán v prestižním Ústavu pro pokročilá studia (Institute for Advanced Study) v Princetonu a po návratu se stal opět ředitelem Courantova ústavu (1992–1994).

I když je Varadhanova práce motivována problémy matematické fyziky a teorií parciálních diferenciálních rovnic, zabývá se především teorií pravděpodobnosti. Když Š. Varadhan nastoupil do Courantova ústavu, našel zde skvělé intelektuální zázemí. Měl štěstí, že se seznámil s D. W. Stroockem. Společně koncem šedesátých let napsali působivou sérii rozsáhlých vědeckých článků (viz např. [15], [16]), kterou v roce 1979 završili monografií *Multidimensional diffusion proces-*

ses [19], obsahující velké množství původních výsledků. Tato monografie brzy získala velký světový ohlas a byla opětovně publikována v letech 1997 a 2006.

V roce 1978 byl prof. Varadhan zvaným řečníkem na Mezinárodním matematickém kongresu a v roce 1994 zde měl plenární přednášku. Během svého plodného života získal řadu ocenění a uznání. Připomeňme například Birkhoffovu cenu (1994) a Steelovu cenu (1996). V roce 1988 byl zvolen do Americké akademie umění a věd, v témže roce do Třetí světové akademie věd, v r. 1995 do Národní akademie věd, v r. 1998 do Královské společnosti v Londýně a v roce 2004 do Indické akademie věd. Databáze Mathematical Reviews eviduje 135 recenzí na jeho práce. Stručná vědecká biografie Š. Varadhana je uveřejněna v článku [1].

5.4 Od teorie pravděpodobnosti k teorii velkých odchylek

Teorie pravděpodobnosti má dlouholetou historii. Její kořeny sahají až do 13. století, kdy úlohu o hodech třemi kostkami (viz [14, s. 57]) řešil Richard de Fournival v básni De vetula (O vědmě). V první polovině 17. století Fermat, Galileo, Huygens a Pascal vyšetřovali jednoduché úlohy na pravděpodobnost a zavedli pojem střední hodnoty. Zabývali se nejvíce matematickým řešením hazardních her, u kterých výhru, resp. prohru podmiňují náhodné jevy [17]. Zejména vyšetřovali hry, u nichž mají všichni hráči stejné matematické naděje na výhru a množina možných výsledků je konečná (např. při házení mincí a kostkou nebo různé karetní hry). Jako příklad uveďme jednu takovou úlohu z té doby, kterou lze nalézt v korespondenci Pierra Fermata s Blaisem Pascalem [18]:

Dva hráči A a B hrají několik her o určitou částku C. Tuto částku dostane hráč, který vyhraje jako první k her. Hry jsou přerušeny ve chvíli, kdy jednomu z hráčů chybí do vítězství l her, druhému m her. Jak bude částka C spravedlivě rozdělena?

Zvolme např. $l = 2$ a $m = 3$. V tomto případě bude $k \geq 3$ libovolné. Fermat si uvědomil, že stačí prověřit jen 16 níže uvedených možností:

aaaa, baaa, abaa, aaba, aaab, bbaa, abba, aabb, baba, abab, baab,
abbb, babb, bbab, bbba, bbbb,

kde a , resp. b znamená vítězství hráče A , resp. B . Odtud je již patrné, že částka C bude spravedlivě rozdělena v poměru $11 : 5$, neboť 11 možností na prvním řádku odpovídá výhře hráče A , zatímco zbývajících 5 možností na řádku druhém odpovídá výhře hráče B . Pro obecné l a m lze postupovat analogicky.

Teorie pravděpodobnosti se pak dále rozvíjela. Studoval se zejména problém, co se stane, když budeme nějaký experiment s náhodným výsledkem opakovat stále dokola. Jak bude vypadat příslušný limitní stav? Tak Jacob Bernoulli přišel koncem 17. století na *zákon velkých čísel*, který lze zhruba vyjádřit takto:

Jestliže se jev vedoucí k náhodnému jevu s pravděpodobností P opakuje n -krát, blíží se poměr počtu jevů skutečně vzniklých k úhrnnému počtu všech jevů tomuto číslu P tím více, čím větší je n .

Když vyhodíme minci do výšky, padne panna nebo orel. Pravděpodobnost obou jevů je zřejmě 50 %. Pokud vyhodíme minci například milionkrát, nepadne sice orel právě 500 000krát, ale relativní četnost tohoto náhodného jevu $p/10^6$, kde p udává počet, kolikrát padl orel, se bude jen velice málo lišit od pravděpodobnosti $\frac{1}{2}$.

A. N. Kolmogorov vyjádřil tento jev následující matematickou větou:

Věta (Zákon velkých čísel). *Nechť $X_1, X_2, \dots$ je posloupnost nezávislých stejně rozdělených náhodných veličin s konečnou střední hodnotou μ a konečným rozptylem.³ Pak*

$$P \left(\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n X_i = \mu \right) = 1.$$

Další důležitou roli při rozvoji teorie pravděpodobnosti sehrála také centrální limitní věta, kterou za jistých omezujících předpokladů používal v první polovině 18. století Abraham de Moivre, tj. mnohem dříve, než se Gauss narodil. I když de Moivre tuto větu nedokázal, její samotná formulace byla velice významná. Centrální limitní věta nám říká, že statistické vlastnosti, které závisejí na velkém množství nezávislých činitelů, mají rozdělení připomínající svým tvarem zvon.

³Poznamenejme, že se může stát, že střední hodnota náhodných veličin X_i vůbec nemusí existovat (např. pro Cauchyovo rozdělení). Pak je ale s pravděpodobností 1 posloupnost náhodných veličin $(X_1 + \dots + X_n)/n$ neohrazená [13].

Takové rozdělení se nazývá *Gaussovo* (nebo též *Gaussovo–Laplaceovo*) *normální rozdělení* a je charakterizováno jen dvěma parametry: střední hodnotou $\mu \in (-\infty, \infty)$ a rozptylem $\sigma^2 > 0$ (viz [14]),

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right), \quad x \in (-\infty, \infty).$$

Pokud si kupříkladu budete zakreslovat do diagramu, kolik vojáků má velikost 175 cm, kolik jich má velikost 176 cm atp., pak výsledný graf bude mít přibližně tvar jako funkce f pro vhodné parametry.

Obě výše zmíněné limitní věty (zákon velkých čísel i centrální limitní věta) jsou důležité v mnoha praktických situacích, kdy pracujeme s obrovským množstvím statistických dat. Například pojišťovací společnosti se příliš nezajímají o jednotlivá auta, ale spíše je zajímá, kolik nehod budou mít všechna jimi pojištěná auta za rok. Pokud budete stavět telefonní síť, pak vás nebudou zajímat jednotliví zákazníci, ale spíše pravděpodobnost, že příliš mnoho z nich bude současně telefonovat během večerní špičky nebo v případě nějaké katastrofy. Limitní věty nám umožňují takovéto úlohy řešit, ale nelze je použít k řešení problému tzv. *velkých odchylek*.

Abychom si přiblížili tento problém, vraťme se k úloze házení mince. Pokud ji vyhodíme jen stokrát, pak existuje velice malá pravděpodobnost, že padne alespoň 75 orlů a nejvýše 25 panen. Umění „velkých odchylek“ spočívá právě ve výpočtu pravděpodobnosti vzniku takových řídkých případů.

Velké odchylky byly prvně studovány významným švédským statistikem a pojišťovacím matematikem Haraldem Cramérem (1893–1985) kolem roku 1930. Snadno nahlédneme, že tento problém zajímá zejména matematiky pracující v pojišťovací matematice. Částka, kterou platíte za pojištění auta, se odvíjí od statistiky z předchozích let. Pojišťovací společnost totiž musí vybrat dostatečné množství peněz, aby mohla pokrýt nehody všech řidičů, kteří havarovali. Co ale dělat, pokud se v některém roce stane mnohem více nehod (v důsledku nějaké nepředvídatelné příčiny) než v předchozích letech? Má-li pojišťovna zaplatit více peněz, než vybrala, pak bude mít samozřejmě potíže.

Bohužel neexistuje žádná cesta, jak se tomuto problému zcela vyhnout. Pokud byste nasadili cenu za pojištění příliš vysokou, abyste

omezili důsledky velkých odchylek, pak si vaše pojištění nikdo nekoupí. Přitom taková velká odchylka nastane jen velmi zřídka. Pojišťovací společnost proto potřebuje spočítat pravděpodobnost velkých odchylek různých velikostí, aby našla rozumnou míru rizika. Proto se pojišťovací společnosti spojují a pojišťují se u zajišťoven. Podobně je třeba stavět telefonní sítě předimenzované, abychom se vyhnuli přetížení v důsledku zřídka se vyskytujících velkých odchylek. Zcela výjimečně se také stane, že Zemi zasáhne velký asteroid, že nestačí protipovodňové zábrany při pětisetleté vodě nebo že velká kasina jsou finančně zruinována, když padne například červená patnáctkrát za sebou.

5.5 Varadhanův princip velkých odchylek

Jeden z významných Varadhanových příspěvků k teorii pravděpodobnosti je použití techniky velkých odchylek jako silného a mnohostranného nástroje v mnoha oblastech matematicko-fyzikálních věd, které se od sebe zdánlivě velice liší (např. statistická fyzika, populační dynamika, ekonometrie, komunikační technologie). Tento výzkum prováděl Varadhan zejména se svým kolegou Monroem Donskerem. Dohromady publikovali přes 20 prací (viz např. [2]–[10]).

Mnoho fyzikálních teorií má statistickou povahu [9], protože nepopisují chování jednotlivých atomů či molekul, ale soustřeďují se na statistické chování všech částic v makroskopických veličinách, jako je tlak, teplota, tok apod. Ale i zde se občas mohou vyskytnout nepředvídatelné fluktuace, které pak vedou např. k tunelovému jevu či k lokálnímu snížení entropie.

Varadhanův princip velkých odchylek si objasníme na jednoduchém případu z článku [2]. Uvažujme Brownův pohyb startující v bodě x a okamžiku 0. Položme

$$L(t, \omega(\cdot), y) = \frac{1}{t} \lambda \{s; 0 \leq s \leq t, \omega(s) \leq y\},$$

kde λ je Lebesgueova míra na $\mathbb{R}^1$, $\omega(\cdot)$ je realizace Brownova pohybu. Hodnota $L(t, \omega(\cdot), y)$ tedy vyjadřuje relativní dobu, po kterou realizace $\omega(\cdot)$ bude menší nebo rovna y do okamžiku t . Dále nechť P_x je pravděpodobnost indukovaná tímto procesem. Problém vyšetřovaný Donskerem a Varadhanem je zaměřen na nalezení limit typu

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log E_x [\exp \{-t\Phi(L(t, \omega(\cdot), \cdot))\}],$$

kde E_x je střední hodnota odpovídající pravděpodobnosti P_x , Φ je funkcionál definovaný na množině distribučních funkcí na $\mathbb{R}^1$ a splňující jisté podmínky. Tato limita dává informaci o asymptotickém průběhu $L(t, \omega(\cdot), y)$. V tomto případě byla limita nalezena jako extrémní hodnota konkrétně daného výrazu. Výsledky jsou v článcích [2]–[7] zobecněny na markovské procesy s diskrétním i spojitým časem, na procesy, jejichž hodnoty jsou ve velmi obecných prostorech, a dále na limes superior a limes inferior výrazů

$$\frac{1}{t} \log Q_{x,t}(C) = \frac{1}{t} P_x\{\omega; S_t(\omega, \cdot) \in C\},$$

kde C je podmnožina pravděpodobnostních měr, L_t je definována vztahem

$$S_t(\omega, A) = \frac{1}{t} \lambda\{\sigma; \omega(\sigma) \in A, 0 \leq \sigma \leq t\}$$

a A je množina ze stavového prostoru markovského procesu. V případech těchto limit se výše uvedené výrazy a jejich zobecnění porovnávají s entropií vyšetřovaných procesů (blíže o tom v [6]).

Předložené výsledky mají důležité aplikace. Uveďme jen některé. Autoři rozřešili důležitý polaronový problém a také problém formulovaný Pekarem [7]. Oba tyto problémy mají význam ve statistické fyzice. Jmenujme ještě analýzu chování nábojů na kružnici, jejichž pohyb je dán složením deterministického vlivu s vlivem daným Brownovým pohybem (viz [10]).

5.6 Další Varadhanovy výsledky

V roce 1905 se Albert Einstein proslavil svou prací, v níž vysvětlil příčinu Brownova pohybu. V příslušných matematických modelech je tento pohyb popsán funkcí, která má nekonečnou variaci (což paradoxně odpovídá nekonečné rychlosti částic). V článcích [15] a [16] Stroock a Varadhan studují difuzní proces v $\mathbb{R}^d$, $d \in \{1, 2, \dots\}$, který je popsán evoluční parabolickou parciální diferenciální rovnicí

$$-\frac{\partial u}{\partial s}(s, x) = \frac{1}{2} \sum_{i,j=1}^d a_{ij}(s, x) \frac{\partial^2 u}{\partial x_i \partial x_j}(s, x) + \sum_{i=1}^d b_i(s, x) \frac{\partial u}{\partial x_i}(s, x), \quad (5.1)$$

kde koeficienty difuze a_{ij} jsou spojitě a omezeně funkce a koeficienty b_i jsou měřitelné.

Rovnice (5.1) má úzký vztah k markovským procesům.⁴ Takové procesy lze vyjádřit pomocí Itoovy rovnice (viz [11])

$$d\xi(t, \omega) = \sigma(t, \xi(t, \omega))dw(t, \omega) + b(t, \xi(t, \omega))dt, \quad (5.2)$$

kde $w(t, \omega)$ je Brownův pohyb, $\xi(t, \omega)$ je hledaný proces, $a(t, x) = \sigma(t, x)\sigma(t, x)^\top$ je tzv. matice difuzních koeficientů a_{ij} a $b(t, x)$ je tzv. vektorový drift (trend). Pokud koeficienty a, b jsou dostatečně regulární, pak existují jednoznačná řešení rovnic (5.1) i (5.2) za jistých dodatečných podmínek na řešení a $\xi(t)$ je markovským procesem. Označme $P(s, x, t, \Gamma)$ pravděpodobnost, že markovský proces ξ padne do množiny Γ v okamžiku t , jestliže v okamžiku s byl v bodě x . Funkce P proměnných s, x je řešením rovnice (5.1) s určitými koncovými podmínkami – v tomto kontextu nazvaná zpětnou Kolmogorovou rovnicí. Výsledky tohoto druhu se již považují za klasické, pokud koeficienty a, b jsou hölderovské. Důkazy obdobných tvrzení v případě méně regulárních koeficientů dlouho odolávaly. Tvrdým oříškem byla jednoznačnost řešení. Autoři však zvolili jinou cestu. Uvědomili si, že problém daný rovnicí (5.2) lze transformovat na hledání pravděpodobnostní míry P tak, aby procesy

$$X_\theta^s(t, x(\cdot)) = \exp \left\{ \langle \theta, x(t) - x(s) \rangle - \frac{1}{2} \int_s^t \langle \theta, a(u, x(u)) \theta \rangle du - \int_s^t \langle \theta, b(u, x(u)) \rangle du \right\},$$

kde $\langle \cdot, \cdot \rangle$ je skalární součin v $\mathbb{R}^d$, byly martingaly pro všechna $\theta \in \mathbb{R}^d$. Nalezená míra P se nazývá řešením martingalového problému. Poznamenejme, že proces $X(t)$ se nazývá *martingal* vůči pravděpodobnosti P a σ -algebřám $\mathcal{F}_s$, jestliže $E^P\{X(t_s)|\mathcal{F}_s\} = X(s)$ pro $t \geq s$, přičemž $E^P\{X(t_s)|\mathcal{F}\}$ je podmíněná střední hodnota vzhledem k σ -algebře $\mathcal{F}$. Martingaly hrají ústřední roli v teorii stochastických her. Pro své výhodné vlastnosti se používají v teorii markovských procesů apod.

Za předpokladů, že $a_{ij}(t, x)$ jsou spojitě a omezeně, matice $a(t, x)$ je pozitivně definitní v každém bodě, $b_i(t, x)$ jsou měřitelné a omezené, autoři dokázali existenci zobecněného řešení a jednoznačnost

⁴Andrej Andrejevič Markov (1856–1922) položil základy teorie náhodných procesů jako posloupností pokusů, když pravděpodobnost budoucích stavů závisí na přítomnosti, ale nezávisí na dříve provedených pokusech [12].

martingalového problému (viz [19]). Odtud plyne i jednoznačnost ve smyslu semigrup. Navíc přechodová funkce $P(s, x, t, \Gamma)$ daná martingalovým problémem je ekvivalentní s odpovídající funkcí danou rovnicí (5.2).

L i t e r a t u r a

- [1] ATHREYA, K. B.: *Professor Srinivasa R. S. Varadhan*. Curr. Sci. 78 (2000), 1151–1152.
- [2] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotic evaluation of certain Markov process expectations for large time, I*. Commun. Pure Appl. Math. 28 (1975), 1–47.
- [3] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotic evaluation of certain Markov process expectations for large time, II*. Commun. Pure Appl. Math. 28 (1975), 279–301.
- [4] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotics for the Wiener Sausage*. Commun. Pure Appl. Math. 28 (1975), 525–565.
- [5] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotic evaluation of certain Markov process expectations for large time, III*. Commun. Pure Appl. Math. 29 (1976), 389–461.
- [6] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotic evaluation of certain Markov process expectations for large time, IV*. Commun. Pure Appl. Math. 36 (1983), 183–219.
- [7] DONSKER, M. D., VARADHAN, S. R. S.: *Asymptotics for the Polaron*. Commun. Pure Appl. Math. 36 (1983), 505–528.
- [8] DONSKER, M. D., VARADHAN, S. R. S.: *Large deviations for stationary Gaussian processes*. Commun. Math. Phys. 97 (1985), 187–210.
- [9] DONSKER, M. D., VARADHAN, S. R. S.: *Large deviations for noninteracting infinite-particle systems*. J. Stat. Phys. 46 (1987), 1195–1232.
- [10] DONSKER, M. D., VARADHAN, S. R. S.: *Large deviations from hydrodynamic scaling limit*. Commun. Pure Appl. Math. 42 (1989), 243–270.

- [11] ITO, K.: *On stochastic differential equations*. Mem. Amer. Math. Soc. 4 (1951), 51.
- [12] NAVARA, M.: *Pravděpodobnost a matematická statistika*. Skripta FEL ČVUT, Praha 2007.
- [13] REKTORYS, K., a kol.: *Přehled užité matematiky II*. Prometheus, Praha 1995.
- [14] RIEČAN, B., LAMOŠ, F., LENÁRT, C.: *Pravdepodobnosť a matematická štatistika*. Alfa, SVTL, Bratislava 1984.
- [15] STROOCK, D. W., VARADHAN, S. R. S.: *Diffusion processes with continuous coefficients, Part I*. Commun. Pure Appl. Math. 22 (1969), 345–400.
- [16] STROOCK, D. W., VARADHAN, S. R. S.: *Diffusion processes with continuous coefficients, Part II*. Commun. Pure Appl. Math. 22 (1969), 479–530.
- [17] ŠOFR, B.: *Populárne o počte pravdepodobnosti*. SVTL, Bratislava 1967.
- [18] ŠOLCOVÁ, A.: *Fermatův odkaz*. Cahiers du CEFRES 28 (2002), 173–202.
- [19] VARADHAN, S. R. S., STROOCK, D. W.: *Multidimensional diffusion processes*. Springer, New York 1979, 1997, 2006.

6. Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup

Michal Krížek, Lawrence Somer

6.1 Prolog

Abelovu cenu za matematiku získali v roce 2008 John Griggs Thompson z USA a Jacques Tits z Francie. Cenu jim udělila Norská akademie věd a předal ji osobně norský král Harald V. dne 20. května 2008 v hlavní aule univerzity v Oslu. Abelova cena byla tentokrát spojena s částkou 1 200 000 USD. Podle vyjádření prof. Kristiana Seipa, předsedy výběrové komise, cenu dostali za *své podstatné výsledky v algebře*



JOHN GRIGGS THOMPSON



JACQUES TITS

a hlavně za zformování moderní teorie grup. Ve středu 21. května oba laureáti přednesli své abelovské přednášky na univerzitě v Oslu.

6.2 Stručné životopisy obou laureátů

John Griggs Thompson působí od r. 1993 jako Graduate Research Professor na Floridské univerzitě a je emeritním profesorem na Cambridgeské univerzitě v Anglii. Narodil se 13. října 1932 v Kansasu. Na slavné Yaleově univerzitě začal studovat teologii. Po roce však přešel na matematiku a udělal dobře. Saunders MacLane jej totiž pozval, aby si udělal doktorát na univerzitě v Chicagu. Zde se začal intenzivně věnovat konečným grupám symetrií a v roce 1959 získal titul Ph.D. Poté rok pracoval v Institutu pro obranné analýzy (Institute for Defense Analyses) a poté dva roky na Harvardově univerzitě. Pak se vrátil do Chicaga a v období 1962–1968 zde působil již jako profesor. V roce 1970, kdy ještě nedosáhl ani 40 let, byla Thompsonova práce oceněna Fieldsovou medailí. V letech 1970–1993 pak působil na Cambridgeské univerzitě. Získal 4 čestné doktoráty, Wolfovu cenu, Coleovu cenu, Sylvesterovu medaili, Poincarého medaili aj.

Jaques Tits je emeritním profesorem na Collège de France, ale je původem z Belgie. Narodil se 12. srpna 1930 v Uccle na předměstí Bruselu. Byl považován za zázračné dítě. Už jako tříletý uměl počítat a později mu bylo umožněno přeskočit několik tříd školní docházky. Ve svých čtrnácti letech tak úspěšně vykonal přijímací zkoušky na Vrije Universiteit Brussel. V roce 1950, když mu bylo pouhých 19 let, získal titul Ph.D. Působil na řadě univerzit, např. v Bruselu, Bonnu a Paříži. Získal 4 čestné doktoráty a celou řadu dalších ocenění (např. Wolfovu cenu). Je členem mnoha akademií a čestným členem Londýnské matematické společnosti.

6.3 Stručně o teorii grup

Připomeňme si nejprve některé základní pojmy. *Grupa* G je množina, na které je definována asociativní binární operace $\circ : G \times G \rightarrow G$ s neutrálním prvkem e a v níž ke každému prvku $g \in G$ existuje právě jeden prvek inverzní $g^{-1} \in G$ tak, že $g \circ g^{-1} = g^{-1} \circ g = e$. Prvkům G se někdy říká *symetrie*, pokud jsou to zobrazení geometrických objektů na sebe.



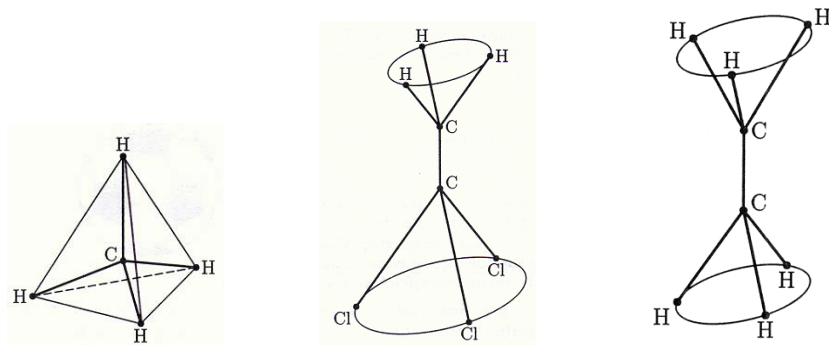
Obr. 6.1 Mozaika v paláci Alhambra v Granadě je příkladem tapetové grupy. Nejmenší úhel otočení zachovávající mozaiku je 90° . Odpovídající středy otáčení leží na průsečících vodorovných a svislých os souměrnosti (foto H. Bílková).

Studium symetrií má dlouhou historii. Jeho kořeny sahají až do antiky. Například staré egyptské a maurské ornamenty (viz obr. 6.1) vykazují symetrie všech 17 tapetových grup (tj. dvojrozměrných krystalografických grup, jejichž existenci udává Fjodorovův teorém). Lidé se totiž odjakživa obdivují a dávají přednost objektům, které vykazují nějaký druh symetrie. Například staří Řekové se zabývali platónskými a archimédovskými tělesy, jejichž symetrie také tvoří grupy, jak se později zjistilo.

Grupu všech permutací prvků $1, 2, \dots, n$ (s operací skládání) nazveme *symetrickou* a označíme ji S_n . Grupu všech sudých permutací prvků $1, 2, \dots, n$ nazveme *alternující*¹ a označíme ji A_n .

Pojem grupa pochází až od Evarista Galoise, který je všeobecně považován za jednoho ze zakladatelů teorie grup. Kolem roku 1830 odvodil z vlastností symetrických grup S_n , že algebraické rovnice

¹Někdy se jí též říká alternativní grupa. Každou permutaci lze složit z transpozic, které prohazují právě 2 prvky a ostatní prvky ponechávají na místě. Permutace se nazývá *sudá*, resp. *lichá*, je-li počet transpozic sudý, resp. lichý [27, s. 85].



Obr. 6.2 Symetrie molekuly metanu CH_4 tvoří grupu o $4! = 24$ prvcích, která je izomorfní² symetrické grupě S_4 . Grupa tzv. přímých symetrií, kdy neuvažujeme zrcadlové obrazy molekuly, má jen 12 prvků a je izomorfní s alternující grupou A_4 . Symetrie prostřední molekuly trichloroetanu $\text{H}_3\text{C}-\text{CCl}_3$ tvoří cyklickou grupu C_3 o třech prvcích. Dihedrál ní grupa D_3 se skládá ze šesti přímých symetrií molekuly etanu C_2H_6 (nakreslil P. Křížek).

stupně vyššího než 4 nejsou obecně řešitelné pomocí odmocnin. Přitom pro řešení tohoto obtížného problému podstatně využil vlastností symetrie mezi jednotlivými kořeny. Niels Henrik Abel dokázal již dříve podobný výsledek pro algebraické rovnice pátého stupně na pouhých šesti stránkách (viz [1], [24]). První knihu o teorii grup publikoval v roce 1870 Camille Jordan. Nazval ji *Traité des substitutions* (viz [12]).

Teorie grup má obrovské množství nejrůznějších praktických aplikací, např. při klasifikaci krystalů, uzlů, symetrií molekul (viz obr. 6.2), popisu silných, slabých a elektromagnetických interakcí, skládání Lorentzových transformací, v teorii kódování³ (viz [17], [20], [21], [27]). Díky symetriím se značně zjednodušují některé výpočty. S grupami se setkáváme i při řešení různých hlavolamů (viz např. obr. 6.3).

²Izomorfismus je vzájemně jednoznačné zobrazení, které zachovává binární grupovou operaci.

³Například německá armáda používala elektromechanický šifrovací stroj Enigma. Jeho kód v roce 1932 rozšifrovali pomocí teorie grup M. Rejewski, J. Rozycki a H. Zygalski, pracující pro polskou tajnou službu. Koncem 2. světové války pak zdokonalený kód rozšifroval Alan Turing, což pomohlo zkrátit válku, a ušetřit tak mnoho lidských životů.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

R	A	T	E
Y	O	U	R
m	i	n	d
p	l	a	

Obr. 6.3 Známa hra *patnáctka* (vlevo) neumožňuje prohodit čísla 15 a 14 v posledním řádku tak, aby poloha ostatních čísel zůstala zachována. Plyne to z vlastností alternujících grup (viz [27, s. 39 a 97]). Na druhé straně l a a v posledním řádku (vpravo) prohodit lze. Víte proč?

6.4 Konečné grupy

Dále se budeme zabývat jen konečnými grupami (slovo **konečný** budeme proto většinou vynechávat). Počet prvků G označíme $|G|$ a nazveme *řádem grupy*⁴. *Podgrupa* $H \subset G$ je podmnožina G se stejnou operací $\circ$ zúženou na $H \times H$, s tímž neutrálním prvkem e , jako má G , a splňující axiomy grupy. Nazývá se *vlastní*, je-li $H \neq G$, a *triviální*, je-li $H = \{e\}$.

Věta (Cayleyova). *Každá grupa řádu n je izomorfní nějaké podgrupě symetrické grupy S_n .*

Poznamenejme, že pro $n \geq 3$ není grupa S_n komutativní (tj. je neabelovská).

Věta (Lagrangeova). *Je-li H podgrupa G , pak $|H|$ dělí $|G|$.*

Jako bezprostřední důsledek dostáváme, že $g^{|G|} = e$ pro každé $g \in G$ (viz [18, s. 131]).

Francouzský matematik Augustin-Louis Cauchy dokázal, že pro každé prvočíslo p , které dělí $|G|$, existuje podgrupa $H \subset G$ taková, že $|H| = p$. Toto tvrzení bylo kolem roku 1872 rozšířeno norským matematikem Ludwigem Sylowem:

Věta (Sylowova). *Je-li p prvočíslo a p^k dělí $|G|$ pro nějaké $k \geq 0$ celé, pak existuje podgrupa $H \subset G$ řádu p^k .*

⁴Počet vzájemně neizomorfních grup řádu n se uvádí ve Sloanově On-line encyclopedia of integer sequences v úplně první položce A000001. Například existuje 267 grup řádu 64, ale jen jedna grupa řádu 65, viz <http://www.research.att.com/~njas/sequences/>

Alternující grupa A_5 je neabelovská grupa všech sudých permutací z pěti prvků. Podle Sylowovy věty má podgrupy řádu 2, 3, 4 a 5, protože $|A_5| = 5!/2 = 60 = 2^2 \cdot 3 \cdot 5$. Nemá ale podgrupy řádu 15 ani 30 (tj. Lagrangeovu větu nelze obrátit). Poznamenejme ještě, že A_5 je izomorfní s grupou všech přímých symetrií pravidelného dvanáctistěnu,⁵ pravidelného dvacetistěnu a též molekuly fullerenu C_{60} , připomínající klasický fotbalový míč.

6.5 Klasifikace jednoduchých grup

Pro jednoduchost budeme symbol binární operace $\circ$ nadále vynechávat. Podgrupa $H \subset G$ se nazývá *normální*, jestliže $g^{-1}hg \in H$ pro všechna $h \in H$ a $g \in G$. V tomto případě budeme psát $H \triangleleft G$, pokud $H \neq G$.

Například $\{e\} \triangleleft A_3 \triangleleft S_3$, protože alternující grupa A_n je normální podgrupou symetrické grupy S_n pro každé $n = 1, 2, \dots$. Také grupa tahů Rubikovy kostky $3 \times 3 \times 3$ obsahuje normální podgrupu, která se skládá z operací pouze na 8 vrcholových kostičkách (viz [22, s. 49, 135], [27]). Na druhé straně podgrupa A_5 grupy A_6 není normální (jak bude patrné z Galoisovy věty).

Definice. Grupa G se nazývá *jednoduchá*, jestliže $\{e\}$ a G jsou její jediné normální podgrupy.

Protože všechny cyklické grupy⁶ C_n jsou abelovské a všechny podgrupy abelovské grupy jsou normální, jednoduché cyklické grupy mají prvočíselný řád nebo řád 1. Cyklické grupy s neprvočíselným řádem nejsou jednoduché, kromě případu C_1 . Rovněž dihedrální grupa D_n přímých symetrií pravidelného n -bokého hranolu není jednoduchá pro $n > 2$.

Pojem jednoduchá grupa také pochází od Galoise, který takto nazval grupy sudých permutací A_n pro $n \geq 5$.

Věta (Galoisova). Alternující grupa A_n je jednoduchá pro $n \geq 5$.

Důkaz je uveden např. v [13, s. 98], [18, s. 542]. Jak již bylo řečeno v kapitole 6.3, grupa A_5 má několik vlastních netriviálních podgrup.

⁵Grupa všech přímých symetrií krychle je S_4 .

⁶Cyklická grupa je grupa generovaná jediným prvkem.

Žádná z nich ale není normální. Pro ilustraci ukážeme, že A_3 není normální podgrupou A_5 , i když $A_3 \triangleleft A_4$. Zřejmě

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

je sudá permutace a grupa $H = \{e, h, h^{-1}\}$ je izomorfní s $A_3 \cong C_3$. Protože

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

je také sudá permutace, platí $g \in G = A_5$. Odtud vyplývá, že

$$\begin{aligned} g^{-1}hg &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} hg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} g = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \end{aligned}$$

není prvkem podgrupy H .

Podobně pro

$$h' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

a stejné g lze zjistit, že A_4 není normální podgrupou A_5 .

Jednoduché grupy tvoří jakési stavební kameny všech grup, podobně jako prvočísla jsou stavebními kameny přirozených čísel větších než jedna. Jestliže G_2 je maximální vlastní normální podgrupa grupy G_1 , pak podílová grupa $G_1/G_2 = \{gG_2; g \in G_1\}$ je jednoduchá. Je-li podobně G_3 maximální vlastní normální podgrupa G_2 , pak G_2/G_3 je také jednoduchá. Tímto způsobem můžeme pokračovat, až dojdeme k $G_{n+1} = \{e\}$. Grupu G lze takto vyjádřit pomocí n jednoduchých grup $G_1/G_2, G_2/G_3, \dots, G_n/G_{n+1}$ a podle Jordanovy–Hölderovy věty z roku 1889 tyto grupy nezávisí na výše uvedené volbě pořadí normálních podgrup (viz [11, s. 249], [13], [16, s. 112]):

Věta (Jordanova–Hölderova). *Nechť grupu G lze rozložit dvěma způsoby ve tvaru $\{e\} = G_{n+1} \triangleleft \dots \triangleleft G_2 \triangleleft G_1 = G$ a $\{e\} = H_{m+1} \triangleleft$*

$\cdots \triangleleft H_2 \triangleleft H_1 = G$ tak, že každá grupa v obou řetězcích je maximální vlastní normální podgrupou grupy následující. Pak $n = m$ a existuje permutace⁷ π prvků $1, \dots, n+1$ taková, že G_i/G_{i+1} je izomorfní $H_{\pi(i)}/H_{\pi(i+1)}$ pro $i = 1, \dots, n$.

Mnoho problémů z teorie grup tak lze pomocí indukce převést na úlohy zahrnující jednoduché grupy. Nejmenší jednoduchá nekomutativní grupa je A_5 . Její řád je $|A_5| = 60$. Grupy A_1 a A_2 jsou triviální, grupa A_3 je komutativní a izomorfní cyklické grupě C_3 a grupa A_4 je sice nekomutativní, ale může být rozložena na dvě abelovské podílové grupy (viz [11, s. 244]). Galois pracoval s grupou S_5 permutací kořenů rovnice pátého stupně, která obsahuje jednoduchou podgrupu A_5 , a nemůže být tedy dále rozložena na cyklické grupy prvočíselných řádů.

V roce 1892 si Otto Hölder položil otázku, zda je možno vytvořit přehledný seznam všech konečných jednoduchých grup (viz [23]). V současnosti již víme, že každá jednoduchá grupa patří do jedné z 18 nekonečných (ale spočetných) tříd konečných grup nebo do zvláštní konečné třídy tzv. *sporadických grup*, které nepatří do žádné z těchto 18 nekonečných tříd a kterých je právě 26 (viz tab. 6.1). Budeme se jim věnovat v kapitole 6.5.

Klasifikační věta. *Je-li G jednoduchá grupa, pak patří do právě jedné z následujících skupin:*

- 1) třídy cyklických grup C_p prvočíselného řádu p a řádu 1,
- 2) třídy alternujících grup A_n pro $n \geq 5$,
- 3) 16 nekonečných tříd Lieova typu⁸ nad konečnými tělesy,⁹
- 4) třídy 26 sporadických grup.

Celková délka důkazu této věty se odhaduje na 15 000 stránek. Klasifikační věta je totiž založena na pěti stech člancích od přibližně

⁷Zřejmě $\pi(1) = 1$ a $\pi(n+1) = n+1$.

⁸Lieovy grupy popisují různé typy geometrií, viz např. [14], [17], [21]. Jako konkrétní příklad uveďme grupy symetrií vícerozměrných krychlí [10]. Šestnáct tříd grup Lieova typu lze rozdělit takto: 4 z nich jsou klasické maticové grupy nad konečnými tělesy, tj. lineární, unitární, symplektické a ortogonální grupy. Dále existuje 5 nekonečných tříd Chevalleyových grup, 4 třídy Steinbergových grup, 1 třída Suzukiho grup a 2 třídy Reeových grup.

⁹Poznamenejme, že jedna grupa z tříd Reeových grup typu F_4 nad dvouprvkovým tělesem se nazývá *Titsova grupa*.

Angl. jméno	Označení	Řád
Mathieu	M_{11}	$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$
	M_{12}	$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$
	M_{22}	$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
	M_{23}	$10200960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
	M_{24}	$244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
Janko	J_1	$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
	J_2	$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
	J_3	$50232960 = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
	J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Higman–Sims	HS	$44352000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McLaughlin	Mc	$898128000 = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Held	He	$4030387200 = 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Suzuki	Sz	$448345497600 = 2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Rudvalis	Ru	$145926144000 = 2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
O’Nan	ON	$460815505920 = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Lyons	Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Conway	Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
	Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
	Co_3	$495766656000 = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fischer	Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
	Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
	Fi_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
Harada–Norton	HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Thompson	Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
Baby Monster	B	$ B \approx 4 \cdot 10^{34}$, viz (6.3)
Monster	M	$ M \approx 8 \cdot 10^{54}$, viz (6.1)

Tab. 6.1 Sporadické grupy

100 autorů, v nichž se podrobně vyšetřují jednotlivé třídy a jejich speciální případy. Samozřejmě vzniká otázka, zda je takto dlouhý důkaz bezchybný. O jedné mezeře v důkazu, kterou se již podařilo zaplnit, pojednává článek [2].

Daniel Gorenstein (zemřel v r. 1992) inicioval projekt, který by důkaz Klasifikační věty zkrátil a dal jej do jednotného stylu. Projektu se ujali Richard Lyons a Ronald Solomon, kteří postupně jednotlivé části důkazu Klasifikační věty zasílají k publikaci do časopisu Ame-

rické matematické společnosti. Celý důkaz bude systematicky podán v mnoha dílech, z nichž 6 již bylo vydáno. Odhaduje se, že počet stránek tentokrát nepřesáhne 4000.

Díky Jordanově–Hölderově větě a dalším hlubokým výsledkům se podařilo ukončit klasifikaci jednoduchých grup kolem roku 1982. John H. Conway¹⁰ inicioval projekt „Atlas“, popisující všechny konečné grupy, který je zveřejněn v [6]. Obsáhlý historický přehled o tomto vysoce netriviálním výsledku je podán např. v [9] a [22].

Georg Frobenius v roce 1893 ukázal, že každá jednoduchá grupa, jejíž řád neobsahuje čtverec prvočísla, musí být cyklická a prvočíselného řádu nebo řádu 1 (viz [23]). V roce 1904 William Burnside dokázal velmi překvapivou větu (viz [3], [9], [22, s. 85]):

Věta (Burnsidova). *Žádná jednoduchá grupa nemá řád $p^k q^m$, kde p a q jsou různá prvočísla a $k, m \geq 1$ celá.*

Pokud tedy jednoduchá grupa není cyklická, musí být její řád dělitelný alespoň třemi prvočísly. Například řád grup A_5 , A_6 a některých jednoduchých grup Lieova typu je dělitelný právě třemi různými prvočísly (druhá nejmenší jednoduchá neabelovská grupa má řád $168 = 2^3 \cdot 3 \cdot 7$). Burnside též dokázal, že každá grupa řádu p^2 je abelovská, je-li p prvočíslo (viz [18, s. 531]). Grupa řádu p^3 ale může být neabelovská, je-li p liché prvočíslo. Například existují dvě neabelovské grupy řádu $3^3 = 27$.

6.6 Sporadické grupy

Největší sporadická grupa se nazývá *Monstrum* a označuje se M . Jde o zcela výjimečný matematický objekt, viz [15]. Jeho existenci předpověděli v roce 1973 na sobě nezávisle Bernd Fischer a Robert L. Griess. Proto se M někdy také nazývá Fischerovo–Griessovo monstrum. Griess z univerzity v Michiganu je pak v roce 1983 zkonstruoval jako konečnou grupu rotací v eukleidovském prostoru $\mathbb{R}^{196883}$. Řád M je vskutku úctyhodný,

$$\begin{aligned} |M| &= 808017424794512875886459904961710757005754368000000000 \\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71. \end{aligned} \quad (6.1)$$

¹⁰Conway je také autorem známého algoritmu Life, který simuluje evoluci bakterií ve čtvercové síti.

Cesta ke konstrukci Monstra však byla značně dlouhá a klikatá. První sporadické grupy M_n pro $n = 11, 12, 22, 23, 24$ objevil francouzský matematik Émile L. Mathieu v období 1861–1873. Jsou to zvláštní podgrupy grupy všech permutací S_n , které nepatří do žádné z 18 nekonečných tříd jednoduchých grup. Grupa M_{24} byla objevena jako první v roce 1861.

Nejsnáze zkonstruovatelná sporadická grupa je však M_{12} . Její řád

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040 \quad (6.2)$$

je sice větší¹¹ než $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7920$, lze ji však definovat pomocí pouhých tří generátorů g_1, g_2, g_3 . Do M_{12} patří všechny permutace, které lze dostat složením konečně mnoha následujících permutací (viz [27, s. 166]):

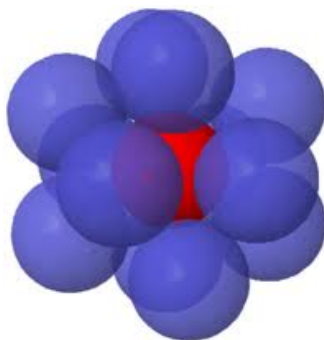
$$\begin{aligned} g_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 12 \end{pmatrix}, \\ g_2 &= \begin{pmatrix} 1 & 12 & 2 & 11 & 3 & 6 & 4 & 8 & 5 & 9 & 7 & 10 \\ 12 & 1 & 11 & 2 & 6 & 3 & 8 & 4 & 9 & 5 & 10 & 7 \end{pmatrix}, \\ g_3 &= \begin{pmatrix} 1 & 2 & 3 & 7 & 11 & 8 & 9 & 10 & 5 & 6 & 4 & 12 \\ 1 & 2 & 7 & 11 & 8 & 3 & 9 & 5 & 6 & 4 & 10 & 12 \end{pmatrix}. \end{aligned}$$

Lze dokázat, že M_{12} neobsahuje žádnou transpozici ani trojcyklus. Tato grupa je ale 5-tranzitivní,¹² tj. pro libovolných pět různých prvků i_1, i_2, i_3, i_4, i_5 a dalších pět libovolných různých prvků j_1, j_2, j_3, j_4, j_5 z množiny $\{1, 2, \dots, 12\}$ existuje permutace $s \in M_{12}$ taková, že $s(i_k) = j_k$ pro $k = 1, 2, 3, 4, 5$. Všimněte si také, že řád M_{12} ve vztahu (6.2) je roven právě počtu možností, jak vybrat 5 prvků z dvanácti, pokud záleží na pořadí.

Termín sporadická grupa se poprvé objevil v práci [4, s. 504] z roku 1911, kde se o Mathieuových grupách píše: *Tyto očividně sporadické jednoduché grupy by si patrně zasloužily podrobnější studium, než jim dosud bylo věnováno*. Podle Burnsidovy věty musí být řád každé sporadické grupy číslo složené z vícera prvočinitelů (srov. tab. 6.1).

¹¹Grupa M_{11} je stabilizátorem grupy M_{12} , podrobnosti viz [27, s. 168–170].

¹²Každá 6-tranzitivní grupa je už buď symetrická, nebo alternující (viz [27]).

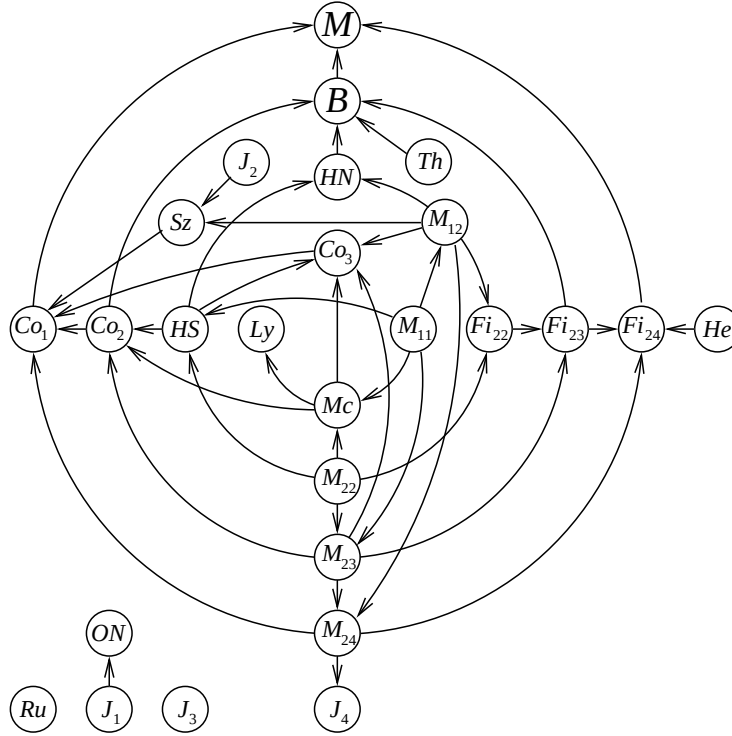


Obr. 6.4 Dvanáct koulí obklopujících centrální kouli v třírozměrném prostoru (zdroj Wikipedia).

V roce 1965, tj. přibližně sto let po objevu prvních pěti sporadických grup M_i , objevil chorvatský matematik Zvonimír Janko šestou sporadickou grupu, označovanou jako J_1 . Existence dalších sporadických grup byla často předpovězena dříve, než byla příslušná grupa zkonstruována. Většina sporadických grup se tak nazývá po autorech, kteří jejich existenci pouze předpověděli. Jde přibližně o období 1965–1975.

Několik sporadických grup bylo zkonstruováno pomocí tzv. Leechovy mřížky (viz [25]). Při nejhustším uspořádání stejně velkých kruhů v rovině se každý kruh dotýká svých šesti sousedů. Pro pravidelná periodická uspořádání stejně velkých koulí v d -rozměrném prostoru označme maximální počet dotyků vybrané centrální koule se sousedními koulemi symbolem $K(d)$ (angl. kissing number). Pak $K(1) = 2$, $K(2) = 6$, $K(3) = 12$ (viz obr. 6.4), $K(4) = 24$ a $K(8) = 240$. Pro ostatní d jsou známy jen hrubé dolní a horní odhady $K(d)$, kromě případu $d = 24$, kdy je horní odhad roven dolnímu, tj. $K(24) = 196560$ (viz [19], [22, s. 242]).

V 60. letech minulého století se John Leech inspiroval 5-tranzitivní Mathieuovou grupou M_{24} , v níž se permutuje 24 prvků tak, že libovolných pět různých z nich se současně zamění za obecně jiných pět různých prvků předem daných. V eukleidovském prostoru $\mathbb{R}^{24}$ zkonstruoval speciální pravidelnou mřížku středů koulí, které dávají nejhustší uspořádání, kdy je centrální koule obklopena právě 196560 dotýkajícími se koulemi. Symetrie Leechovy mřížky v $\mathbb{R}^{24}$ umožňují zkonstruo-



Obr. 6.5 Orientovaný graf ukazuje vztahy mezi všemi 26 sporadickými grupami (šipka $H \rightarrow G$ označuje, že H je vlastní podgrupa G). Lyonsova grupa Ly a Jankova grupa J_4 nejsou podle Lagrangeovy věty podgrupy Monstra, protože jejich řád je dělitelný 37, viz tab. 6.1 a vztah (6.1) (nakreslil P. Křížek).

vat celkem 12 sporadických grup.¹³ Některé z nich našly uplatnění v teorii samoopravných kódů (viz [25]), v teorii strun a supergravitace (viz [10]).

Připomeňme ještě jednu zajímavou vlastnost čísla 24:

$$1^2 + 2^2 + 3^2 + \cdots + 22^2 + 23^2 + 24^2 = 70^2,$$

tj. součet čtverců po sobě jdoucích čísel od 1 do 24 je roven čtverci. Číslo 24 je jediné přirozené číslo větší než 1, které má takovou vlastnost.

¹³Jsou to J_2 , HS , Mc , Sz a dále všechny Mathieuovy a Conwayovy grupy (viz [7], [22, s. 155]).

Druhá největší sporadická grupa B se anglicky nazývá Baby Monster. Má rovněž úctyhodný řád:

$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47. \quad (6.3)$$

Objevil ji B. Fischer v roce 1974.

Z 26 sporadických grup lze vyčlenit 20 grup, z nichž každá je buď vlastní podgrupou Monstra M , nebo podílovou grupou jeho podgrup. K této skupině se navíc přiřazují ještě dvě grupy Ly a J_4 , které obsahují některé netriviální podgrupy Monstra (viz obr. 6.5). Těmto 22 sporadickým grupám se říká *Šťastná rodinka* (angl. Happy Family). Skupina zbývajících čtyř sporadických grup Ru , ON , J_1 a J_3 nese přílehavý název *Vyvrhelové* (angl. Pariahs).

6.7 Thompsonův a Titsův přínos k teorii neabelovských grup

Oba noví laureáti Abelovy ceny se podstatně zasloužili o některé části důkazu Klasifikační věty jednoduchých grup. Již v roce 1963 Walter Feit a John G. Thompson publikovali článek [8], který na 255 stránkách přináší důkaz tehdy 60 let staré Burnsidovy domněnky pro jednoduché neabelovské grupy:

Věta (Feitova–Thompsonova). *Každá jednoduchá neabelovská grupa má sudý řád.*

Na druhé straně jediné jednoduché abelovské grupy jsou C_p , kde p je prvočíslo nebo $p = 1$, tj. řád jednoduché grupy C_p je lichý, když $p \neq 2$. Každá grupa G s lichým neprvočíselným řádem má netriviální normální podgrupu a podle Jordanovy–Hölderovy věty může být rozložena pouze na cyklické podílové (a tedy abelovské) grupy [22, s. 114]. Jako netriviální důsledek Feitovy–Thompsonovy věty tak dostáváme (viz [8]):

Věta. *Každou grupu lichého řádu alespoň 3 lze rozložit na jednoduché abelovské grupy prvočíselného řádu.*

Thompson dále zkonstruoval sporadickou grupu označovanou Th , jejíž řád činí $|Th| \approx 9 \cdot 10^{16}$ (viz tab. 6.1 a obr. 6.5). Pomohl také svému mladšímu kolegovi J. H. Conwayovi při konstrukci sporadické grupy Co_1 a vypočítal řád některých dalších grup (viz

např. [22, s. 153, 184]). Thompson objevil i dvě nové nekonečné grupy označované T a V . Databáze MathSciNet eviduje přes 250 Thompsonových prací především z teorie grup.

Jacques Tits se již od mládí zajímal o Lieovy grupy s konečným řádem. Objevil nové nekonečné třídy takových grup současně (ale nezávisle) s Robertem Steinbergem z Kalifornie. Studoval také grupy symetrií krystalů a pravidelných těles ve vícerozměrných prostorech.¹⁴ Titsova grupa, kterou objevil, má řád $17971200 = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$ a patří ke grupám Lieova typu.

Jacques Tits (a nezávisle též Marshall Hall) explicitně zkonstruoval Jankovu grupu J_2 , což je speciální sporadická grupa permutací 100 symbolů (viz tab. 6.1). Přitom použil čistě geometrické úvahy. Tits je autorem známé monografie [26]. Také poněkud zjednodušil Griessovu konstrukci Monstra (viz [22, s. 209]). Další zjednodušení se popisuje v článku [5].

Podle prohlášení výběrové komise *Thompson způsobil převrat v teorii konečných grup tím, že dokázal nesmírně obtížné věty, které vedly k položení základů pro úplnou klasifikaci konečných grup, jednoho z největších výsledků matematiky 20. století.*

Tits vytvořil nový a velmi účelný pohled na grupy jako geometrické objekty. Zavedl matematický objekt, který je znám jako Titsova konstrukce (angl. Tits building), jež vyjadřuje algebraickou strukturu lineárních grup v geometrických termínech.

Poznámka. Pokud vám v hlavě stále vrtá paradox z obr. 6.3 vpravo, pak vám napovíme, že je třeba zaměnit dvě nerozlišitelná R v prvním a druhém řádku, což vyžaduje sudý počet tahů. Lze to dokázat takto: Nejprve obarvíme všech 16 čtverečků černě a bíle jako políčka na šachovnici. Tento podklad se nebude během řešení měnit. Při každém tahu tedy prázdné políčko změní barvu. Protože prázdné políčko zůstane ve stejné poloze, když je problém vyřešen, bude mít stejnou barvu jako na začátku. Proto je potřeba sudý počet tahů. Při každém tahu se zamění písmeno s prázdným políčkem a změní se parita permutace. K tomu, abychom prohodili dva páry písmen a zbytek zůstal zachován, potřebujeme sudý počet tahů. Pokud tedy prohodíme R z prvního a druhého řádku a zároveň l a a z posledního

¹⁴Poznamenejme, že nový Vítězný oblouk v La Défense v Paříži představuje znázornění čtyřrozměrné krychle v trojrozměrném prostoru.

řádku, vykonáme sudý počet tahů a problém je tedy potenciálně řešitelný. Nyní si můžete prakticky vyzkoušet, že problém lze skutečně vyřešit.

L i t e r a t u r a

- [1] ABEL, N. H.: *Mémoire sur les équations algébriques où on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*. Goendahl, Christiana 1824.
- [2] ASCHBACHER, M.: *The status of the classification of the finite simple groups*. Notices Amer. Math. Soc. 51 (2004), 736–740.
- [3] BURNSIDE, W.: *On groups of order $p^\alpha q^\beta$* . Proc. London Math. Soc. 2 (1904), 388–392.
- [4] BURNSIDE, W.: *Theory of groups of finite order*. Cambridge 1911, Dover Publ., New York 1955, (reprinting 2004).
- [5] CONWAY, J. H.: *A simple construction of the Fischer–Griess monster group*. Invent. Math. 79 (1985), 513–540.
- [6] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A., WILSON, R. A.: *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups*. Oxford Univ. Press 1985.
- [7] CONWAY, J. H., SLOANE, N. J. A.: *Sphere packing, lattices and groups*. Springer, Berlin 1988.
- [8] FEIT, W., THOMPSON, J. G.: *Solvability of groups of odd order*. Pacific J. Math. 13 (1963), 775–1029.
- [9] GALLIAN, J. A.: *The search for finite simple groups*. Math. Magazine 49 (1976), 163–180.
- [10] HALL, B. C.: *Lie groups, Lie algebras, and representations*. Springer-Verlag, New York 2003.
- [11] JACOBSON, C.: *Basic algebra I*, 2nd ed. W.H. Freeman and Company 1985.
- [12] JORDAN, C.: *Traité des substitutions*. Gauthier-Villars, Paris 1870.
- [13] KARGAPOLOV, M. I., MERZJAKOV, JU. I.: *Osnovy teorii grupp*. 2. vyd., Nauka, Moskva 1977.

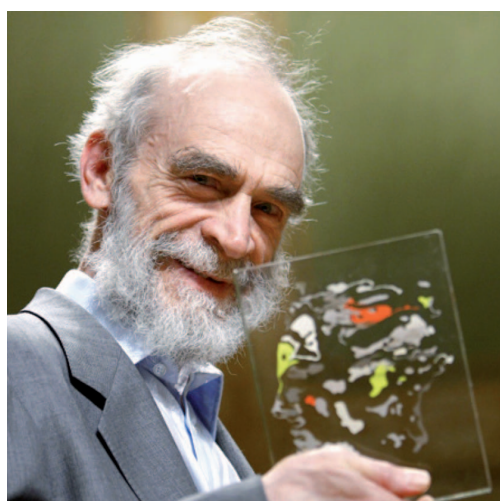
- [14] KARGER, A., NOVÁK, J.: *Prostorová kinematika a Lieovy grupy*. SNTL, Praha 1987.
- [15] KRÍŽEK, M., SOMER, L.: *Architects of symmetry in finite nonabelian groups*. *Symmetry: Culture and Science* 21 (2010), 333–344.
- [16] KUROŠ, A. G.: *Kapitoly z obecné algebry*. Academia, Praha 1968.
- [17] LITZMAN, O., SEKANINA, M.: *Užití grup ve fyzice*. Academia, Praha 1982.
- [18] MAC LANE, S., BIRKHOFF, G.: *Algebra*. Alfa, Bratislava 1973.
- [19] PFENDER, F., ZIEGLER, G. M.: *Kissing numbers, sphere packings, and some unexpected proofs*. *Notices Amer. Math. Soc.* 51 (2004), 873–883.
- [20] PRADLOVÁ, J., KRÍŽEK, M.: *Grupy kolem nás*. *Rozhledy mat.-fyz.* 76 (1999), 209–216, 261–267, 77 (2000), 5–12.
- [21] PRAVDA, V.: *Maticové Lieovy grupy a Lieovy algebry*. *PMFA* 52 (2007), 219–230.
- [22] RONAN, M.: *Symmetry and the Monster. One of the greatest quests of mathematics*. Oxford Univ. Press 2006.
- [23] SOLOMON, R.: *A brief history of the classification of the finite simple groups*. *Bull. Amer. Math. Soc.* 38 (2001), 315–352.
- [24] SYLOW, L., LIE, S. (Eds): *Œuvres complètes de Niels Henrik Abel, vol. I, II*. Nouvelle Edition, Oslo 1881.
- [25] THOMPSON, T. M.: *From error-correcting codes through sphere packing to simple groups*. Math. Assoc. Amer., Washington 1983.
- [26] TITS, J.: *Buildings of spherical type and finite BN-pairs*. LN in Math. 386, Springer, New York 1974.
- [27] TŮMA, J.: *Matematické hlavolamy a základy teorie grup*. Mladá fronta, Praha 1988.

7. Abelova cena v roce 2009 udělena Michailu Gromovovi

Oldřich Kowalski, Michal Krížek

7.1 Prolog

Podle klasifikace Mathematical Reviews v dnešní době existuje přibližně 100 základních matematických disciplín, a tak je velice obtížné zvolit vhodného kandidáta. V roce 2003 získal první Abelovu cenu Jean-Pierre Serre za své průkopnické práce z algebraické geometrie, teorie čísel a několika příbuzných oborů. V dalších letech pak následovaly ceny za topologii a algebru (2004), aplikovanou a numerickou matematiku (2005), harmonickou analýzu a teorii dynamických



MICHAIL LEONIDOVICH GROMOV

systémů (2006), teorii pravděpodobnosti a statistiku (2007) a teorii grup (2008). O prvních pěti Abelových cenách podrobně pojednává publikace [11]. V roce 2009 získal Abelovu cenu rusko-francouzský matematik Michail Leonidovič Gromov za své revoluční výsledky týkající se především diferenciální geometrie, algebry a topologie. Výběrová komise pracovala ve složení Kristian Seip (předseda), John Kingman, Sergej Novikov, Neil Trudinger a Efim Zelmanov.

V březnu 2009 prezident Norské akademie věd Øyvind Østerud oznámil veřejnosti jméno nového laureáta, jemuž pak cenu osobně předal norský král Harald V. v hlavní aule univerzity v Oslu dne 19. května 2009. Pamětní řeč pronesla paní Ingrid Daubechiesová (Princetonská univerzita), bývalá členka výběrové komise a zakladatelka teorie waveletů. Poté následovaly čtyři abelovské přednášky, z nichž první měl právě M. Gromov (viz [17]).

7.2 Kdo je Michail Gromov?

Michail Gromov se narodil 23. prosince 1943 v Boksitogorsku (100 km jihovýchodně od Ladožského jezera). Univerzitní studia absolvoval v roce 1965 v Leningradu. Již ve svých pětadvaceti letech zde získal doktorát. Jeho školitelem byl vynikající matematik V. A. Rochlin. V letech 1967–1974 pracoval Gromov jako odborný asistent na Leningradské univerzitě. Poté odešel na Newyorskou státní univerzitu v Stony Brook na Long Islandu.

V roce 1981 se M. Gromov natrvalo přestěhoval do Francie. Nejprve nastoupil na Université de Paris a o rok později získal stálé místo profesora ve výzkumném ústavu Institut des hautes études scientifiques v Bures-sur-Yvette (na jižním předměstí Paříže), kde pracuje dodnes. Od roku 1992 je francouzským občanem.

Gromovovy myšlenky neustále inspirují matematiky z celého světa. Profesor Gromov je znám především svými výsledky v těch oblastech matematiky, které úzce souvisejí s geometrií. Je autorem celé řady monografií, viz např. [3]–[8]. V poslední době se intenzivně věnuje také matematické genetice (viz např. [1], [9]).

M. Gromov získal za svou práci mnoho uznání. Mezi nejvýznamnější patří cena Moskevské matematické společnosti (1971), Cartanova cena pařížské Akademie věd (1984), Wolfova cena (1993), Lobačevského medaile (1997), Steelova cena (1997), Balzanova ce-

na (1999) a Bolyaiova cena (2005). Profesor Gromov je zahraničním členem Národní akademie věd v USA, Americké akademie umění a věd a řádným členem Francouzské akademie věd. Čtyřikrát byl zvaným plenárním řečníkem na mezinárodních matematických kongresech v Nice (1970), Helsinkách (1978), Varšavě (1982) a v Berkeley (1986). Je také profesorem matematiky v Courantově ústavu matematických věd v New Yorku (viz obr. 3.1). V této prestižní instituci pracují i Peter Lax a Šrínivása Varadhan, kteří získali Abelovu cenu v roce 2005, resp. 2007.

7.3 Stručně o diferenciální geometrii

Slovo *geometrie* pochází z řečtiny: *geo* = země, *metria* = míra. V klasické diferenciální geometrii se zprvu vyšetřovaly speciální plochy v prostoru, jako např. kulové plochy, kužele, válce, elipsoidy či hyperbolické paraboloidy. Klíčovým pojmem, o který se diferenciální geometrie opírá, je *křivost*. Leonhard Euler (1707–1783) byl prvním matematikem, který si to uvědomil.

Podstatným způsobem se ale o rozvoj diferenciální geometrie zasloužil až Carl Friedrich Gauss (1777–1855). Jeho průkopnická práce *Disquisitiones generales circa superficies curvas* z roku 1827 už podává moderní definici zakřivené plochy a algoritmus, jak počítat její křivost (tzv. Gaussovu křivost v dnešní terminologii). Připomeňme, že Gaussova křivost K v bodě P plochy v trojrozměrném eukleidovském prostoru je rovna součinu křivostí v P dvou křivek,¹ které vzniknou jako řezy plochy normálovými rovinami v tzv. hlavních směrech. To je dáno známou formulkou $K = k_{\max} k_{\min}$.

Gauss také definoval první a druhou základní formu plochy, a položil tak základy Riemannově geometrii. V roce 1828 vyslovil jedno ze základních tvrzení v klasické diferenciální geometrii, které lze zhruba charakterizovat takto:

Gaussova Theorema Egregium.² *Pokud budeme zakřivenou plochu izometricky deformovat v prostoru, její (Gaussova) křivost v každém bodě zůstane zachována.*

¹Křivost neprotínající se hladké rovinné křivky v daném bodě je rovna převrácené hodnotě poloměru příslušné oskulační kružnice.

²Latinsky *egregius* znamená nádherný, vynikající, výtečný, výborný, znamenitý.

Uveďme si názorný příklad. Rovina reprezentovaná listem papíru má Gaussovu křivost nula. Jestliže stočíme list do válcové či kuželové plochy, bude její Gaussova křivost stále nula.

V souvislosti s diferenciální geometrií 19. století je vhodné zmínit ještě jména Nikolaj I. Lobačevskij (1792–1856), János Bolyai (1802–1860), Sophus Lie (1842–1899) a Felix Klein (1849–1925). Skutečně ucelené počátky tzv. klasické (nebo též lokální) diferenciální geometrie lze datovat inaugurační přednáškou Bernharda Riemanna v Göttingenu roku 1854. V tomto oboru se studují především hladké křivky, zakřivené plochy a nadplochy. Vyšetřují se zde jejich lokální vlastnosti (např. křivost ploch a křivek, význačné křivky na plochách, metrická ekvivalence ploch, studují se též přímkové kongruence a komplexy aj.). Asi v polovině 20. století se začíná rozvíjet moderní (nebo též globální) diferenciální geometrie. Ta studuje globální vlastnosti ploch a nadploch v souvislosti s topologií. Vyšetřuje též geometrii *hladkých variet* opatřených metrikou nebo jinými geometrickými strukturami.

Příkladem globální vlastnosti je orientovatelnost plochy. Jestliže budeme postupně natírat známý Möbiův list barvou, pak se nám podaří natřít obě strany listu, aniž překročíme jeho okraj. Proto je to plocha neorientovatelná.

V následujícím textu představíme pojem hladké variety, která je abstraktním modelem hladké plochy libovolné dimenze v eukleidovském prostoru.

Topologická d -rozměrná varieta M je metrizable prostor, který je lokálně homeomorfní s d -rozměrným eukleidovským prostorem $\mathbb{R}^d$ pro dané $d \in \{1, 2, 3, \dots\}$ (viz [12]). Jinými slovy, každý bod v M má otevřené okolí, které je homeomorfní s nějakou otevřenou množinou v $\mathbb{R}^d$.

Hladká d -rozměrná varieta M je d -rozměrná topologická varieta s tzv. *hladkou strukturou*, tj. pokrytím otevřenými množinami, kterým říkáme *obory lokálních souřadnic* a kde přechody mezi dvěma soustavami lokálních souřadnic jsou vyjádřeny diferencovatelnými funkcemi třídy C^∞ .

Vložení (angl. embedding) je hladké zobrazení f variety M do variety N , jehož obraz $f(M)$ s indukovanou topologií z N je homeomorfní s varietou M .

Obecně nelze d -rozměrnou varietu vložit do $\mathbb{R}^{d+1}$. Nejznámějším

příkladem této překvapivé skutečnosti je Kleinova láhev (viz [21, Corollary 11.16]), což je dvojrozměrná varieta ve čtyřrozměrném prostoru, kterou nelze vložit do trojrozměrného prostoru.³ Tato plocha navíc není orientovatelná. Platí však následující tvrzení (viz [21, Th. 11.14]):

Věta. *Je-li M kompaktní hladká d -rozměrná varieta v $\mathbb{R}^{d+1}$, pak M je orientovatelná.*

Z tvrzení věty vyplývá, že množina $\mathbb{R}^{d+1} \setminus M$ má dvě komponenty (vnitřek a vnějšek). Jejich hranicí je v obou případech M . Následující důležitou větu o vložení lze nalézt např. v [10, s. 24].

Whitneyova věta. *Každou hladkou d -rozměrnou varietu lze hladce vložit do eukleidovského prostoru $\mathbb{R}^{2d+1}$.*

Dvojici (M, g) nazveme *Riemannovou varietou*, jestliže M je hladká varieta, jejíž tečný prostor v každém bodě $x \in M$ je opatřen skalárním součinem g_x , a ten se hladce mění od bodu k bodu. Takto vytvořená struktura g se nazývá *Riemannova metrika*.

Další významné tvrzení v diferenciální geometrii vyjadřuje Gaussova–Bonnetova věta pro dvojrozměrné kompaktní Riemannovy variety (M, g) (bez okraje). Týká se *totální křivosti plochy*, která vznikne integrací Gaussovy křivosti K přes celou plochu.

Gaussova–Bonnetova věta. *Nechť K označuje Gaussovu křivost variety $M \subset \mathbb{R}^3$. Potom*

$$\int_M K dM = 2\pi\chi(M),$$

kde na levé straně je tzv. *plošný integrál* a $\chi(M)$ označuje *Eulerovu charakteristiku variety M* .

Podotkněme, že Eulerova charakteristika je topologický invariant, jenž se počítá následujícím způsobem. Uvažujme mnohostěn (obecně nekonvexní), jehož povrch je homeomorfní dané varietě a je pokryt nějakou triangulací (tj. množinou trojúhelníků, z nichž každé dva mají společnou právě jednu celou hranu, nebo právě jeden vrchol, nebo jsou

³Poznamenejme, že často vystavovaný trojrozměrný skleněný model „Kleinovy láhve“ nereprezentuje topologickou varietu (viz obr. 13.1). V bodech, kde se plocha protíná, totiž neexistuje otevřené okolí, které by bylo homeomorfní s otevřeným kruhem v $\mathbb{R}^2$.

disjunktní). Označme s počet stěn, h počet hran a v počet vrcholů v této triangulaci. Pak definujeme $\chi(M) = s - h + v$. V případě sféry S^2 , která je homeomorfní s povrchem čtyřstěnu, okamžitě zjistíme, že $\chi(S^2) = 2$.

Pro anuloid T^2 snadno nalezneme triangulaci toroidálního mnohostěnu a jemu odpovídající Eulerovu charakteristiku $\chi(T^2) = 0$. Anuloid má v bodech bližších k jeho rotační ose zápornou Gaussovu křivost (podobně jako sedlový bod), v bodech odvrácených od osy má kladnou křivost a na dvou kružnicích oddělujících tyto množiny bodů má nulovou křivost. Totální křivost anuloidu je však poněkud překvapivě nula, jak plyne ihned z Gaussovy–Bonnetovy věty.

Snadno si také představíme dutý „preclík“ se dvěma či více otvory. Pak platí obecně, že Eulerova charakteristika je rovna $2 - 2q$, kde q je tzv. *rod plochy* a je to v podstatě počet otvorů v preclíku. Sféra s q „držadly“ je plocha rodu q .

Gaussova–Bonnetova formule pak zní

$$\int_M K dM = 4\pi(1 - q).$$

Odtud například odvodíme, že každá Riemannova metrika definovaná na sféře musí mít alespoň v jednom bodě kladnou Gaussovu křivost a že Riemannova metrika definovaná na anuloidu nemůže mít všude kladnou nebo všude zápornou Gaussovu křivost.

Připomeňme si ještě jednu důležitou aplikaci diferenciální geometrie. Albert Einstein (1879–1955) zjistil, že všechny hmotné objekty (planety, hvězdy, galaxie aj.) náš prostoročas lokálně zakřivují.⁴ Proto potřeboval „novou geometrii“ k tomu, aby mohl zformulovat obecnou teorii relativity. Diferenciální geometrie tak našla zcela nové uplatnění.

Nejkratší cestu mezi dvěma body na hmotném modelu nějaké zakřivené plochy můžeme znázornit pomocí natažené gumičky. Taková nejkratší cesta, které říkáme *geodetický oblouk*, ale nemusí být určena jednoznačně. Například na ideálním modelu povrchu Země jsou všechny poledníky nejkratšími spojnicemi obou pólů.

Geodetika nemusí být vždy nejkratší spojnici dvou bodů. To platí pouze lokálně, kdy všechny perturbované křivky mezi dvěma dostatečně blízkými body na geodetice jsou delší. Nejednoznačné geodetiky

⁴O zakřiveném vesmíru uvažoval jako první už v roce 1900 německý matematik a fyzik Karl Schwarzschild [19].

ve vesmíru objevil i Hubbleův kosmický dalekohled díky tzv. gravitačním čočkám, které způsobují, že obraz některých vzdálených galaxií je vícenásobný. Přitom fotony z téhož zdroje (pohybující se po geodetikách) mohou absolvovat různě dlouhou cestu. Mnohdy tak vidíme různé obrazy jedné galaxie časově posunuté až o několik let.

Zatím není známo, zda je náš vesmír ohraničený a uzavřený do sebe a jaká je jeho totální křivost. Vesmír budeme modelovat izochronou v prostoročasu, která odpovídá určitému časovému okamžiku po velkém třesku. Einstein zformuloval následující *kosmologický princip*: *Vesmír je (na velkých škálách) v každém bodě homogenní a izotropní.*

Homogenita znamená, že pro daný čas jsou střední hustota hmoty i tlak konstantní, tj. Gaussova křivost vesmíru je ve všech bodech stejná. Izotropie říká, že pozorovatel nemůže rozlišit daný směr od ostatních směrů. Podle [16, kap. 27.3] izotropie implikuje homogenitu. Astronomická pozorování rozložení supernov, γ -záblesků a reliktního záření zatím izotropii vesmíru v zásadě potvrzují.

Einsteinův kosmologický princip nám dává odpověď na otázku, jaká by mohla být topologie našeho vesmíru, pokud lze odpovídající varietu vložit do čtyřrozměrného prostoru. Platí totiž následující tvrzení (viz [13], [21]), že každá souvislá metricky úplná hladká varieta dimenze d v $\mathbb{R}^{d+1}$, která má stejnou Gaussovu křivost v každém bodě a každém směru, je nadsféra nebo nadrovina. Jestliže varietu modelující vesmír nelze vložit do $\mathbb{R}^4$, pak lze připustit i hyperbolické geometrie.

Netriviální topologie vesmíru nesplňují podmínku izotropie. Kdyby náš vesmír měl např. toroidální topologii $\mathbb{T}^3$ v $\mathbb{R}^4$, pak by pozorovatel mohl určit směr, který se odlišuje od ostatních, neboť v libovolném bodě má $\mathbb{T}^3$ v různých směrech obecně různé křivosti.

V letech 2002–2003 Grigorij Jakovlevič Perelman dokázal slavnou Poincarého domněnku (viz Science 314 (2006), s. 1848). Podle ní je každá jednoduše souvislá kompaktní trojrozměrná topologická varieta homeomorfní se sférou

$$\mathbb{S}^3 = \{(x_0, x_1, x_2, x_3) \in \mathbb{R}^4 \mid x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1\},$$

tj. trojrozměrným povrchem čtyřrozměrné jednotkové koule (viz [18, kap. 5]).⁵ Pokud jsou uvedené předpoklady pro model vesmíru splně-

⁵Pro dvojrozměrné variety byla tato domněnka dokázána již v 19. století. Pro čtyřrozměrné variety ji dokázal Freedman v roce 1982 (viz [2]), za což získal Fieldsovu medaili v r. 1986. Důkaz pro všechny vyšší dimenze byl znám již dříve [19].

ny, můžeme si vesmír a jeho rozpínání představit jako trojrozměrný povrch nerovnoměrně se nafukující nadkoule o poloměru $R = R(t)$ v $\mathbb{R}^4$, v jejímž středu je velký třesk (srov. [16, kap. 27.5]). Takový model vesmíru je izomorfní s komplexní kružnicí $\{(x, y) \in \mathbb{C}^2; |x|^2 + |y|^2 = R^2(t)\}$ se vzrůstajícím poloměrem.

7.4 Hlavní Gromovovy výsledky

Michail Gromov přispěl podstatně k pokroku v globální diferenciální geometrii i v dalších matematických disciplínách. Připomeňme si zde jen některé z jeho hlavních výsledků. Definice uváděných pojmů lze najít např. v [10]–[13], [15].

1) Bishopova–Gromovova nerovnost

Nechť M je úplná d -rozměrná Riemannova varieta s pozitivně se-midefinitní Ricciho křivostí. Pak objem koule v M je menší nebo roven objemu koule⁶ o stejném poloměru v eukleidovském prostoru $\mathbb{R}^d$. Jestliže navíc $v_P(r)$ označuje objem koule o středu P a poloměru r na varietě M a jestliže $V(r) = c_d r^d$ označuje objem koule o poloměru r v d -rozměrném eukleidovském prostoru, pak je funkce $r \mapsto v_P(r)/V(r)$ nerostoucí. Tato vlastnost hraje mj. klíčovou roli při důkazu Gromovovy věty o kompaktnosti (viz bod 3).

2) Gromovova věta o grupách polynomiálního růstu

Nechť $S' = \{g_1, \dots, g_n\}$ je množina generátorů konečně generované grupy G a $S = \{g_1, \dots, g_n, g_1^{-1}, \dots, g_n^{-1}\}$ je symetrizace množiny S' . Označme $S^{(n)}$ počet prvků z G , které se dají zapsat jako slova vytvořená z S a délky nepřesahující n . Je zřejmé, že v obecném případě číslo $S^{(n)}$ roste exponenciálně. Joseph Wolf ukázal, že pokud je grupa G nilpotentní, potom existuje polynom $p(n)$ takový, že $S^{(n)} < p(n)$ pro každé přirozené n , což jinými slovy znamená, že taková grupa má polynomiální růst. Gromovova věta charakterizuje grupy polynomiálního růstu právě jako ty grupy, které obsahují nilpotentní podgrupy s konečným indexem. K původnímu důkazu této věty použil Gromov jím vytvořenou definici konvergence kompaktních metrických prostorů, která se nyní nazývá Gromovova–Hausdorffova konvergence a stále se hojně používá v geometrii a topologii. O tomto tématu nyní stručně pojednáme:

⁶Například Slunce má o trochu menší objem (resp. povrch a obvod) než $\frac{4}{3}\pi r^3$ (resp. $4\pi r^2$ a $2\pi r$), protože gravitace zakřivuje prostor, srov. [14], [16, s. 1099].

3) Gromovova–Hausdorffova konvergence

Připomeňme nejprve klasický pojem Hausdorffovy vzdálenosti v metrických prostorech. Necht' A a B jsou dvě neprázdné omezené uzavřené množiny metrického prostoru (M, ρ) . Potom jejich Hausdorffova vzdálenost v M je dána vzorcem

$$\rho_H(A, B) = \max\{\sup\{\rho(a, B) \mid a \in A\}, \sup\{\rho(b, A) \mid b \in B\}\}.$$

Dále se zavádí *Gromovova–Hausdorffova vzdálenost* $d_{GH}(X, Y)$ dvou kompaktních metrických prostorů X a Y jako infimum všech čísel $\rho_H(f(X), g(Y))$, kde probíháme všechny metrické prostory (M, ρ) a všechna izometrická vložení $f: X \rightarrow M$, $g: Y \rightarrow M$.

Gromovova–Hausdorffova vzdálenost pak definuje množinu všech tříd izometrie kompaktních metrických prostorů jako nový metrický prostor. Takto je možno definovat konvergenci posloupností kompaktních metrických prostorů, která se nazývá *Gromovova–Hausdorffova konvergence*. Limitní metrický prostor při takové konvergenci se nazývá *Hausdorffova limita* dané posloupnosti prostorů. Takto definovaná konvergence má některé překvapující vlastnosti. Například posloupnost kompaktních Riemannových prostorů (variet) dimenze 3 může konvergovat k metrickému (ale ne již Riemannovu!) prostoru Hausdorffovy dimenze 4, jak ukázal jeden ze žáků M. Gromova. Na druhé straně platí *Gromovova věta o (pre)kompaktnosti* v Riemannově geometrii, která říká, že množina kompaktních Riemannových variet dané dimenze, jejichž Ricciho křivosti jsou omezeny zdola společnou konstantou a jejichž průměry jsou omezeny shora některou jinou konstantou, je relativně kompaktní v Gromovově–Hausdorffově metrice (tj. uzávěr této množiny je kompaktní).

4) Gromovův součin

Tento pojem je rovněž svázán s metrickými prostory. Motivací je určit vzdálenost, pro kterou dvě geodetické křivky vycházející ze stejného bodu zůstávají stále „v dosahu této vzdálenosti“. Necht' (X, d) je metrický prostor a necht' $x, y, z \in X$ jsou libovolné body. Potom Gromovův součin bodů y a z při x označený symbolem $(y, z)_x$ je definován vztahem $(y, z)_x = \frac{1}{2}((d(x, y) + d(x, z) - d(y, z)))$ a má tyto vlastnosti:

- a) Symetrie: $(y, z)_x = (z, y)_x$.
- b) Degenerovanost v koncových bodech: $(y, z)_y = (y, z)_z = 0$.

c) Pro každých pět bodů $p, q, x, y, z \in X$ platí

$$\begin{aligned} d(x, y) &= (x, z)_y + (y, z)_x, \\ 0 &\leq (y, z)_x \leq \min\{d(x, y), d(x, z)\}, \\ |(y, z)_p + (y, z)_q| &\leq d(p, q), \\ |(x, y)_p + (x, z)_p| &\leq d(y, z). \end{aligned}$$

Metrický prostor (X, d) se nazývá δ -hyperbolický, jestliže pro všechny body $p, x, y, z \in X$ platí $(x, z)_p \geq \min\{(x, y)_p, (y, z)_p\} - \delta$, kde $\delta > 0$ je reálné číslo.

Nežli uvedeme jednu z hlavních vět, připomeňme si definici geodetiky v metrickém prostoru. *Geodetická křivka* v metrickém prostoru (X, d) je křivka $\gamma : I \rightarrow X$, která lokálně minimalizuje vzdálenosti. Přesněji řečeno, existuje konstanta $\nu \geq 0$ s vlastností, že pro každé $t \in I$ existuje okolí $J(t) \subset I$ takové, že pro každá dvě $t_1, t_2 \in J(t)$ platí rovnost

$$d(\gamma(t_1), \gamma(t_2)) = \nu|t_1 - t_2|.$$

Jeden z hlavních výsledků pak říká: Zvolme $\delta > 0$. Potom metrický prostor (X, d) je δ -hyperbolický, právě když pro každý geodetický trojúhelník ABC v (X, d) a pro každý bod $P \in AB$ existuje bod $Q \in AC \cup BC$ takový, že $d(P, Q) \leq \delta$. Jinými slovy, metrický prostor (X, d) je δ -hyperbolický, právě když každý jeho geodetický trojúhelník je „ δ -tenký“. Je zřejmé, že každý omezený prostor (X, d) je δ -hyperbolický pro některé $\delta > 0$. Teorie je tedy netriviální pouze pro neomezené metrické prostory. Na toto téma vyšlo velké množství prací jiných autorů včetně monografií.

5) Hyperbolické grupy

Tyto grupy jsou známy též pod názvy *lexikografické hyperbolické grupy*, *Gromovovy hyperbolické grupy* nebo *negativně zakřivené grupy*. Každá taková grupa je konečně generovaná grupa s „lexikografickou metrikou“ a splňuje některé vlastnosti charakteristické pro hyperbolickou geometrii (viz [5]). *Lexikografická metrika* na grupě G je způsob, jak měřit vzdálenost mezi dvěma prvky z G . Je to metrika na G přiřazující každým dvěma prvkům g a h jejich vzdálenost $d(g, h)$, která vyjadřuje, jak krátkým slovem (jehož písmena jsou prvky množiny generátorů) lze vyjádřit jejich rozdíl. Množina generátorů grupy G musí být vždy pevně zvolena. Různé volby množiny generátorů obvykle vedou k různým lexikografickým metrikám. I přes

zmíněnou nejednoznačnost může být tento pojem využit k důkazům vět o geometrických vlastnostech grup, jak je tomu například v *geometrické teorii grup*. Obzvláště vlivným a velkým tématem v tomto směru je *Gromovův program* klasifikace konečně generovaných grup vzhledem k jejich globální geometrii. Formálně to znamená klasifikaci konečně generovaných grup opatřených lexikografickými metrikami až na kvazi-izometrii. Tento program zahrnuje velkou řadu různých aspektů z algebry, geometrie a topologie a je stále v intenzivním vývoji. Zde podotkněme, že zobrazení $f: X \rightarrow Y$ se nazývá *kvazi-izometrie*, jestliže existují konstanty $K \geq 1$ a $C \geq 0$ takové, že platí

$$\frac{1}{K} d_X(x, y) - C \leq d_Y(f(x), f(y)) \leq K d_X(x, y) + C$$

a každý bod z Y má vzdálenost nejvýše C od nějakého bodu z $f(X)$. Poznamenejme ještě, že kvazi-izometrie nemusí být spojitě zobrazení a například každé zobrazení mezi kompaktními metrickými prostory je kvazi-izometrie. Přesto má tento pojem překvapivě velký význam pro matematiku.

6) *Skoro ploché variety*

Hladká kompaktní varieta M se nazývá *skoro plochá*, jestliže pro každé $\varepsilon > 0$ na ní existuje Riemannova metrika $g(\varepsilon)$ taková, že průměr $\text{diam}(M, g(\varepsilon))$ variety M vzhledem k této metrice nepřesahuje 1 a $g(\varepsilon)$ je ε -plochá, tj. pro sekcionální křivost této metriky platí $|K_{g(\varepsilon)}| \leq \varepsilon$.

Nil-varieta je kvocient nilpotentní Lieovy grupy podle její uzavřené podgrupy. Dále nechť nilpotentní Lieova grupa N operuje na sobě pomocí levých translací a nechť je dána konečná grupa automorfismů F grupy N . Pak lze definovat akci semidirektního součinu $N \rtimes F$ na N . Kompaktní kvocient grupy N podle podgrupy součinu $N \rtimes F$ (operující volně na N) se nazývá „infrasil-varieta“. Infrasil-variety jsou kvocienty nil-variet podle konečných podgrup (ale opak obecně neplatí).

Gromov a Ruh dokázali, že kompaktní varieta M je skoro plochá, když a jen když je to infrasil-varieta. Opět tu máme příklad hluboké souvislosti mezi algebrou a geometrií.

7) *Gromovovy systolické nerovnosti*

Systola (nebo přesněji *1-systola*) kompaktního metrického prostoru X je metrický invariant definovaný jako nejmenší délka netažitelné smyčky v X , tj. uzavřené křivky, která nemůže být v X

spojitě deformována do svého výchozího bodu. Tento pojem tedy souvisí s fundamentální grupou (první homotopickou grupou) $\pi_1(X)$ prostoru X . Dále označujeme takto definovanou systolu symbolem $\text{sys } \pi_1$, abychom ji odlišili od podobného pojmu v teorii homologie. Poznamenejme, že kompaktní, orientovatelná a $(d-1)$ -souvislá d -rozměrná varieta M se nazývá *podstatná*, jestliže platí $\int_M \omega \neq 0$ pro některý netriviální element objemu (tj. vnější diferenciální formu ω stupně d) na M . Nechť M je nyní podstatná kompaktní Riemannova varieta. Základní Gromovova systolická nerovnost potom zní

$$(\text{sys } \pi_1)^d \leq C_d \text{vol}(M),$$

kde C_d je univerzální konstanta závisající pouze na dimenzi variety M .

Vyplňující poloměr jednoduché smyčky C v rovině je definován jako největší poloměr $R > 0$ kružnice, která se vejde dovnitř této smyčky. Označuje se symbolem $\text{FillRad}(C)$. Nyní se pokusíme názorně charakterizovat *vyplňující poloměr variety*. Uvažujme epsilonové okolí smyčky C v rovině, které označíme symbolem $U_\varepsilon C \subset \mathbb{R}^2$. Když číslo $\varepsilon > 0$ roste, potom ε -okolí $U_\varepsilon C$ pohlcuje stále více vnitřku smyčky. Poslední bod, který bude pohlcen, je přesně střed největší vepsané kružnice. Můžeme tedy podat jinou definici vyplňujícího poloměru jako infima všech čísel $\varepsilon > 0$ takových, že smyčka C se dá stáhnout do jediného bodu v $U_\varepsilon C$.

Je-li nyní dána podstatná kompaktní varieta M bez okraje vložená například do eukleidovského prostoru $\mathbb{R}^d$, můžeme definovat vyplňující poloměr podvariety M vzhledem k danému vložení tak, že budeme minimalizovat velikost epsilonového okolí $U_\varepsilon M \subset \mathbb{R}^d$ variety M , ve kterém se M stane homotopicky ekvivalentní s nějakým objektem nižší dimenze, například polyedrem. K zavedení obecné definice vyplňujícího poloměru $\text{FillRad}(M)$ pro obecnou varietu potřebujeme teorii homologií, a proto se tím zde nebudeme zabývat. Gromov také dokázal následující (druhou) systolickou nerovnost:

$$\text{sys } \pi_1 \leq 6 \text{FillRad}(M).$$

Dále ještě našel odhad shora $\text{FillRad}(M) \leq C_d (\text{vol}(M))^{1/d}$ pro vyplňující poloměr. Z druhé systolické nerovnosti a poslední nerovnosti pak snadno plyne první systolická nerovnost.

8) *Symplektická geometrie*

Symplektická geometrie je oblast diferenciální geometrie a diferenciální topologie, která studuje *symplektické variety*, tj. diferencovatelné variety, které mají uzavřenou nedegenerovanou vnější diferenciální 2-formu. (Uzavřenost zde znamená, že vnější diferenciál této formy je roven nule.) Symplektická geometrie má svoje počátky v Hamiltonově formulaci klasické mechaniky, kde fázový prostor jistých klasických systémů má strukturu symplektické variety. Každá Kählerova varieta je rovněž symplektickou varietou. Až do 70. let zůstávala otevřena otázka, zdali existují kompaktní symplektické variety, které nejsou Kählerovy. První takové příklady byly sestrojeny Williamem P. Thurstonem⁷. Nyní lze dokonce říci, že „většina“ symplektických variet nepřipouští Kählerovu strukturu. M. Gromov ale udělal důležitý objev v tom směru, že všechny symplektické variety připouštějí hojnost struktur splňujících všechny axiomy Kählerových variet s výjimkou toho, že by přechodové funkce mezi dvěma lokálními souřadnicovými soustavami byly holomorfní. Tento poznatek použil k rozvinutí teorie *pseudoholomorfních křivek*, což vedlo k podstatnému pokroku v symplektické geometrii, zejména k zavedení symplektických invariantů, které jsou nyní známy jako *Gromovovy–Wittenovy invarianty*. Tyto invarianty hrají klíčovou roli ve fyzikální teorii strun.

L i t e r a t u r a

- [1] CARBONE, A., GROMOV, M.: *Functional labels and syntactic entropy on DNA strings and proteins*. Theoret. Comput. Sci. 303 (2003), 35–51.
- [2] FREEDMAN, M. H.: *The topology of four-dimensional manifolds*. J. Differ. Geom. 17 (1982), 357–453.
- [3] GROMOV, M.: *Structures métriques pour les variétés riemanniennes*. CEDIC, Paris 1981.
- [4] GROMOV, M.: *Partial differential relations*. Springer-Verlag, Berlin 1986.
- [5] GROMOV, M.: *Hyperbolic groups*. In Essays in Group Theory (ed. G. M. Gersten), MSRI Publ. 8 (1987), 75–263.

⁷Thurston získal v roce 1982 Fieldsovu medaili zejména za teorii Hakenových variet.

- [6] GROMOV, M.: *Asymptotic invariants of infinite groups. Geometric Group Theory, vol. 2.* London Math. Soc., LN 182, Cambridge Univ. Press 1993.
- [7] GROMOV, M.: *Carnot–Carathéodory spaces seen from within. Sub-Riemannian Geometry.* Prog. Math. 144, Birkhäuser, Basel 1996, 79–323.
- [8] GROMOV, M.: *Metric structures for Riemannian and non-Riemannian spaces.* Birkhäuser, Boston 1999.
- [9] GROMOV, M.: *Mendelian dynamics and Sturtevant’s paradigm.* Contemp. Math. 469 (2008), 227–242.
- [10] HIRSCH, M. W.: *Differential topology.* Springer, Berlin 1976, 1997.
- [11] HOLDEN, H., RIENE, R. (Eds): *The Abel Prize 2003–2007. The first five years.* Springer-Verlag, Berlin, New York 2009.
- [12] KLINGENBERG, W.: *Riemannian geometry.* Walter de Gruyter, Berlin, New York 1982.
- [13] KOBAYASHI, S., NOMIZU, K.: *Foundation of differential geometry*, vol. II. Interscience, London, New York 1969.
- [14] KRÍŽEK, M.: *Proč je obvod Slunce menší než $2\pi r$?* Obzory mat. fyz. inf. 46 (3) (2017), 7–18.
- [15] MAC LANE, S., BIRKHOFF, G.: *Algebra.* Alfa, Bratislava 1973.
- [16] MISNER, C. W., THORNE, K. S., WHEELER, J. A.: *Gravitation* (20th edition). Freeman, New York 1997.
- [17] SAPIRO, G.: *Abel Prize science lecture: Revolutionary work in geometry and shape analysis.* SIAM News 42 (2009), 1, 3.
- [18] O SHEA, D.: *Poincarého domněnka.* Edice Galileo, Academia, Praha 2010.
- [19] K. SCHWARZSCHILD: *Über das zulässige Krümmungsmaß des Raumes.* Vierteljahrsschrift der Astronomischen Gesellschaft 35 (1900), 337–347; English translation: *On the permissible numerical value of the curvature of space.* Abraham Zelmanov J. 1 (2008), 64–73.
- [20] SMALE, S.: *Generalized Poincaré’s conjecture in dimensions greater than four.* Ann. Math. 74 (1961), 391–406.
- [21] SPIVAK, M.: *A comprehensive introduction to differential geometry*, vol. 1, 4. Brandeis Univ., Brandeis 1970, 1975.

8. John Tate získal Abelovu cenu za rok 2010

Michal Křížek, Lawrence Somer

8.1 Prolog

V roce 2010 Abelovu cenu obdržel americký matematik prof. John Tate z Texaské univerzity v Austinu za práce v oblasti algebraické teorie čísel. Dne 25. května byl přijat k audienci v královském paláci v Oslu. Poté v hlavní aule univerzity v Oslu převzal Abelovu cenu z ru-



JOHN TATE

kou norského krále Haralda V. Při této příležitosti přednesl slavnostní proslov předseda Norské akademie věd Nils Ch. Stenseth a předseda výběrové komise Kristian Seip. Další den pak pronesl prof. Tate laureátskou přednášku na téma *The arithmetic of elliptic curves*.

O eliptických křivkách pojednáme v kapitolách 8.4 a 14.4. Připomeneme i některé jejich aplikace v kryptografii.

Tateovy výsledky z teorie eliptických křivek podstatně přispěly k důkazu Velké Fermatovy věty — jednoho z nejslavnějších matematických problémů (viz např. kap. 14.1 a [15], [20], [21], [22]).

Velká Fermatova věta. *Neexistují přirozená čísla $n > 2$ a a, b, c tak, že*

$$a^n + b^n = c^n. \quad (8.1)$$

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 [25], [26]). 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.¹ Na večerním banketu pak promluvil mj. Michael Atiyah, který získal Abelovu cenu v roce 2004.

8.2 Kdo je John Tate?

John Tate se narodil 13. března 1925 v Minneapolis. Titul bakaláře získal na Harvardově univerzitě a doktorát v Princetonu. Jeho školitelem byl Emil Artin.

Profesor 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–

¹Článek [12] na podobné téma vyšel i v PMFA (viz též [27]).

Tateův parametr, Tateova stopa, Lubinova–Tateova grupa, Tateovy–Šafarevičovy grupy, Satoova–Tateova domněnka aj.

Tateovy výsledky jsou též 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 produkoval skvělé matematické výsledky více než šest desetiletí. V roce 1990 přešel na Texaskou univerzitu v Austinu. Předtím 36 let učil na Harvardově univerzitě.

J. Tate proslovil 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 v roce 1995 Steelovu cenu za celoživotní dílo. Za zmínku jistě stojí i Wolfova cena z let 2002–2003 za vytvoření fundamentálních konceptů v algebraické teorii čísel.

John Tate byl v roce 1969 zvolen do Národní akademie věd, v roce 1992 byl jmenován zahraničním členem Francouzské akademie věd a čestným členem Londýnské matematické společnosti se stal v roce 1999. Nyní se seznámíme s některými základními tvrzeními teorie čísel, protože J. Tate dosáhl nejvíce matematických výsledků právě v této disciplíně.

8.3 Stručně o teorii čísel

Teorie čísel je jednou z nejstarších vědních disciplín. Avšak teprve ve 20. století matematici objevili její obrovské množství praktických aplikací, např. při tvorbě samoopravných kódů, digitálního podpisu, algoritmů rychlého násobení, při generování pseudonáhodných čísel či šifrování tajných zpráv (viz [7]). Poznatky z teorie čísel také podstatně přispívají ke zvyšování informační bezpečnosti internetu.

Teorie čísel se zabývá vlastnostmi množin různých typů čísel, např. množiny přirozených čísel

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

Připomeňme, že přirozené číslo se nazývá *prvočíslem*, jestliže má právě dva různé dělitele (každé prvočíslo je tak dělitelné pouze sebou samým

a jedničkou). Už Eukleides (4.–3. stol. př. n. l.) uměl dokázat následující tvrzení [7, s. 53]:

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.

Za zakladatele moderní teorie čísel je považován francouzský matematik Pierre de Fermat (viz [22]). Jeho nejčastěji používaný výsledek, který má i velké množství praktických aplikací (viz [7]), lze zformulovat takto:

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

Tvrzení věty okamžitě plyne pro $p = 2, 3$, protože rozdíly $n^2 - n = n(n - 1)$ a $n^3 - n = (n + 1)n(n - 1)$ lze vyjádřit jako součin po sobě jdoucích přirozených čísel. Pro libovolné prvočíslo p existuje velké množství rozličných důkazů (viz např. [7]).

Dalším významným francouzským matematikem, který podstatně ovlivnil rozvoj teorie čísel, je Marin Mersenne.² Studoval mj. čísla tvaru

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

kde p jsou prvočísla. Čísla M_p se po něm nazývají *Mersennova čísla*. Požadavek prvočíselnosti exponentu ilustruje následující věta.

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

Největším známým prvočíslem v roce 2018 bylo Mersennovo číslo $2^{77232917} - 1$ ($\approx 10^{23249425}$). Pro srovnání uveďme, že počet atomů v pozorovatelné části vesmíru je přibližně jen 10^{80} , což je o více než 23 milionů řádů menší číslo než $M_{77232917}$. Tak velká Mersennova prvočísla dokážou matematici odhalit (známe jich už 50).

Jedním z nejkrásnějších a zároveň nejpřekvapivějších matematických výsledků počátku 21. století je následující tvrzení z roku 2004 (podrobnosti viz [5]):

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 [7].

²M. Mersenne (1588–1648) je též považován za duchovního otce Francouzské akademie věd (viz [7, s. 110]).

8.4 Eliptické křivky

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

$$y^2 = x^3 + Ax^2 + Bx + C, \quad (8.2)$$

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 (8.2) s celočíselnými koeficienty se zabýval již řecký matematik Diofantos právě pro jejich zajímavé vlastnosti.

Popíšme 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 $\circ: G \times G \rightarrow G$ 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. (8.1) a [13]) 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 konkrétní křivkou $\mathcal{C}$ danou vztahem

$$y^2 = x^3 - x + \frac{1}{4}, \quad (8.3)$$

jejíž graf se skládá ze dvou větví (viz obr. 8.1).

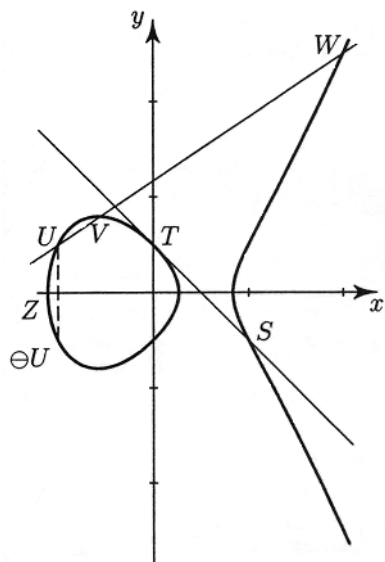
Na této křivce budeme definovat komutativní grupu bodů. Pro každý bod $U = (x, y) \in \mathcal{C}$ nejprve zavedeme inverzní prvek vztahem

$$\ominus U = (x, -y), \quad (8.4)$$

který opět leží na $\mathcal{C}$, jak plyne z (8.3). Graf na obr. 8.1 je tak symetrický podle osy x . Pokuste se nyní předem odhadnout, kde se nalézá neutrální prvek (za chvíli vám to prozradíme).

Dále popíšeme, jak budeme definovat binární grupovou operaci $\oplus$. Nechť $U, V \in \mathcal{C}$ jsou dva různé body ležící na přímkce $y = kx + q$. Potom z (8.3) dostáváme kubickou rovnici

$$(kx + q)^2 = x^3 - x + \frac{1}{4}, \quad (8.5)$$



Obr. 8.1 Komutativní grupa bodů na eliptické křivce (nakreslil P. Křížek).

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 (8.5) 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 $W \equiv V$.

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 takových bodů křivky $\mathcal{C}$ definujeme grupovou operaci $\oplus$ předpisem

$$U \oplus V = \ominus W. \quad (8.6)$$

Je ihned patrné, že tato operace je komutativní. Pomocí (8.3), (8.4), (8.5) a (8.6) si můžete sami ověřit, že např. pro bod $T = (0, \frac{1}{2})$ na obr. 8.1. platí

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

V (8.4) 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 8.1 bod $Z = \ominus Z$). Jaký bod je ale neutrálním prvkem vyšetřované grupy? Musí to být takový bod N grupy, že pro libovolné $U \in \mathcal{C}$ platí

$$N \oplus U = U \oplus N = U. \quad (8.7)$$

Co to konkrétně geometricky znamená? Body U , $\ominus U$ a N leží na jedné přímce, která je rovnoběžná s osou y . Taková přímka ale není tvaru $y = kx + q$, a proto (8.5) nelze použít. Protože však (8.7) 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 $\mathcal{C}$ neleží. Ke vztahům (8.6) a (8.7), definujícím grupovou operaci $\oplus$, je třeba ještě dodat rovnost $N \oplus N = N$.

Abychom dokázali, že body křivky (8.3), k nimž je doplněn neutrální prvek N , tvoří grupu s operací $\oplus$, zbývá ještě dokázat asociativitu grupové operace. Takový důkaz ale není snadný a přesahuje rámec tohoto výkladu.

Poznamenejme ještě (srov. [13]), že rovnici (8.6) lze ekvivalentně zapsat takto

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

8.5 Hlavní Tateovy vědecké výsledky

John Tate se během života zaměřoval především na teorii čísel a algebru. Poprvé získal mezinárodní uznání díky své vynikající doktorské dizertační práci [23] z univerzity v Princetonu z roku 1950. Tehdy mu bylo pouhých 25 let. V dizertaci studoval některé třídy algebraických těles používaných v teorii čísel. Zabýval se zejména aritmetikou speciálních rozšíření racionálních čísel, která se nazývají *číselná algebraická tělesa* a mají abelovské Galoisovy grupy nad racionálními čísly. Původní přístup k této teorii používal analytické metody zahrnující L -funkce. V roce 1936 Claude Chevalley [4] představil sofistikovanou algebraickou metodu studia těchto těles pomocí prvočísel.

J. Tate na radu svého školitele a významného číselného teoretika Emila Artina rozšířil Chevalleyův algebraický přístup pomocí analytického postupu Ericka Henckeho, který zahrnoval nový typ

L -funkcí. K tomu Tate ve své dizertační práci použil harmonickou analýzu. Nyní jsou Tateovy metody standardní částí teorie algebraických těles. Tateova dizertace také hraje důležitou roli v moderní teorii automorfních reprezentací. V letech 1951–1952 pak na slavném semináři na univerzitě v Princetonu Artin a Tate [1] představili Galoisovy kohomologie.

John Tate ve společném článku s S. Langem [9] a nezávisle též I. R. Šafarevič [19] zavedli Tateovy–Šafarevičovy grupy. Již dříve E.-C. Lind [10] a E. S. Selmer [17] předložili příklady rovnic

$$x^4 - 17 = 2y^2 \quad \text{a} \quad 3x^3 + 4y^3 + 5z^3 = 0,$$

které mají řešení v množině reálných čísel. Mají reálná řešení, i pokud je uvažujeme modulo všechny prvočíselné mocniny, ale nemají řešení v množině racionálních čísel. A právě Tateova–Šafarevičova grupa pomáhá vysvětlit tuto překvapivou vlastnost. Význačná domněnka týkající se Tateovy–Šafarevičovy grupy tvrdí, že tato grupa je vždy konečná. Speciální případy této domněnky dokázal K. Rubin [16] a V. A. Kolyvagin [6].

Diofantické 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

$$y^2 = x^3 - 43x + 166 \tag{8.8}$$

typu (8.2) 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

$$y = 3x - 1 \quad \text{a} \quad y = -3x + 1.$$

Přidáme-li k těmto bodům ještě neutrální prvek, dostaneme konečnou grupu, která je izomorfní cyklické grupě 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 (8.2) je tedy *Která z těchto rovnic má konečný počet racionálních řešení a která jich má nekonečný počet?*

A byl to právě John Tate, kdo vyvinul sofistikovanou metodu, jež pomáhá překonávat záhady eliptických křivek a rozhodovat, zda odpovídající diofantické 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,³ i když je vždy konečně generována (Mordellova věta, viz kap. 14.4).

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. Poznamenejme, že Elias Lampakis pomocí křivky

$$y^2 + x^3 = 432$$

dokázal (viz [8]), že rovnice

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

pro $xyz \neq 0$ nemá řešení v množině Gaussových celých komplexních čísel (viz obr. 8.2)

$$\mathbb{Z}[i] = \{x \in \mathbb{C}; x = x_1 + ix_2, x_1, x_2 \in \mathbb{Z}\}.$$

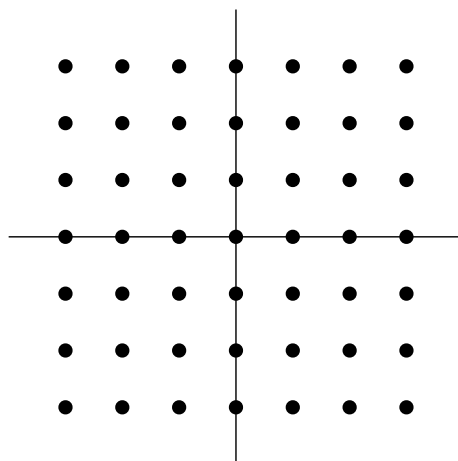
Ukažme si ještě jednoduchou aplikaci Velké Fermatovy věty (8.1). Dokážeme, že číslo $\sqrt[n]{2}$ je iracionální⁴ pro $n > 2$. Předpokládejme naopak, že

$$\sqrt[n]{2} = \frac{c}{b}$$

pro nějaká přirozená čísla c a b . Pak $2 = c^n/b^n$. Odtud plyne, že $2b^n = c^n$, což je speciálním případem (8.1), jenž podle Velké Fermatovy věty nemá řešení.

³Existují však výjimky – viz např. (8.8).

⁴Případ $n = 2$ je třeba vyšetřovat odděleně. Opět předpokládejme, že $\sqrt{2}$ je racionální číslo. Protože množina přirozených čísel je dobře uspořádaná, lze definovat číslo $k = \min\{m \in \mathbb{N}; m\sqrt{2} \in \mathbb{N}\}$. Pak ale $k(\sqrt{2} - 1) \in \mathbb{N}$, protože $k, k\sqrt{2} \in \mathbb{N}$ a $\sqrt{2} > 1$. Vidíme, že $k(\sqrt{2} - 1)\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{N}$ a $k(\sqrt{2} - 1) < k$, což je spor. Číslo $\sqrt{2}$ je proto iracionální.



Obr. 8.2 Množina Gaussových celých komplexních čísel $x = x_1 + ix_2$, kde $x_1, x_2 \in \mathbb{Z}$ a navíc $|x_j| \leq 3$ pro $i = 1, 2$ (nakreslil P. Křížek).

8.6 Tateův odkaz

John Tate se v roce 1950 ve své doktorské dizertaci [23] zabýval Fourierovou analýzou v číselných tělesech. Tím vytyčil zcela ojedinělou cestu k moderní teorii automorfních forem. Vyškolicil 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 Tanijamovy–Šimurovy domněnky,⁵ a tím pomohl A. Wilesovi a R. Taylorovi 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 dizertaci 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 [14], spolupodílel se na efektivní metodě pro testování prvočíselnosti (spoluautoři Adleman a Rumely) a na důkazu, že Carmichaelových čísel je nekonečně mnoho [7]. Profesor Tate tak měl podstatný vliv na rozvoj moderní teorie čísel i prostřednictvím svých studentů.

Sám Tate má velké množství publikací v prestižních matematických časopisech, např. v *Annals of Mathematics* ([2], [11], [18] a [24]).

⁵Viz např. PMFA 42 (1997), 169–187.

Přítom práci [18] napsal s Jean-Pierrem Serrem, který získal Abelovu cenu za matematiku jako vůbec první. J. Tate se svým bývalým školitelem Emilem Artinem napsal 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.

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 $\mathbb{Q}$: wild 3-adic exercises*. J. Amer. Math. Soc. 14 (2001), 843–939.
- [4] CHEVALLEY, C.: *Généralisation de la théorie du corps de classes pour les extensions infinies*. J. Math. Pures Appl. 15 (1936), 359–371.
- [5] KLAZAR, M.: *Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti*. PMFA 49 (2004), 177–188.
- [6] KOLYVAGIN, V. A.: *Finiteness of $E(\mathbb{Q})$ and $SH(E, \mathbb{Q})$ for a subclass of Weil curves* (in Russian). Izv. Akad. Nauk SSSR, Ser. Math. 52 (1988), 522–540, 670–671.
- [7] KRÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Academia, Praha 2009, 2011.
- [8] LAMPAKIS, E.: *In Gaussian integers $x^3 + y^3 = z^3$ has only trivial solutions – a new approach*. Electron. J. Comb. Number Theory 8 (2008), #A32.
- [9] LANG, S., TATE, J.: *Principal homogeneous spaces over abelian varieties*. Amer. J. Math. 80 (1958), 659–684.
- [10] LIND, C.-E.: *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht eins* (Thesis). Univ. of Uppsala, 1940.
- [11] LUBIN, J., TATE, J.: *Formal complex multiplication in local fields*. Ann. of Math. 81 (1965), 380–387.

- [12] MLÝNEK, J.: *Informační bezpečnost*. PMFA 51 (2006), 89–98.
- [13] NEKOVÁŘ, J.: *Modulární křivky a Fermatova věta*. Math. Bohem. 119 (1994), 79–96.
- [14] POMERANCE, C.: *Vyprávění o dvou sítích*. PMFA 43 (1998), 9–29.
- [15] RIBENBOIM, P.: *Fermat's Last Theorem for amateurs*. Springer, New York 1999.
- [16] RUBIN, K.: *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*. Invent Math. 89 (1987), 527–559.
- [17] SELMER, E. S.: *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$* . Acta Math. 85 (1951), 203–362.
- [18] SERRE, J.-P., TATE, J.: *Good reduction of abelian varieties*. Ann. of Math. 88 (1968), 492–517.
- [19] SHAFAREVICH, I. R.: *The group of principal homogeneous algebraic manifolds* (in Russian). Doklady Akad. Nauk SSSR 124 (1959), 42–43.
- [20] SINGH, S.: *Velká Fermatova věta*. Academia, Praha 2000.
- [21] SKULA, L.: *Některé historické aspekty Fermatova problému*. PMFA 39 (1994), 318–330.
- [22] ŠOLCOVÁ, A., KŘÍŽEK, M., MINK, G. (Eds): *Matematik Pierre de Fermat*. Cahiers du CEFRES No. 28, Praha, 2002.
- [23] 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.
- [24] TATE, J.: *The higher dimensional cohomology groups of class field theory*. Ann. of Math. 56 (1952), 294–297.
- [25] TAYLOR, R., WILES, A.: *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. 141 (1995), 553–572.
- [26] WILES, A.: *Modular elliptic curves and Fermat's Last Theorem*. Ann. of Math. 141 (1995), 443–551.
- [27] <http://www.dtc.umn.edu/~odlyzko>

9. Abelovu cenu za rok 2011 získal John Milnor

Michal Krížek, Martin Markl

9.1 Prolog

Dne 23. března 2011 ve 12 hodin středoevropského času prezident Norské akademie věd, Øyvind Østerud, ohlásil, že Abelovu cenu za rok 2011 získává John Willard Milnor z univerzity v Stony Brook



JOHN WILLARD MILNOR

v USA. Vzápětí laureátovi telefonovali tuto radostnou zprávu. J. Milnor byl velice potěšen, přestože jej vzbudili v 6 hodin ráno místního času. Abelova cena je totiž všeobecně považována za nejprestižnější ocenění za matematiku.

John Milnor převzal Abelovu cenu z rukou norského krále Harald V. na slavnostním shromáždění v Oslu dne 24. května 2011. Další den na univerzitě v Oslu pronesl laureátskou přednášku¹ s názvem *Sféry*, kterou uvedl rektor Ole Petter Ottersen. Po ní následovaly další tři zvané popularizační přednášky:

C. McMullen: *Variety, topologie a dynamika*,

M. Hopkins: *Bernoulliho čísla, homotopické grupy a Milnor*,

E. Ghys: *Výlet s průvodcem do sedmi rozměrů*.

Po slavnostní ceremonii se Johna Milnora ptali, zda se cítí být spíše řešitelem problémů, nebo budovatelem velkých teorií. Milnor odpověděl: *Řešitelem problémů. Nikdy jsem se nepokoušel vytvořit nějakou velkou teorii, ale snažil jsem se řešit různé drobné problémy a klást si závažné otázky. Nikdy však nevíte, co z toho může vzejít.*

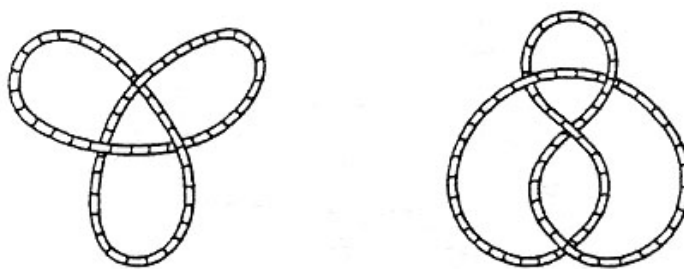
Abelova cena se uděluje za fundamentální výsledky, které významně ovlivnily matematické vědy. Podle vyjádření výběrové komise John Milnor získal cenu za objevené práce v oblasti topologie, geometrie a algebry. Významný je i jeho přínos k teorii čísel. Milnorovy myšlenky a objevy podstatně formovaly architekturu matematiky ve druhé polovině 20. století. Výběrová komise se skládala z pěti mezinárodně uznávaných matematiků. Ze závěrů jejího jednání citujeme:

Milnor je úžasně nadaný propagátor sofistikované matematiky. Často řešil závažné otázky, na něž v literatuře dosud neexistovala odpověď. Když do nich přidal svoje vlastní myšlenky, vytvořil plejádu mistrovských děl. Podobně jako hudební skladatel, který je zároveň charismatickým umělcem, je John Milnor zároveň objevitelem i propagátorem.

9.2 Vědecký životopis Johna Milnora

John Willard Milnor se narodil 20. února 1931 ve městě Orange (asi 15 km od Manhattanu) ve státě New Jersey. Studoval na univerzitě

¹Přednáška je k dispozici na webové stránce Johna Milnora, stejně jako děkovací řeč a řada fotografií.



Obr. 9.1 Schematické znázornění dvou zauzlených křivek (nakreslil P. Křížek)

v nedalekém Princetonu, kde jako osmnáctiletý dokázal následující větu z teorie uzlů, kterou publikoval v renomovaném časopise *Annals of Mathematics* v roce 1950 (viz [8]).

Fáryho–Milnorova věta. *Nechť K je uzavřená křivka v trojrozměrném eukleidovském prostoru dostatečně hladká tak, aby v každém jejím bodě existovala křivost κ . Splňuje-li celková křivost nerovnost*

$$\oint_K \kappa(s) ds \leq 4\pi, \quad (9.1)$$

*pak K není zauzlená.*²

Větu ve stejné době nezávisle vyslovil i István Fáry, jenž její důkaz publikoval v *Bulletin de la Société Mathématique de France* v roce 1949. Jestliže je tedy hladká uzavřená křivka zauzlená (srov. obr. 9.1), je její celková křivost větší než 4π . Výše uvedený odhad (9.1) je optimální v tom smyslu, že pro libovolné $\varepsilon > 0$ existuje hladká uzavřená zauzlená křivka, jejíž celková křivost je $4\pi + \varepsilon$. Poznamenejme ještě, že pro kružnici je křivkový integrál v (9.1) roven 2π .

Již v roce 1951 přešel Milnor na doktorské studium, kde byl jeho školitelem Ralph Fox. O tři roky později obhájil dizertační práci *Isotopy of Links*, v níž se zabýval klasickými uzlovými grupami³ a jejich zobecněními. Po absolvování doktorského studia pokračoval na Princetonské univerzitě a později na Ústavu pro pokročilá studia též v Princetonu (New Jersey). V roce 1989 přestoupil na univerzitu v Stony Brook v severní části Long Islandu, kde se spolupodílel na řízení Ústavu matematických věd.

²Symbol s označuje délku oblouku měřenou od nějakého daného bodu křivky.

³Uzlová grupa je fundamentální grupa doplňku uzlu v $\mathbb{R}^3$.

Milnorův nejznámější výsledek je datován rokem 1956, kdy Milnor objevil zvláštní sedmirozměrnou varietu – tzv. exotickou topologickou sféru, která má nestandardní diferenciální strukturu, a není tedy difeomorfní se standardní sférou S^7 . Podrobněji o ní pojednáme v následující kapitole. Objev Milnorovy exotické sféry byl velkým překvapením. Do roku 1956 se totiž soudilo, že všechny topologicky ekvivalentní (homeomorfní) hladké sféry jsou také hladce ekvivalentní (difeomorfní). Milnorův výsledek tak odporuje naší intuici. Od té doby vzrostl zájem topologů o vícerozměrné sféry a zejména o samotný pojem hladkosti. Citovaný výsledek se proto často pokládá za zrod nové disciplíny – diferenciální topologie.

Databáze matematických časopisů Zentralblatt a Mathematical Reviews evidují více než 150 Milnorových vědeckých prací, z toho 13 článků v časopise Annals of Mathematics. PMFA uveřejnily překlad jeho článku [13]. Od roku 1963 John Milnor napsal přes 10 monografií. Ty podstatně ovlivnily řadu jeho následovníků. Mezi Milnorovy studenty, kteří se později proslavili, patří např. Tadatoši Akiba, Jon Folkman, John Mather, Laurent C. Siebenmann, Jonathan Sondow a Michael Spivak.

John Milnor se zabývá především diferenciální a geometrickou topologií, K -teorií, dynamickými systémy, teorií komplexní proměnné, vlastnostmi Mandelbroty množiny a také lokální souvislosti Juliovy množin. Některé matematické termíny nesou jeho jméno: kromě Milnorovy exotické sféry se můžeme setkat s pojmy Milnorova fibrace, Milnorovo číslo, Milnorovo zobrazení a též „Milnor–Thurston kneading theory“.

Profesor Milnor získal během svého života celou řadu ocenění za vynikající vědecké výsledky. Připomeňme ty nejdůležitější. V roce 1962 dostal Fieldsovu medaili a vzápětí se stal editorem Annals of Mathematics, kde působil několik let. V roce 1967 obdržel Národní vyznamenání za vědu a v roce 1989 Wolfovu cenu. Je jediným matematikem, který získal tři Steelovy ceny Americké matematické společnosti za klíčový příspěvek k výzkumu (1982), za matematický výklad (2004) a celoživotní dílo (2011). V roce 1994 byl zvolen zahraničním členem Ruské akademie věd a v roce 2004 se stal řádným členem Evropské akademie věd a umění. Poznamenejme ještě, že Milnorova manželka je také profesorkou matematiky. V dalších kapitolách pojednáme o některých Milnorových výsledcích podrobněji.

9.3 Exotické sféry

John Milnor na sebe upozornil v roce 1956 překvapivou konstrukcí nestandardní hladké struktury na sedmírozměrné sféře (viz [9]). Tento výsledek má navíc výhodu určité názornosti, proto mu v následujícím přehledu věnujeme nejvíce prostoru.

Ve zbytku kapitoly bude n označovat přirozené číslo. Standardní jednotková n -rozměrná sféra $\mathbb{S}^n$ je podmnožina bodů $(x_0, \dots, x_n)$ z $(n+1)$ -rozměrného Eukleidova prostoru $\mathbb{R}^{n+1}$ vyhovujících rovnici $x_0^2 + \dots + x_n^2 = 1$. Jednorozměrná sféra je tedy jednotková kružnice a dvourozměrná sféra je povrch třírozměrné jednotkové koule. Přestože jsou sféry zdánlivě jednoduché prostory, je s nimi svázáno mnoho hlubokých vět a hypotéz. Nejslavnější je jistě Poincarého domněnka⁴ z roku 1904, dokázaná až G. Perelmanem v letech 2002–2003.

Topologická n -rozměrná sféra je topologický prostor X *homeomorfní* se standardní sférou $\mathbb{S}^n$. Připomeňme, že homeomorfismus je spojitě vzájemně jednoznačné zobrazení se spojitou inverzí. Jeho spojitost znamená, že body blízké zobrazuje na body blízké. Zdá se zřejmé, že každá hladká topologická n -rozměrná sféra X je také *difeomorfní* se standardní sférou $\mathbb{S}^n$, tedy že existuje vzájemně jednoznačné zobrazení prostoru X na prostor $\mathbb{S}^n$, které je nejen spojitě, ale má ve všech bodech derivace všech řádů. O to více překvapil Milnorův příklad sedmírozměrné hladké topologické sféry, jež *není* difeomorfní se standardní sférou $\mathbb{S}^7$. Takové sféry Milnor nazval *exotické*. Dnes se tento pojem běžně používá.

Abychom mohli formulovat Milnorův výsledek přesněji, zopakujeme si nejprve základní pojmy diferenciální topologie. Připomeňme, že *atlas* $\mathcal{A}$ na topologickém prostoru X je tvořen otevřeným pokrytím $\{U_\alpha\}_{\alpha \in A}$ prostoru X indexovaným nějakou množinou A , spolu se systémem homeomorfismů $\{\phi_\alpha\}_{\alpha \in A}$ otevřených podmnožin $U_\alpha \subset X$ na otevřené podmnožiny eukleidovského prostoru $\mathbb{R}^n$. Prostor X si můžeme představit jako krajinu pokrytou souborem map $\{U_\alpha\}_{\alpha \in A}$ sestavených do zeměpisného atlasu. Indexující množina A čísluje stránky tohoto atlasu a mapující zobrazení $\phi_\alpha : U_\alpha \hookrightarrow \mathbb{R}^n$ popisují, jak jsou příslušné části zemského povrchu zakresleny na mapy atlasu $\mathcal{A}$. Po všimněme si, že topologický prostor X s atlasem $\mathcal{A}$ je podle definice

⁴Poincarého domněnce jsou v PMFA věnovány články [2] a [15].

lokálně homeomorfní prostoru $\mathbb{R}^n$. Tvoří tedy *n-rozměrnou topologickou varietu*.⁵

Příkladem je standardní atlas $\mathcal{A}_0$ sféry $\mathbb{S}^n$. Jeho indexující množina má $2(n+1)$ -prvků,

$$A := \{(h, 0), \dots, (h, n), (d, 0), \dots, (d, n)\},$$

kde pro $0 \leq i \leq n$ je

$$U_{(h,i)} := \{(x_0, \dots, x_n) \in \mathbb{S}^n; x_i > 0\}$$

a

$$U_{(d,i)} := \{(x_0, \dots, x_n) \in \mathbb{S}^n; x_i < 0\}.$$

Označme π_i ortogonální projekci prostoru $\mathbb{R}^{n+1}$ do nadroviny

$$\{(x_0, \dots, x_n) \in \mathbb{R}^{n+1}; x_i = 0\},$$

tedy zobrazení vynechávající *i*-tou souřadnici:

$$\pi_i(x_0, \dots, x_n) := (x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{R}^n$$

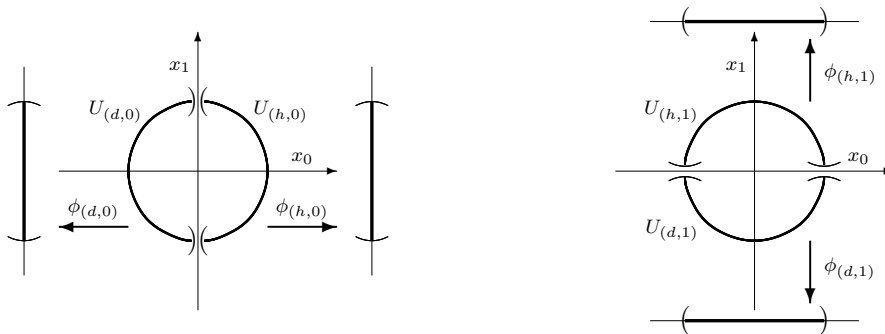
pro

$$(x_0, \dots, x_n) \in \mathbb{R}^{n+1}.$$

Mapující zobrazení $\phi_{(h,i)}$, resp. $\phi_{(d,i)}$ atlasu $\mathcal{A}_0$ jsou restrikce projekcí π_i na $U_{(h,i)}$, resp. $U_{(d,i)}$. Vše ozřejmí obrázek 9.2, ilustrující případ kružnice $\mathbb{S}^1$. Čtenář snadno nahlédne, že standardní atlas pro dvojrozměrnou sféru $\mathbb{S}^2$ má šest map: pro horní a dolní otevřenou polosféru, pro přední a zadní otevřenou polosféru a pro levou a pravou otevřenou polosféru. Všechny tyto oblasti jsou prostřednictvím mapujících zobrazení homeomorfní s otevřeným jednotkovým kruhem v rovině $\mathbb{R}^2$.

Vraťme se k atlasu $\mathcal{A}$ na topologické varietě X . Pro každou dvojici indexů $\alpha, \beta \in A$ s neprázdným průnikem $U_\alpha \cap U_\beta$ definujme *přechodové zobrazení* $\phi_{\alpha\beta}: \phi_\alpha(U_\alpha \cap U_\beta) \rightarrow \phi_\beta(U_\alpha \cap U_\beta)$ předpisem $\phi_{\alpha\beta}(x) := \phi_\beta(\phi_\alpha^{-1}(x))$ pro $x \in \phi_\alpha(U_\alpha \cap U_\beta)$, viz diagram:

⁵Obvykle se v definici topologické variety navíc předpokládá, že X je Hausdorffův prostor se spočetnouází. Tento předpoklad je v našich příkladech splněn automaticky.



Obr. 9.2 Atlas $\mathcal{A}_0$ pokrývá kružnici $\mathbb{S}^1$ čtyřmi otevřenými polokružnicemi. Mapující zobrazení jsou homeomorfismy na otevřené podintervaly $\mathbb{R}^1$ (nakreslil M. Markl).

$$\begin{array}{ccc}
 & U_\alpha \cap U_\beta & \\
 \phi_\alpha \swarrow & & \searrow \phi_\beta \\
 \mathbb{R}^n \supset \phi_\alpha(U_\alpha \cap U_\beta) & \xrightarrow{\phi_{\alpha\beta}} & \phi_\beta(U_\alpha \cap U_\beta) \subset \mathbb{R}^n.
 \end{array}$$

Přechodová zobrazení jsou zobrazeními mezi otevřenými podmnožinami $\mathbb{R}^n$. Atlas $\mathcal{A}$ je *hladký*, jestliže všechny jeho přechodové funkce jsou hladké v obvyklém smyslu, tedy mají parciální derivace všech řádů. Každý hladký atlas lze jediným způsobem doplnit do maximálního hladkého atlasu. Říkáme, že tento maximální hladký atlas definuje na X strukturu *hladké variety*.

Hladké atlasy tedy hrají v teorii hladkých variet úlohu báze otevřených množin v teorii topologických prostorů. Podobně jako jedna množina může nést mnoho bází definujících různé topologie, tak stejnou topologickou varietu může pokrývat mnoho různých, navzájem neslučitelných hladkých atlasů určujících různé hladké struktury.

V analogii se zeměpisným atlasem popisují přechodová zobrazení překrytí jednotlivých map. Zatímco u obecného atlasu se překrývají spojitě, tedy bez „roztržení“, u hladkého atlasu navíc požadujeme překrytí bez vzniku hrotů, hran a nadhran. Není těžké ověřit, že standardní atlas $\mathcal{A}_0$ sféry $\mathbb{S}^n$ je hladký. Příslušnou hladkou strukturu nazýváme *standardní hladkou strukturou sféry $\mathbb{S}^n$* .

Uvažujme homeomorfismus $f: X \rightarrow Y$ hladkých variet X a Y s hladkými atlasy $\mathcal{A} = \{\phi_\alpha, U_\alpha\}_{\alpha \in A}$, resp. $\mathcal{B} = \{\psi_\beta, V_\beta\}_{\beta \in B}$. Říkáme, že f je *hladký*, jestliže je kompozice

$$\psi_\beta \circ f \circ \phi_\alpha^{-1}: \phi_\alpha(f^{-1}(V_\beta) \cap U_\alpha) \rightarrow \psi_\beta(V_\beta)$$

hladké zobrazení otevřených podmnožin $\mathbb{R}^n$ pro každou dvojici $\alpha \in A$, $\beta \in B$, pro kterou je průnik $f(U_\alpha) \cap V_\beta$ neprázdný. Hladký homeomorfismus s hladkou inverzí se nazývá *difeomorfismus*. O varietách X a Y pak říkáme, že jsou *difeomorfní*.

Vraťme se nyní k exotické sedmirozměrné sféře. Vyjděme z kartézského součinu $\mathbb{B}^4 \times \mathbb{S}^3$ jednotkové čtyřrozměrné koule se standardní trojrozměrnou sférou a definujme prostor M_3^7 jako kvocient⁶

$$M_3^7 := (\mathbb{B}^4 \times \mathbb{S}^3 \sqcup \mathbb{B}^4 \times \mathbb{S}^3) / \sim$$

disjunktního sjednocení dvou stejných kopií $\mathbb{B}^4 \times \mathbb{S}^3$ podle relace

$$\mathbb{B}^4 \times \mathbb{S}^3 \supset \mathbb{S}^3 \times \mathbb{S}^3 \ni (a, b) \sim (a, a^2ba^{-1}) \in \mathbb{S}^3 \times \mathbb{S}^3 \subset \mathbb{B}^4 \times \mathbb{S}^3,$$

která identifikuje bod (a, b) hranice $\mathbb{S}^3 \times \mathbb{S}^3$ první kopie $\mathbb{B}^4 \times \mathbb{S}^3$ s bodem (a, a^2ba^{-1}) hranice $\mathbb{S}^3 \times \mathbb{S}^3$ druhé kopie. Přitom sféru $\mathbb{S}^3$ ztotožňujeme s jednotkovými kvaterniony a výraz a^2ba^{-1} interpretujeme v algebře kvaternionů⁷. Milnor v [9] dokázal následující větu:

Věta. *Prostor M_3^7 je homeomorfní, ne však difeomorfní sedmirozměrné sféře $\mathbb{S}^7$ se standardní hladkou strukturou.*

Volně řečeno, Milnorovu sféru M_3^7 sice můžeme homeomorfně zobrazit na standardní sféru $\mathbb{S}^7$, musíme ji však přitom „pomačkat“. Proto překvapí, že existuje homeomorfismus prostoru M_3^7 na $\mathbb{S}^7$, který je difeomorfismem všude kromě jediného bodu. Z tohoto důvodu se Milnorovým sférám někdy říká „rohaté sféry“. V roce 1963 J. Milnor společně s M. A. Kervairem v [5] dokázal, že existuje 28 různých⁸ hladkých struktur na $\mathbb{S}^7$. Jinými slovy, na sedmirozměrné sféře existuje 28 hladkých atlasů určujících 28 různých hladkých struktur.

Než uvedeme další výsledek zmíněného článku, připomeňme, že *souvislé sjednocení* $X' \# X''$ dvou hladkých n -rozměrných variet je varieta vzniklá vyříznutím malých n -rozměrných koulí z variet X' a X'' a ztotožněním takto vzniklých hraničních sfér. Definujme *monoid hladkých struktur* na n -rozměrné sféře jako soubor tříd difeomorfních orientovaných hladkých variet homeomorfních se sférou $\mathbb{S}^n$. Struktura

⁶V české literatuře se používá nepěkný a nesprávný termín „faktorprostor“.

⁷Kvaterniony se v PMFA zabývá např. článek [1]. Podotkněme, že Milnorův původní popis prostoru M_3^7 se formálně liší od našeho. Výsledek je však stejný.

⁸Dvě hladké struktury považujeme za různé, jestliže se na sebe nedají převést homeomorfismem.

monoidu je dána operací souvislého sjednocení, přitom standardní n -rozměrná sféra $\mathbb{S}^n$ tvoří jednotku. V práci [5] je dokázáno, že pro $n \neq 3, 4$ je zmíněný monoid konečná abelovská grupa. Její řád je pro $n \leq 18$ uveden v následující tabulce z velké části také převzaté z [5]:

dimenze n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
řád grupy	1	1	1	?	1	1	28	2	8	6	992	1	3	2	16 256	2

Dodnes se neví, zdali existují čtyřrozměrné exotické sféry. Proto jsme na odpovídajícím místě ponechali otazník. Tvrzení, že $\mathbb{S}^4$ nese jedinou hladkou strukturu, je známo jako *hladká Poincarého domněnka* (viz [3]). Z mnoha hledisek jsou dimenze 3 a 4 nejobtížnější. Z jiného pohledu o tom v PMFA pojednávají články [2, s. 268] a [6, s. 52].

Poznamenejme, že existují topologické variety nemající *žádnou* hladkou strukturu. První příklad sestrojil v roce 1960 M. A. Kervaire v práci [4] za použití konstrukce, kterou Milnor publikoval o rok dříve v [10].

9.4 Ostatní výsledky

V této kapitole krátce uvedeme některé další Milnorovy výsledky, z prostorových důvodů již bez nároků na vysokou přesnost výkladu.

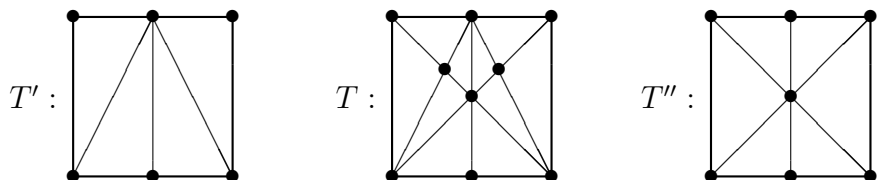
1) *Hauptvermutung*

Připomeňme, že n -rozměrný *standardní simplex* Δ^n je konvexní obal souřadnicových vektorů $\{e_0, \dots, e_n\} \subset \mathbb{R}^{n+1}$. Můžeme jej také definovat jako množinu

$$\Delta^n := \{(x_0, \dots, x_n) \in \mathbb{R}^{n+1}; x_i \geq 0 \text{ pro } 0 \leq i \leq n \text{ a } x_0 + \dots + x_n = 1\}.$$

Tedy Δ^0 je bod, Δ^1 uzavřený interval, Δ^2 trojúhelník a Δ^3 je čtyřstěn. Topologický prostor X je *triangulovatelný*, jestliže je možné jej pokrýt standardními simplexy tak, aby jejich průniky byly buď prázdné, nebo byly opět simplexem. Takové pokrytí se nazývá *triangulací* prostoru X . Daný topologický prostor může mít několik triangulací, jak vidíme na obrázku 9.3, ukazujícím tři různé triangulace čtverce.

Triangulace T' sestává ze čtyř 2-simplexů, devíti 1-simplexů a šesti 0-simplexů. Triangulace T má deset 2-simplexů, osmnáct 1-simplexů a devět 0-simplexů. Konečně triangulace T'' je tvořena šesti 2-simplexy, dvanácti 1-simplexy a sedmi 0-simplexy.



Obr. 9.3 Tři triangulace čtverce (nakreslil M. Markl)

Triangulace T_1 prostoru X je *zjemněním* triangulace T_2 , jestliže je každý simplex triangulace T_1 obsažen v nějakém simplexu triangulace T_2 . Na našem obrázku je triangulace T společným zjemněním triangulací T' a T'' . *Hauptvermutung* (česky hlavní domněnka) geometrické topologie tvrdí, že libovolné dvě triangulace stejného topologického prostoru mají společné zjemnění.

V [11] Milnor ukázal, že kónus nad kartézským součinem čočkového prostoru⁹ s hranicí třírozměrného simplexu má dvě konečné triangulace bez společného zjemnění. Tím sestrojil *protipříklad* k Hauptvermutungu. Povšimněme si, že tento výsledek má podobnou příchut' jako konstrukce exotické sféry. Opět jsme v situaci, kdy daný topologický prostor nese jemnější strukturu (hladký atlas v předchozím, triangulace v tomto případě), a ptáme se, nakolik je tato jemná struktura determinována topologií. Výsledky uvedené ve zbytku této kapitoly publikoval J. Milnor v knize [12].

2) Milnorovo číslo

Uvažujme komplexní funkci g v n komplexních proměnných, holomorfní na nějakém otevřeném okolí bodu $\xi = (\xi_1, \dots, \xi_n) \in \mathbb{C}^n$. Připomeňme, že bod ξ je *singulárním bodem* funkce g , jestliže se v něm nulují parciální derivace prvního řádu ve všech směrech. V opačném případě říkáme, že ξ je *regulární*. Singulární bod ξ je *izolovaný*, jestliže je jediným singulárním bodem v nějakém svém okolí. Konečně singulární bod ξ je *degenerovaný*, jestliže se v něm nuluje determinant *Hessiánu* funkce g , což je matice druhých derivací

$$\left[\frac{\partial^2 g}{\partial z_i \partial z_j} \right]_{1 \leq i, j \leq n}.$$

Následující výklad zaměříme na funkce se singulárním bodem

⁹Čočkový prostor (angl. lens space) je kvocient třírozměrné sféry $\mathbb{S}^3$ podle akce specifické cyklické grupy.

v počátku $\mathbf{0} := (0, \dots, 0)$ a s nulovou funkční hodnotou v tomto bodě. Příklad obecného singulárního bodu a obecné funkční hodnoty převedeme na tento speciální případ posunutím.

Označme tedy $\mathcal{O}$ okruh holomorfních funkcí f definovaných na nějakém otevřeném okolí počátku $\mathbf{0}$ prostoru $\mathbb{C}^n$ a takových, že $f(0, \dots, 0) = 0$. Pro každou $f \in \mathcal{O}$ vezměme ideál J_f algebry $\mathcal{O}$ generovaný parciálními derivacemi funkce f a označme $\mathcal{A}_f := \mathcal{O}/J_f$ kvocientovou algebru. *Milnorovo číslo* $\mu(f)$ funkce f v bodě $\mathbf{0}$ je komplexní dimenze¹⁰ komplexního vektorového prostoru $\mathcal{A}_f$,

$$\mu(f) := \dim_{\mathbb{C}}(\mathcal{A}_f).$$

Z definice plyne, že $\mu(f)$ je buď celé nezáporné číslo, nebo nekonečno. Přitom $\mu(f) = 0$, pokud je $\mathbf{0}$ regulárním bodem funkce f , a $\mu(f) = 1$, pokud je $\mathbf{0}$ nedegenerovanou singularitou. Dále platí, že $\mu(f)$ je konečné právě tehdy, když je $\mathbf{0}$ izolovaným singulárním bodem.

Důležitost Milnorova čísla tkví v jeho alternativních interpretacích. Předpokládejme, že $\mathbf{0}$ je izolovaný singulární bod funkce f . Pro $a = (a_1, \dots, a_n) \in \mathbb{C}^n$ definujme perturbaci f_a funkce f předpisem

$$f_a(\xi_1, \dots, \xi_n) := f(\xi_1, \dots, \xi_n) + a_1\xi_1 + \dots + a_n\xi_n.$$

Ukazuje se, že pro dostatečně malá a se izolovaný singulární bod $\mathbf{0}$ funkce f rozpadá na izolované *nedegenerované* singulární body perturbace f_a . Jejich počet je roven $\mu(f)$.

Milnorovo číslo má i topologickou charakterizaci. Symbolem $\mathbb{S}_{\varepsilon}^{2n-1}$ označme $(2n-1)$ -rozměrnou sféru v $\mathbb{C}^n$ o poloměru ε se středem v počátku. Pokud opět předpokládáme, že $\mathbf{0}$ je izolovaný singulární bod funkce f , pak pro dostatečně malá ε předpis

$$\psi(\xi) := \frac{\left(\frac{\partial f}{\partial z_1}(\xi), \dots, \frac{\partial f}{\partial z_n}(\xi)\right)}{\sqrt{\left|\frac{\partial f}{\partial z_1}(\xi)\right|^2 + \dots + \left|\frac{\partial f}{\partial z_n}(\xi)\right|^2}}$$

definuje spojitě zobrazení $\psi : \mathbb{S}_{\varepsilon}^{2n-1} \rightarrow \mathbb{S}^{2n-1}$. Milnorovo číslo $\mu(f)$ je rovno *stupni* tohoto zobrazení. To je homotopický invariant vyjadřující, kolikrát ψ „omotá“ sféru $\mathbb{S}^{2n-1}$ sférou $\mathbb{S}_{\varepsilon}^{2n-1}$.

¹⁰Jde o celé číslo, jehož dvojnásobek je dimenze reálná.

3) Milnorova fibrace

Připomeňme, že lokálně triviální hladká fibrace $p: E \rightarrow B$ je zobrazení hladkých variet, které je lokálně projekcí $B \times F \rightarrow B$, kde F je hladká varieta nazývaná *fíbr* p . Přesnou definici lokality nebudeme uvádět. Je formulována pomocí otevřeného pokrytí variety B a má podobný charakter jako definice hladkého atlasu z kapitoly 9.3.

Předpokládejme, že $f: \mathbb{C}^n \rightarrow \mathbb{C}$ je nenulový komplexní polynom splňující $f(0, \dots, 0) = 0$. Označme $\mathfrak{Z}_f$ nulovou množinu polynomu f ,

$$\mathfrak{Z}_f := \{(z_1, \dots, z_n) \in \mathbb{C}^n; f(z_1, \dots, z_n) = 0\}.$$

Tedy $\mathfrak{Z}_f$ je komplexní nadplocha dimenze $n - 1$ obsahující počátek $\mathbf{0}$. *Argument* funkce f je definován v bodech $\xi \in \mathbb{C}^n$ neležících v $\mathfrak{Z}_f$ předpisem

$$\text{Arg}_f(\xi) := \frac{f(\xi)}{|f(\xi)|} \in \mathbb{S}^1.$$

Milnor dokázal, že pro dostatečně malá ε je restrikce

$$\text{Arg}_f: \mathbb{S}_\varepsilon^{2n-1} \setminus \mathfrak{Z}_f \rightarrow \mathbb{S}^1$$

lokálně triviální hladká fibrace, jejíž fíbr je varieta dimenze $2n - 2$. V případě, že $\mathbf{0}$ je izolovaný singulární bod, má tento fíbr homotopický typ¹¹ sjednocení $\mathbb{S}^{n-1} \vee \dots \vee \mathbb{S}^{n-1}$ se ztotožněnými báзовými body určitého počtu standardních $(n - 1)$ -rozměrných sfér.

John Milnor se proslavil učebnicí [14], kterou napsal společně s Jimem Stasheffem. Její četba je požitek, stejně jako četba všeho, na čem se Milnor podílel. Martin Markl (druhý autor této kapitoly) později s Jimem napsal několik článků a monografii [7].

L i t e r a t u r a

- [1] BEČVÁŘ, J.: *150 let od objevu kvaternionu*. PMFA 38 (1993), 305–317.
- [2] CIPRA, B.: *Jeden ze sedmi problémů tisíciletí se přibližuje k úplnému vyřešení*. PMFA 55 (2010), 265–277.

¹¹Zhruba řečeno, topologické prostory mají stejný homotopický typ, pokud se neliší až na spojitou deformaci.

- [3] FREEDMAN, M., GOMPF, R., MORRISON, S., WALKER, K.: *Man and machine thinking about the smooth 4-dimensional Poincaré conjecture*. Quantum Topology 1(2) (2010), 171–208.
- [4] KERVAIRE, M. A.: *A manifold which does not admit any differentiable structure*. Comment. Math. Helv. 34 (1960), 257–270.
- [5] KERVAIRE, M. A., MILNOR, J.: *Groups of homotopy spheres: I*. Ann. of Math. (2) 77(3) (1963), 504–537.
- [6] KRÍŽEK, M., ŠOLC, J.: *Od Keplerových mozaik k pětičetné symetrii*. PMFA 54 (2009), 41–56.
- [7] MARKL, M., SHNIDER, S., STASHEFF, J.: *Operads in algebra, topology and physics*. Math. Surveys and Monographs 96, Amer. Math. Soc., Providence, Rhode Island 2002.
- [8] MILNOR, J.: *On the total curvature of knots*. Ann. of Math. (2) 52(2) (1950), 248–257.
- [9] MILNOR, J.: *On manifolds homeomorphic to the 7-sphere*. Ann. of Math. (2), 64(2) (1956), 399–405.
- [10] MILNOR, J.: *Differentiable structures on spheres*. Amer. J. Math. 81 (1959), 962–972.
- [11] MILNOR, J.: *Two complexes which are homeomorphic but combinatorially distinct*. Ann. of Math. (2) 74(3) (1961), 575–590.
- [12] MILNOR, J.: *Singular points of complex hypersurfaces*. Ann. of Math. Stud. 61, Princeton Univ. Press, Princeton, New Jersey 1968.
- [13] MILNOR, J.: *Nobelova cena pro Johna Nashe*. PMFA 41 (1996), 169–179.
- [14] MILNOR, J., STASHEFF, J.: *Characteristic classes*. Ann. of Math. Stud. 76, Princeton Univ. Press, Princeton, New Jersey 1974.
- [15] SMALE, S.: *Příběh Poincarého hypotézy ve vyšších dimenzích*. PMFA 36 (1991), 38–49.

10. Maďarský matematik Endre Szemerédi získal Abelovu cenu za rok 2012

Michal Křížek, Pavel Pudlák, Lawrence Somer

10.1 Prolog

V roce 2012 putovala Abelova cena za matematiku do Maďarska k prof. Endre Szemerédimu, který ji dostal za své fundamentální objevy v diskrétní matematice a teoretické informatice a jejich dlouho-



ENDRE SZEMERÉDI

trvajícím vlivům na aditivní teorii čísel a ergodickou teorii. Dalším matematikem maďarského původu, který tuto nejprestižnější cenu za matematiku získal v roce 2005, se stal Peter Lax. Matematika v Maďarsku má totiž dlouholetou tradici. Vzpomeňme na několik dalších významných maďarských matematiků světového významu, jakými byli např. János Bolyai, Lipót Fejér, Marcel Grossmann, Alfréd Haar, András Hajnal, Cornelius Lanczos, László Lovász, John von Neumann, Rózsa Péterová, George Pólya, Alfréd Rényi, Marcel Riesz, Endre Süli, Pál Turán a jeho manželka Vera T. Sóssová, Karl Zsigmondy a též Pál Erdős, který má v databázi Mathematical Reviews registrováno přes 1 500 vědeckých prací. Jen málo zemí velikosti Maďarska může předvést podobný seznam. Maďaři se navíc mohou pochlubit 13 nositeli Nobelových cen.

Profesor Endre Szemerédi převzal Abelovu cenu z rukou norského krále Haralda V. dne 22. května 2012 v hlavní aule univerzity v Oslu. Při této příležitosti přednesli slavnostní proslov norská ministryně pro školství a vědu Kristin Halvorsenová, předseda Norské akademie věd Nils Ch. Stenseth a předseda výběrové komise Ragni Piene (viz [20]).

O den později pak byly prosloveny 4 abelovské přednášky. V úvodní přehledové přednášce *Randomness and Pseudorandomness*, určené pro širší veřejnost, prof. Avi Wigderson z Ústavu pro pokročilá studia v Princetonu vyzdvihl Szemerédiův přínos k teorii pseudonáhodných čísel. Pak sám prof. Szemerédi přednesl hlavní laureátskou přednášku na téma *In Every Chaos There is an Order*, v níž popsal historii a současnost Szemerédiový věty, které se budeme věnovat v kapitole 10.3. Další dvě abelovské přednášky pronesli László Lovász: *The Many Facets of the Regularity Lemma* a známý britský kombinatorik a nositel Fieldsovy medaile Timothy Gowers:¹ *The Afterlife of Szemerédi's Theorem*.

10.2 Stručný životopis

Profesor Endre Szemerédi se narodil 21. srpna 1940 v Budapešti, kde později vystudoval Univerzitu Loranda Eötvöse. Titul kandidáta věd získal na Moskevské státní univerzitě. Jeho školitelem byl slavný ma-

¹V nakladatelství Dokořán vyšel v roce 2006 překlad knihy T. Gowerse: *Matematika. Průvodce pro každého*. Gowers ji napsal prý hlavně pro svoji ženu, aby věděla, čím se on – matematik – v práci zabývá.

tematik Israel Gelfand. Za své klíčové výsledky z teorie čísel, kombinatoriky a teoretické informatiky Szemerédi získal celou řadu prestižních ocenění: Grünwaldovu cenu (1967, 1968), Rényiho cenu (1973), Pólyovu cenu za aplikovanou matematiku (SIAM 1975), Cenu Maďarské akademie věd (1979), Cenu Rolfa Schocka za matematiku (2008), Steelovu cenu Americké matematické společnosti (2008).

Připomeňme ještě, že prof. Szemerédi navštívil Prahu v roce 2010, když mu Univerzita Karlova udělila čestný doktorát. V současnosti pracuje v Matematickém ústavu Alfréda Rényiho Maďarské akademie věd v Budapešti. Je též zaměstnán na Státní univerzitě v New Jersey (Rutgers Department of Computer Science). Současně je členem věhlasného Ústavu pro pokročilá studia v Princetonu. Endre Szemerédi je ženatý a má pět dětí.

10.3 Aditivní teorie čísel

V této části se soustředíme na nejznámější Szemerédiový výsledek z aditivní teorie čísel, z teorie grafů a teoretické informatiky. Aditivní teorie čísel se věnuje studiu podmnožin celých čísel a jejich vlastností při sčítání (viz [11] a [12]). Jako příklad uveďme známou **Goldbachovu hypotézu**:

Každé sudé číslo větší než 2 lze napsat jako součet dvou prvočísel.

Tato domněnka dodnes není dokázána. Vznikla během vzájemné korespondence mezi Eulerem a Goldbachem v roce 1742 (např. vidíme, že $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5 = 3 + 7$). Podle některých pramenů ji poprvé vyslovil Euler inspirován Goldbachem. V roce 1937 ruský matematik Ivan Matvejevič Vinogradov (1891–1983) dokázal, že existuje přirozené číslo n_0 tak, že každé liché $n > n_0$ lze vyjádřit jako součet tří prvočísel (viz [19]). Navíc nedávno Terence Tao dokázal, že každé liché číslo větší než jedna je součtem nejvýše pěti prvočísel [18].

V roce 1973 čínský matematik Ťing-žun Čchen dokázal, že každé dostatečně velké sudé číslo je součtem prvočísla a součinu nejvýše dvou prvočísel (viz [8]). Tato věta se zatím považuje za nejlepší výsledek týkající se Goldbachovy hypotézy. Jiná Čchenova věta tvrdí, že pro každé sudé číslo s existuje nekonečně mnoho prvočísel p tak, že $p + s$ je buď prvočíslu, nebo součin dvou prvočísel.

Dalším příkladem z aditivní teorie čísel je Waringův problém,

který formuloval Edward Waring (1734–1798) kolem roku 1770. Pro dané přirozené číslo k označme

$$A_k = \{0^k, 1^k, 2^k, 3^k, \dots\}$$

množinu k -tých mocnin. Ve *Waringově problému* jde o určení nejmenšího h tak, aby se každé přirozené číslo n dalo napsat ve tvaru

$$n = \sum_{m=1}^h a_m, \quad a_m \in A_k.$$

Pravděpodobně již Diofantos znal následující tvrzení:

Věta. *Každé přirozené číslo je součtem čtyř čtverců.*

Tuto tzv. *čtyřčtvercovou větu*² dokázal až Joseph Louis Lagrange v roce 1770. Pro $k = 2$ můžeme tedy volit $h = 4$ a snadno ověříme, že h nelze zmenšit (stačí uvažovat např. $n = 7 = 1^2 + 1^2 + 1^2 + 2^2$).

Pro dané přirozené číslo k označme $g(k)$ nejmenší počet k -tých mocnin čísel $0, 1, 2, \dots$, jejichž součtem lze vyjádřit jakékoliv přirozené číslo. Zřejmě $g(1) = 1$ a podle čtyřčtvercové věty je $g(2) = 4$. Číslo

$$23 = 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 2^3 + 2^3$$

lze vyjádřit jako součet devíti třetích mocnin nezáporných celých čísel a snadno nahlédneme, že tento počet nelze snížit. Podobně zjistíme, že číslo 79 lze vyjádřit pomocí součtu 19 čtvrtých mocnin, ale nelze je vyjádřit jejich menším počtem. Tedy $g(3) \geq 9$ a $g(4) \geq 19$. Roku 1909 Arthur Wieferich [19] odvodil, že $g(3) = 9$, a v roce 1986 Ramačandran Balasubramanian a kol. [3] dokázali, že $g(4) = 19$. Dnes víme, že $g(5) = 37$ (viz [7]) a $g(6) = 73$ (viz [13]). Pro obecné k řešení Waringova problému dosud není známo, i když se zdá, že $g(k) = 2^k - 2 + \lfloor (3/2)^k \rfloor$, kde $\lfloor r \rfloor$ označuje celou část reálného čísla r .

Nyní se soustředíme na van der Waerdenova čísla, kterými se rovněž zabývá aditivní teorie čísel. Ukážeme si, jak se tato čísla zavádějí pomocí různě obarvených přirozených čísel. Pro jednoduchost uveďme jen jeden ilustrační příklad.

Každé přirozené číslo obarvíme buď červenou, anebo modrou barvou. Pak snadno nahlédneme, že posloupnost $1, 2, \dots, 9$ obsahuje aritmetickou podposloupnost stejné barvy a délky 3.

²Např. $1634 = 1^2 + 9^2 + 16^2 + 36^2$.

Pokusme se dokázat opak, tj. předpokládejme, že posloupnost $1, 2, \dots, 9$ neobsahuje aritmetickou podposloupnost stejné barvy a délky 3. Tedy 1, 5 a 9 nemají stejnou barvu. V dalším budeme červená čísla podtrhávat a modrá čísla budeme psát s pruhem nahoře. Rozlišujeme dva případy:

1. Nechť $\underline{1}$ a $\underline{5}$ jsou obarveny červeně a $\overline{9}$ modře. Protože $\underline{1}$ a $\underline{5}$ jsou obarveny červeně, musí být číslo $\overline{3}$ modré. Číslo $\overline{9}$ je však modré, a proto $\underline{6}$ musí být červené. Jelikož čísla $\underline{5}$ a $\underline{6}$ jsou červená, jsou $\overline{4}$ a $\overline{7}$ modrá. Číslo $\underline{8}$ musí být však červené, protože $\overline{7}$ a $\overline{9}$ jsou modrá. Protože $\overline{3}$ a $\overline{4}$ jsou modrá, musí být $\underline{2}$ červené. Pak ale aritmetická posloupnost $\underline{2}, \underline{5}$ a $\underline{8}$ obsahuje jen červená čísla, což je spor.

2. Příklad, že čísla $\underline{1}$ a $\underline{9}$ jsou červená a $\overline{5}$ je modré, vede ke sporu podobným způsobem.

Dále vidíme, že posloupnost $\underline{1}\overline{2}\underline{3}\overline{4}\underline{5}\overline{6}\overline{7}\underline{8}$ neobsahuje stejně obarvenou aritmetickou podposloupnost délky 3. Tedy počet členů 9 je nejmenší možný pro výše uvedený příklad. Přitom se nemusí jednat jen o posloupnost $1, 2, \dots, 9$, ale o jakoukoliv posloupnost po sobě jdoucích celých čísel o devíti členech. Pomocí výše uvedeného postupu lze zavést van der Waerdenovo číslo $W(2, 3) = 9$ odpovídající dvěma barvám a aritmetickým posloupnostem délky 3. Podobně se zavádějí i další van der Waerdenova čísla.

10.4 Szemerédiova věta

Szemerédiova věta, která zobecňuje vlastnosti van der Waerdenových čísel, je jedním z nejkrásnějších výsledků aditivní teorie čísel. Než ji vyslovíme, uvedeme několik okolností, jež vedly k jejímu vzniku.

V roce 1936 Erdős a Turán vyslovili následující hypotézu [5] (jejíž tvrzení ze Szemerédiový věty plyne):

Pro každé $d \in (0, 1]$ a přirozené číslo k existuje n_0 tak, že pro všechna $n \geq n_0$ každá podmnožina $\mathbb{B} \subset \{1, \dots, n\}$, jejíž mohutnost je alespoň dn , obsahuje aritmetickou posloupnost délky k .

Pro libovolnou podmnožinu $\mathbb{B}$ množiny přirozených čísel $\mathbb{N} = \{1, 2, 3, \dots\}$ definujeme *horní asymptotickou hustotu* $\mathbb{B}$ následovně

$$\overline{d}(\mathbb{B}) = \limsup_{n \rightarrow \infty} = \frac{|\mathbb{B} \cap \{1, 2, \dots, n\}|}{n},$$

kde $|\cdot|$ označuje počet prvků.

Uveďme nejprve několik triviálních příkladů. Jestliže $\mathbb{B}$ je množina sudých čísel, pak její horní asymptotická hustota je $1/2$. Je-li $\mathbb{B} = \{1, 2, \dots, 10\}$, pak horní asymptotická hustota $\mathbb{B}$ je nula. Rovněž pro

$$\mathbb{B} = \{1, 10, 100, 1000, \dots\}$$

je horní asymptotická hustota nulová.

V roce 1953 Klaus Friedrich Roth dokázal následující tvrzení.

Rothova věta. *Každá podmnožina $\mathbb{B} \subset \mathbb{N}$, jejíž horní asymptotická hustota je kladná, obsahuje aritmetickou posloupnost délky 3.*

V roce 1969 Szemerédi zvýšil tento počet na 4 a v roce 1975 pak dokázal překvapivou větu (viz [16]):

Szemerédiva věta. *Každá podmnožina $\mathbb{B} \subset \mathbb{N}$ s kladnou horní asymptotickou hustotou obsahuje aritmetickou posloupnost libovolné délky.*

Již v roce 1973 Pál Erdős formuloval silnější tvrzení, které ovšem dodnes není dokázáno:

Erdősova–Turánova domněnka. *Necht' součet převrácených hodnot prvků z množiny $\mathbb{B} \subset \mathbb{N}$ je větší než jakékoliv přirozené číslo. Pak $\mathbb{B}$ obsahuje aritmetickou posloupnost libovolné délky.*

V roce 2004 Ben Green a Terence Tao dokázali, že množina prvočísel obsahuje aritmetické posloupnosti libovolné délky (viz též kap. 8.3). Jedná se tedy o důležitou speciální část Erdősovy–Turánovy domněnky pro případ, že $\mathbb{B} = \mathbb{P}$ je množina prvočísel (viz [6], [10]). Kdyby tato domněnka byla pravdivá, pak by výsledek Greena a Taa byl jejím důsledkem, protože

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty.$$

V tomto případě Szemerédiovu větu nelze použít, neboť horní asymptotická hustota množiny $\mathbb{P}$ všech prvočísel je nula.

10.5 Erdősova–Szemerédiva věta

V roce 1983 Endre Szemerédi publikoval s Pálem Erdősem mírně modifikovanou větu uvedenou níže (viz [4]).

Nejprve však zavedeme následující označení. Pro konečnou podmnožinu A množiny reálných čísel položíme

$$A + A = \{a + b; a, b \in A\}, \quad A \cdot A = \{ab; a, b \in A\}.$$

Erdősova–Szemerédiova věta. *Existují kladné reálné konstanty C a ε tak, že pro každou konečnou a neprázdnou podmnožinu A množiny reálných čísel platí*

$$\max(|A + A|, |A \cdot A|) \geq C|A|^{1+\varepsilon}.$$

Všimněme si, že velikost $A + A$ je srovnatelná s A , je-li A tvořena konečnou aritmetickou posloupností. Na druhé straně, je-li A tvořena konečnou geometrickou posloupností, pak zase $A \cdot A$ má velikost srovnatelnou s A . Je-li A dostatečně velká, pak se nemůže současně podobat aritmetické i geometrické posloupnosti. Erdős a Szemerédi navíc vyslovili domněnku, že číslo ε může být libovolně blízko 1. József Solymosi [15] později dokázal, že ε může být libovolně blízko $1/3$.

10.6 Szemerédiovo lemma o regularitě

Nejprve definujeme několik pojmů. Nechť G je (konečný) graf. *Hustotou páru dvou disjunktních podmnožin jeho vrcholů X a Y* nazveme číslo

$$\rho(X, Y) = \frac{|E(X, Y)|}{|X||Y|},$$

kde $|\cdot|$ opět označuje počet prvků (kardinalitu) a $E(X, Y)$ je množina hran, které mají jeden vrchol v X a druhý v Y .

Nechť $\varepsilon > 0$ je dáno. Pár dvou disjunktních podmnožin vrcholů X a Y grafu G nazveme *ε -pseudonáhodný* (ε -regulární), jestliže pro všechny podmnožiny $A \subset X$ a $B \subset Y$ splňující nerovnosti $|A| \geq \varepsilon|X|$ a $|B| \geq \varepsilon|Y|$ platí

$$|\rho(X, Y) - \rho(A, B)| \leq \varepsilon.$$

Jinými slovy, hustota $\rho(X, Y)$ se příliš neliší od hustoty $\rho(A, B)$ párů svých podmnožin.

Rozklad množiny vrcholů grafu G na k podmnožin $V_1, \dots, V_k$ se nazývá *ε -rozklad*, jestliže

$$||V_i| - |V_j|| \leq 1 \text{ pro všechna } i \text{ a } j \quad (10.1)$$

a všechny páry $V_i, V_j, i < j$, jsou ε -pseudonáhodné kromě nejvýše εk^2 párů.

Následující lemma je dokázáno v [17].

Lemma o regularitě. *Pro každé $\varepsilon > 0$ a přirozené číslo m existuje přirozené číslo M takové, že když G je graf s alespoň m vrcholy, pak existuje přirozené číslo k v intervalu $m \leq k \leq M$ a ε -rozklad vrcholů grafu G na k podmnožin.*

Szemerédiovo lemma o regularitě zhruba tvrdí, že každý dostatečně velký graf lze rozdělit na podmnožiny, které mají přibližně stejnou velikost, tj.

$$|V_1| \leq |V_2| \leq \dots \leq |V_k| \leq |V_1| + 1$$

(srov. (10.1)), přičemž hrany mezi různými podmnožinami jsou rozloženy téměř náhodně. Pro každé k takový rozklad vždy existuje. Při praktických aplikacích se často uvažuje rozklad speciálních grafů na podmnožiny stejné velikosti (tj. v (10.1) platí ostrá nerovnost).

Brzy po publikaci Szemerédiho lemmatu o regularitě se ukázalo, že je lze použít na jednoduchý důkaz Rothovy věty (viz kap. 10.3). Tím se objevila přirozená otázka, zda by se Szemerédiovo lemma nedalo zobecnit tak, aby z něj plynula Szemerédiho věta v celé obecnosti. Na to bylo potřeba zobecnit Szemerédiovo lemma na hypergrafy.³ To je poměrně netriviální záležitost, která se teprve nedávno podařila Vojtěchu Rödlvi a jeho studentům a nezávisle také T. Gowersovi.

10.7 Szemerédiho práce v teoretické informatice

Endre Szemerédi se proslavil také výsledky v teoretické informatice. Většina těchto prací vznikla ve spolupráci s Miklósem Ajtaiem a Jánosem Komlósem. Jeden z nejznámějších výsledků, který vznikl při této spolupráci, je tzv. *AKS třídící síť*, pojmenovaná podle počátečních písmen autorů článku [1].

V informatice se často používají algoritmy na třídění. Jde o úlohu, kde je zadána posloupnost prvků $(a_1, \dots, a_n)$ nějaké uspořádané množiny a cílem je tuto posloupnost přerovnat tak, aby v ní byly prvky

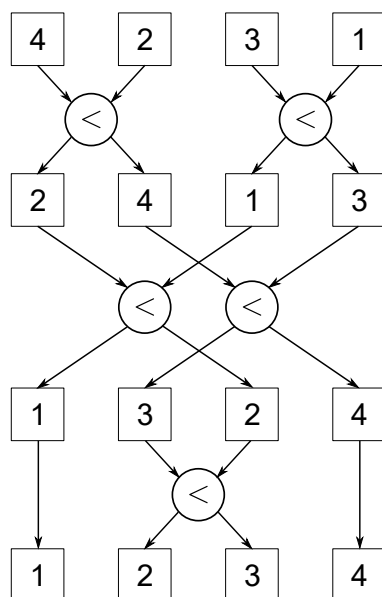
³V grafu jsou spojeny některé dvojice vrcholů hranou, zatímco hypergraf dává do souvislosti trojice, čtveřice, pětičky, ... vrcholů.

ve vzestupném pořadí. Bez újmy na obecnosti můžeme předpokládat, že zadaná posloupnost je permutací konečné posloupnosti $1, 2, \dots, n$.

Třídící algoritmus (sít') je posloupnost k kroků, kde každý krok je pevně daná množina vzájemně disjunktních dvojic indexů z množiny $\{1, 2, \dots, n\}$. Tento algoritmus se na vstupní permutaci $a_1 a_2 \dots a_n$ čísel $1, 2, \dots, n$ aplikuje takto:

V každém kroku se zvolí množina disjunktních dvojic indexů. Pro každou z těchto dvojic se příslušná čísla porovnají a zamění se, pokud nejsou ve vzestupném pořadí. Důležité je, že dvojice pro každý krok jsou zvoleny předem, nezávisle na tom, jakou posloupnost třídíme. Proto lze tento algoritmus znázornit jako síť. Počet kroků potom odpovídá hloubce sítě. Na obr. 10.1 je jednoduchý ilustrační příklad třídící sítě $n = 4$ (není to AKS síť, protože tu lze vytvářet jen pro větší n).

Je snadné dokázat, že každá třídící síť musí mít hloubku alespoň $\log_2 n$. Třídící síť si totiž můžeme představit jako způsob, jak



Obr. 10.1 Příklad třídící sítě a jejího použití na přerovnání posloupnosti 4, 2, 3, 1 podle velikosti. Kroužky jsou označeny bloky, v nichž se rozhoduje, zda je třeba dané dva vstupní údaje prohodit podle velikosti. Stejná síť srovná podle velikosti libovolnou posloupnost délky 4 se vzájemně různými prvky (nakreslil P. Pudlák).

realizovat permutaci. Pro každou permutaci můžeme přiřadit rozhodovacím blokům sítě nuly a jedničky podle toho, zda v daném rozhodovacím bloku dojde k záměně prvků či nikoliv. Počet možných ohodnocení je tedy horním odhadem na počet permutací. Má-li síť m rozhodovacích bloků, musí platit $2^m \geq n!$ (srov. obr. 10.1, kde $m = 5$ a $n = 4$). Odtud $m \geq c \cdot n \log n$ pro nějakou konstantu c . Protože v každém kroku můžeme porovnat nejvýše $n/2$ dvojic, musí mít síť hloubku alespoň $c \log(n/2)$.

Tento lehký důkaz může svádět k domněnce, že je také snadné sestrojit síť hloubky $\text{konst} \times \log n$. Ve skutečnosti to není vůbec jednoduché. Výsledek Ajtai, Komlóse a Szemerédiho [1], že taková síť se dá sestrojit, je velice složitý. Nejtěžší částí je důkaz tvrzení, že zkonstruovaná síť setřídí každou posloupnost.

10.8 Závěrečné poznámky

Szemerédiova věta z kapitoly 10.3 vlastně ukazuje na jistý skrytý řád v každé dostatečně velké množině přirozených čísel. Celá řada dalších matematických tvrzení také nese Szemerédiovo jméno, např. Hajnalova–Szemerédiova věta o vyvážených obarveních grafů⁴ či Szemerédiova–Trotterova věta o počtu incidencí přímek a bodů. Databáze Mathematical Reviews eviduje přes 170 Szemerédiho prací. Na některých z nich spolupracoval i s českými matematiky (Václavem Chvátalem, Vojtěchem Röddlem či Pavlem Pudlákem, viz [2], [9]). Matematická společnost Jánosa Bolyaie vydala v nakladatelství Springer sborník *An Irregular Mind*, věnovaný sedmdesátým narozeninám E. Szemerédiho, kde se podrobně rozebírá jeho přínos pro matematiku. Nedávno s ním byl také publikován rozhovor [14].

Szemerédi se ve svém výzkumu soustředil na dva protichůdné pojmy: řád a chaos ve velkých kombinatorických strukturách. Szemerédiova genialita umožnila dokázat existenci jistého řádu ve velkých strukturách při použití výsledků o náhodnosti.

L i t e r a t u r a

- [1] AJTAI, M., KOMLÓS, J., SZEMERÉDI, E.: *Sorting in $c \log n$ parallel steps*. *Combinatorica* 3(1) (1983), 1–19.

⁴Každý graf s maximálním stupněm vrcholů d se dá vrcholově řádně obarvit $d + 1$ barvami tak, že počty vrcholů téže barvy se liší maximálně o 1.

- [2] BABAI, L., PUDLÁK, P., RÖDL, V., SZEMERÉDI, E.: *Lower bounds to the complexity of symmetric Boolean functions*. Theoret. Comput. Sci. 74 (1990), 313–323.
- [3] BALASUBRAMANIAN, R., DESHOUILERS, J.-M., DRESS, F.: *Problème de Waring pour les bicarrés (Waring’s problem for biquadrates, Part I, II)*. C.R. Acad. Sci. Paris Sér. I Math. 303 (1986), 85–88, 161–163.
- [4] ERDŐS, P., SZEMERÉDI, E.: *On sums and products of integers*. In: Studies in Pure Mathematics, Birkhäuser, Basel 1983, 213–218.
- [5] ERDŐS, P., TURÁN, P.: *On some sequences of integers*. J. London Math. Soc. 11 (1936), 261–264.
- [6] GREEN, B., TAO, T.: *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math. 167 (2008), 481–547.
- [7] CHEN, J. R.: *Waring’s problem for $g(5) = 37$ (in Chinese)*. Sci. Sinica 13 (1964), 1547–1568. Chinese Math. 6 (1965), 105–127. Translation from Acta Math. Sin. 14 (1964), 715–734.
- [8] CHEN, J. R.: *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*. Sci. Sinica 16 (1973), 157–176.
- [9] CHVÁTAL, V., SZEMERÉDI, E.: *Short cycles in directed graphs*. J. Combin. Theory Ser. B 35 (1983), 323–327.
- [10] KLAZAR, M.: *Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti*. PMFA 49 (2004), 177–188.
- [11] NATHANSON, M. B.: *Additive number theory: Inverse problems and the geometry of sunsets*. Springer, New York 1996.
- [12] NATHANSON, M. B.: *Additive number theory: The classical bases*. Springer, New York 1996.
- [13] PILLAI, S. S.: *On Waring’s problem $g(6) = 73$* . Proc. Indian Acad. Sci. Sect. A. 12 (1940), 30–40.
- [14] RAUSSEN, M., SKAU, C.: *Interview with Endre Szemerédi*. Notices Amer. Math. Soc. 60 (2013), 221–231.
- [15] SOLYMOSI, J.: *An upper bound on the multiplicative energy*. Dostupné z: <http://arxiv.org/abs/0806.1040>

- [16] SZEMERÉDI, E.: *On sets of integers containing no k elements in arithmetic progression*. Acta Arithmetica 27 (1975), 199–245.
- [17] SZEMERÉDI, E.: *Regular partitions of graphs*. In: Problèmes combinatoires et théorie des graphs, Colloques Internationaux CNRS 260, 1976, Univ. Orsay, Paris 1978, 399–401.
- [18] TAO, T.: *Every odd number greater than 1 is the sum of at most five primes*. Math. Comp. 83 (2014), 997–1038.
- [19] VINOGRADOV, I. M.: *Some theorems concerning the theory of primes*. Rec. Math. Moscou New Ser. 2 (1937), 179–195.
- [20] WIEFERICH, A.: *Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt (Proof of theorem that every integer can be written as a sum of at most nine positive cubes)*. Math. Ann. 66 (1909), 95–101.
- [21] <http://www.abelprisen.no/en/>

11. V roce 2013 získal Abelovovu cenu Pierre Deligne za fundamentální práce svazující algebru a geometrii

Michal Křížek, Martin Markl, Lawrence Somer

11.1 Prolog

Dne 21. května 2013 získal Abelovu cenu za matematiku Pierre Deligne, emeritní profesor Ústavu pro pokročilá studia v americkém Princetonu. Podle vyjádření výběrové komise ji získal *za své průkopnické práce v algebraické geometrii a jejich dopad na teorii čísel, teorii*



PIERRE RENÉ DELIGNE

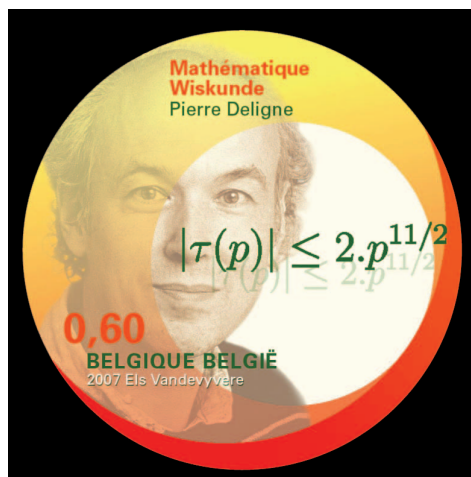
reprezentací a příbuzné obory. Deligneho účinné koncepty, skvělé myšlenky, silné výsledky a metody ovlivňují algebraickou geometrii, jakož i celou matematiku (viz [23]). Deligne to komentoval slovy: *Krásná věc na matematice je dělat matematiku. Ocenění přijde později*. Cenu mu udělila Norská akademie věd, která byla založena již v roce 1857 a jejímž současným čestným předsedou je Jeho Veličenstvo norský král Harald V. O předchozích deseti Abelových cenách pojednává též přehledová publikace [15].

11.2 Stručný životopis

Pierre René Deligne se narodil 3. října 1944 v Bruselu. Když mu bylo 12 let, začal si číst univerzitní matematické učebnice svého staršího bratra. Na střední škole mu pak profesor matematiky půjčil několik svazků *Éléments de mathématique* od Nicolase Bourbakiho (což je pseudonym skupiny francouzských matematiků). To mladému Pierrovi navždy změnilo život. Jeho otec sice chtěl, aby se stal inženýrem, ale Pierre se rozhodl pro univerzitní studia matematiky. Na univerzitu v Bruselu nastoupil s ambicemi stát se středoškolským učitelem. Tam se však setkal s dalším budoucím nositelem Abelovy ceny Jacquesem Titsem, který jej přivedl k výzkumu v matematice. V roce 1966 získal Deligne titul B.A. Pod vedením Alexandera Grothendiecka obhájil v r. 1968 doktorskou dizertační práci. V témže roce začal spolupracovat na reprezentacích modulárních forem [6] s pozdějším prvním laureátem Abelovy ceny Jeanem-Pierrem Serrem, který se mj. zabýval analogiemi Weilových domněnek (viz kap. 11.5 a [20]). V roce 1970 byl Pierre Deligne přijat do Institut des hautes études scientifiques v Bures-sur-Yvette nedaleko Paříže. V roce 1972 obhájil na univerzitě Paris-Sud velký doktorát (Doctorat d'État) v oblasti matematických věd.

P. Deligne se zasloužil o nalezení nových spojitostí mezi různými oblastmi matematiky, což vedlo k řadě důležitých objevů. Jeho největším přínosem je velkolepý důkaz Weilovy domněnky, publikovaný v roce 1973. O pět let později za něj dostal Fieldsovu medaili a v roce 1988 ještě Crafoordovu cenu společně se svým bývalým školitelem Alexanderem Grothendieckem. Stručně řečeno, jde o důkaz analogie slavné Riemannovy hypotézy nad konečnými tělesy, jež v původní formulaci pro komplexní rovinu $\mathbb{C}$ doposud vyřešena nebyla (je to jeden

ze sedmi problémů pro třetí tisíciletí [8]). Deligne získal také Cenu Henriho Poincarého v r. 1974, Balzanovu cenu v r. 2004 a prestižní Wolfovu cenu v r. 2008 společně s Phillipem Griffithsem a Davidem Mumfordem. V roce 2006 jej belgický král Albert II. jmenoval vikomtem. Pierre Deligne je čestným členem Moskevské matematické společnosti a Londýnské matematické společnosti. Je také čestným zahraničním členem Americké akademie věd a umění, Americké filozofické společnosti a Královské švédské akademie věd. Za své fundamentální objevy v matematice se dokonce dostal na belgické poštovní známky (viz obr. 11.1).



Obr. 11.1 Pierre Deligne na belgické poštovní známce

11.3 Rozřešení Rámanudžanovy domněnky

Deligne se poprvé proslavil důkazem Rámanudžanovy (Rámanudžanovy–Petersonovy) domněnky z teorie modulárních forem. Definujme koeficienty $\tau(n)$ pomocí vztahu

$$q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n, \quad (11.1)$$

kde $q \in \mathbb{C}$. Rovnost mezi nekonečným součinem vlevo a mocninnou řadou pravo je třeba chápat čistě formálně, protože jejich konvergence je vedlejší. Pro konkrétní přirozené číslo n je totiž koeficient $\tau(n)$ jednoznačně dán součtem jen konečně mnoha čísel.

V roce 1916 Šrinivása Rámanudžan vyslovil domněnku (viz [19, s. 176]), že pro libovolné prvočíslo p platí

$$|\tau(p)| \leq 2p^{11/2},$$

kterou dokázal právě Deligne [4]. Koeficienty¹ $\tau(n)$ jsou hodnoty tzv. *Rámanudžanovy τ -funkce*. Rámanudžanovu domněnku lze zobecnit takto:

Pro přirozené číslo n je $|\tau(n)| \leq d(n)n^{11/2}$, kde $d(n)$ označuje počet dělitelů čísla n .

Za q nyní zvolme komplexní číslo $e^{2\pi iz} \in \mathbb{C}$, kde $z = a + ib \in \mathbb{C}$ pro reálná $a, b \in \mathbb{R}$, to jest

$$q = e^{2\pi iz} = e^{2\pi i(a+ib)} = e^{2\pi ia - 2\pi b} = e^{2\pi ia} e^{-2\pi b}.$$

Vidíme, že absolutní hodnota $|q| = e^{-2\pi b}$, protože $|e^{2\pi ia}| = 1$. Odtud plyne, že $|q| < 1$, kdykoliv je imaginární část z kladná. Podmínka $|q| < 1$ zajišťuje konvergenci nekonečného součinu v (11.1), který tak bude definován pro z z horní otevřené poloroviny komplexní roviny. Tuto funkci proměnné z označme $\Delta(z)$.

Funkce Δ je holomorfní a lze ji rozšířit na celou komplexní rovinu. Je periodická v tom smyslu, že platí

$$\Delta(z) = \Delta(z + 1) \quad \forall z \in \mathbb{C}$$

a navíc $\Delta(-1/z) = z^{12}\Delta(z)$ pro všechna $z \in \mathbb{C}$. Jestliže roste imaginární část z do nekonečna, potom $\Delta(z)$ konverguje k nule. Uvedené vlastnosti znamenají, že Δ je modulární forma. Tento typ funkcí hraje významnou roli ve Wilesově důkazu Velké Fermatovy věty.

Záhadný exponent 24 ve vztahu (11.1) souvisí s Leechovou mřížkou nejhustšího uspořádání stejně velkých nadkoulí v eukleidovském prostoru $\mathbb{R}^{24}$ (podrobnosti viz [14]). Můžeme se ptát: Kolika různými způsoby můžeme zvolené přirozené číslo n napsat ve tvaru $x_1^2 + x_2^2 + \dots + x_{24}^2$, kde $x_1, \dots, x_{24}$ jsou celá čísla? Jinými slovy, kolik mřížových bodů s celočíselnými souřadnicemi leží na nadsféře o poloměru $\sqrt{n}$? Kolik mřížových bodů leží uvnitř této nadsféry? Odhady počtu mřížových bodů úzce souvisejí s koeficienty $\tau(n)$ (viz [11, s. 6]). Nejvyšší hustota stejně velkých nadkoulí je zatím známa jen v prostorech $\mathbb{R}^k$ pro $k = 1, 2, 3, 4, 8$ a 24 .

¹Celou řadu vztahů pro koeficienty $\tau(n)$ lze najít v monografii [17].

11.4 Riemannova hypotéza

Označme $\pi(n)$ počet prvočísel $p \leq n$. Pravděpodobnost, že $n \geq 2$ je prvočíslo, je zhruba rovna $1/\ln n$. Na základě této vlastnosti Carl Friedrich Gauss (1777–1855) předložil jako domněnku² prvočíselnou větu³

$$\pi(n) \approx \frac{n}{\ln n},$$

kde symbol $\approx$ označuje asymptotickou rovnost pro $n \rightarrow \infty$. Jedna z několika verzí slavné a dosud nerozřešené Riemannovy hypotézy tvrdí, že pro každé $\varepsilon > 0$ je

$$\pi(n) = \text{Li}(n) + O(n^{1/2+\varepsilon}),$$

kde

$$\text{Li}(n) = \int_2^n \frac{dt}{\ln t} \quad (\text{integrállogaritmus}).$$

Funkce $\text{Li}(n)$ se přitom asymptoticky chová jako $n/\ln n$.

Připomeňme nyní stručně ekvivalentní verzi Riemannovy hypotézy. Pak zformulujeme její verzi nad konečnými tělesy (viz kap. 11.5), za jejíž vyřešení byl Deligne oceněn. Položme

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \quad (11.2)$$

kde suma konverguje pro libovolné komplexní číslo z takové, že $\text{Re}(z) > 1$. Funkce ζ se nazývá *Riemannova ζ -funkce*. Platí, že $\zeta(1) = \infty$ (součet harmonické řady) a $\zeta(2) = \frac{\pi^2}{6}$.

Nejprve dokážeme následující překvapivou rovnost obsahující na pravé straně nekonečný součin přes všechna prvočísla $p \in P = \{2, 3, 5, 7, \dots\}$,

$$\zeta(z) = \prod_{p \in P} \frac{1}{1 - p^{-z}}. \quad (11.3)$$

Eulerova věta. Definice (11.2) a (11.3) jsou ekvivalentní pro všechna komplexní čísla z taková, že $\text{Re}(z) > 1$.

²Domněnku nezávisle dokázali v roce 1896 Jacques Hadamard (1865–1963) a Charles-Jean de la Vallée Poussin (1866–1962).

³Lze však ukázat, že asymptotika $\pi(n) = n/\ln n + O(n/\ln^3 n)$ neplatí.

Uveďme snadný, ale nádherný důkaz. Označíme-li i -té prvočíslo p_i , pak každé přirozené číslo n lze podle základní věty aritmetiky (viz [16, s. 51]) jednoznačně vyjádřit součinem $p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots$ s nezápornými celými exponenty $k_1, k_2, k_3, \dots$. Jinak řečeno, množinu $\mathbb{N}$ přirozených čísel je možné popsat konečnými součiny

$$\mathbb{N} = \{p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots \mid k_1, k_2, k_3, \dots \text{ jsou nezáporná celá čísla}\}.$$

Podle vztahu pro součet geometrické řady platí pro každé $i = 1, 2, \dots$, že

$$\sum_{j=0}^{\infty} \left(\frac{1}{p_i^z}\right)^j = \frac{1}{1 - p_i^{-z}}.$$

Vynásobíme-li mezi sebou tyto rovnice, dostaneme

$$\begin{aligned} \prod_{i=1}^{\infty} \frac{1}{1 - p_i^{-z}} &= \left(1 + \frac{1}{2^z} + \frac{1}{2^{2z}} + \cdots\right) \left(1 + \frac{1}{3^z} + \frac{1}{3^{2z}} + \cdots\right) \cdots \\ &\quad \cdots \left(1 + \frac{1}{p_i^z} + \frac{1}{p_i^{2z}} + \cdots\right) \cdots \\ &= \sum_{k_1, k_2, k_3, \dots \geq 0} \frac{1}{(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots)^z} = \sum_{n=1}^{\infty} \frac{1}{n^z}, \end{aligned}$$

což je žádaná rovnost⁴ výrazů (11.2) a (11.3). $\square$

Německý matematik Bernhard Riemann (1826–1866) odvodil pro ζ -funkci další užitečný vztah

$$\pi^{-\frac{z}{2}} \Gamma\left(\frac{z}{2}\right) \zeta(z) = \pi^{-\frac{1-z}{2}} \Gamma\left(\frac{1-z}{2}\right) \zeta(1-z), \quad (11.4)$$

který říká, jak se ζ -funkce chová při substituci z za $1 - z$. Zde je Γ -funkce definována vztahem

$$\Gamma(z) = \int_0^{\infty} e^{-t} t^{z-1} dt$$

a je přirozeným rozšířením faktoriálu

$$\Gamma(n) = (n-1)!$$

⁴Rovnost výrazů (11.2) a (11.3) je jedním z několika důvodů, proč 1 nezařazujeme mezi prvočísla. Dalším důvodem je požadavek na jednoznačnost rozkladu přirozeného čísla $n > 1$ na součin mocnin prvočísel.

do oboru komplexních čísel. Funkce $\zeta(1-z)$ na pravé straně (11.4) má pól pro $z = 0$ a $\Gamma\left(\frac{1-z}{2}\right)$ má póly v bodech $z = 1, 3, 5, 7, \dots$. Protože levá strana (11.4) je v bodech $z = 3, 5, 7, \dots$ konečná, platí

$$0 = \zeta(-2) = \zeta(-4) = \zeta(-6) = \dots$$

Tyto kořeny se nazývají *triviální*. Funkci ζ lze rozšířit na funkci meromorfní v komplexní rovině s pólem v bodě 1. *Riemannova hypotéza* tvrdí, že všechny netriviální kořeny tohoto rozšíření funkce ζ mají reálnou část rovnou $1/2$.

Rozřešení této hypotézy je dnes pokládáno za jeden z nejtěžších a nejdůležitějších problémů teorie čísel, neboť úzce souvisí s otázkou rozložení prvočísel (srov. (11.3)). Na jeho vyřešení byla vypsána odměna 1 000 000 dolarů (viz [8]).

11.5 Weilovy domněnky

P. Deligne se proslavil zejména rozřešením třetí Weilovy domněnky. Před její formulací připomeneme některé pojmy. *Charakteristika tělesa* F je nejmenší přirozené číslo q takové, že jednotka $1 \in F$ splňuje rovnici

$$\underbrace{1 + 1 + \dots + 1}_{q\text{-krát}} = 0.$$

Pokud takové číslo neexistuje, říkáme, že F má *charakteristiku nula*. Je zřejmé, že konečná charakteristika je vždy prvočíslem. Příkladem těles charakteristiky 0 jsou reálná nebo komplexní čísla. Příkladem tělesa prvočíselné charakteristiky q je těleso $\mathbb{Z}_q$ celých čísel modulo q .

Je snadné dokázat, že konečné těleso prvočíselné charakteristiky q musí mít q^m prvků pro nějaké přirozené číslo m . Příkladem⁵ je množina $\mathbb{F}_{q^m}$ kořenů polynomu $t^{q^m} - t$ v nějakém algebraickém rozšíření tělesa $\mathbb{Z}_q$. Ověřme, že $\mathbb{F}_{q^m}$ je těleso. Protože

$$t^{q^m} - t = t(t-1)(t^{q^m-2} + t^{q^m-3} + \dots + t + 1),$$

0 i 1 náležejí do $\mathbb{F}_{q^m}$. Multiplikativní uzavřenost je zřejmá: pokud $a, b \in \mathbb{F}_{q^m}$, pak $a^{q^m} = a$, $b^{q^m} = b$, tedy $(ab)^{q^m} = a^{q^m}b^{q^m} = ab$, což

⁵Příklad je motivován implikací: Je-li q prvočíslo a $m, n \in \mathbb{N}$, pak q dělí $n^{q^m} - n$. Případ $m = 1$ je Malá Fermatova věta [16]. Pro $m > 1$ lze použít indukci.

znamená, že $ab \in \mathbb{F}_{q^m}$. Podobně ukážeme, že jestliže $a \in \mathbb{F}_{q^m}$, potom $a^{-1} \in \mathbb{F}_{q^m}$. Zbývá dokázat, že $a + b \in \mathbb{F}_{q^m}$ pro $a, b \in \mathbb{F}_{q^m}$. Podle binomické věty

$$(a + b)^{q^m} = \sum_{i=0}^{q^m} \binom{q^m}{i} a^i b^{q^m-i}.$$

Pokud $1 \leq i \leq q^m - 1$, pak

$$\binom{q^m}{i} = \frac{q^m}{i} \binom{q^m - 1}{i - 1}. \quad (11.5)$$

Vynásobíme-li tuto rovnost i , vidíme, že (srov. [16, s. 86])

$$q^m \text{ dělí } \binom{q^m}{i},$$

protože oba binomické koeficienty v (11.5) jsou přirozená čísla a q^m nedělí i . Máme tedy $(a + b)^{q^m} = a^{q^m} + b^{q^m} = a + b$, a proto $a + b \in \mathbb{F}_{q^m}$. Těleso $\mathbb{F}_{q^m}$ se nazývá *Galoisovo konečné těleso* s q^m prvky. Lze ukázat, že všechna tělesa s q^m prvky jsou izomorfní s tímto tělesem.⁶

Afinní varieta se obvykle definuje jako množina řešení určitého systému polynomiálních rovnic (třeba $x^2 + y^2 = 1$) nad tělesem reálných či komplexních čísel. Stejně ovšem můžeme definovat variety i nad konečným tělesem F . Například dvojice $(4, 6)$ patří „kružnici“ $x^2 + y^2 = 1$ nad tělesem $\mathbb{F}_{17}$, protože $4^2 + 6^2 = 52$ dává zbytek 1 při dělení 17. Jiným příkladem je dvojice $(3, 3)$. Podobně je projektivní varieta množina řešení soustavy homogenních polynomiálních rovnic v projektivním prostoru.⁷

André Weil vyslovil v roce 1949 čtyři domněnky (viz [22] a [9]) o počtu bodů algebraických variet nad konečnými tělesy (jejich speciální případ formuloval již v roce 1924 Emil Artin [1]). Předpokládejme, že q je prvočíslo a X hladká (regulární) n -rozměrná projektivní varieta nad tělesem $\mathbb{F}_q$. V této situaci definujeme ζ -funkci variety X předpisem

$$\zeta(X, z) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} (q^{-z})^m\right), \quad (11.6)$$

⁶Podobné tvrzení pro grupy neplatí. Existuje např. 5 neizomorfních grup o $3^3 = 27$ prvcích, z nichž 3 jsou komutativní.

⁷Projektivní prostor je tvořen třídami ekvivalence vektorů $(x_0, \dots, x_n) \in F^{\times(n+1)}$, přičemž ekvivalentní jsou vektory $(x_0, \dots, x_n)$ a $(\lambda x_0, \dots, \lambda x_n)$ pro nenulové $\lambda \in F$.

ve kterém $z \in \mathbb{C}$ a N_m je počet bodů variety X nad rozšířením $\mathbb{F}_{q^m}$ tělesa $\mathbb{F}_q$. Weil předpověděl, že by ζ -funkce měly být racionální, že by měly splňovat jistou funkcionální rovnici a že by měly mít kořeny na přesně vymezených přímkách. *Weilovy domněnky* lze přesněji formulovat takto:

1. *Racionalita*. Funkce $\zeta(X, z)$ je racionální v proměnné $t = q^{-z}$ a má tvar

$$\zeta(X, z) = \frac{P_1(t)P_3(t) \cdots P_{2n-1}(t)}{P_0(t)P_2(t) \cdots P_{2n}(t)}, \quad (11.7)$$

kde $P_i(t)$ jsou polynomy s celočíselnými koeficienty, přičemž $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$. Racionalitu funkce (11.6) dokázal Bernard Dwork [10].

2. *Funkcionální rovnice a Poincarého dualita*. Funkce ζ splňuje vztah

$$\zeta(X, n - z) = \pm q^{nE/2 - Ez} \zeta(X, z),$$

kde E je Eulerova charakteristika variety X . Položíme-li $t = q^{-1}$, obdržíme funkcionální rovnici

$$\zeta(X, q^{-n}t^{-1}) = \pm q^{nE/2} t^E \zeta(X, z).$$

Z ní plyne, že substituce $t \mapsto 1/q^n t$ zaměňuje kořeny polynomu $P_i(t)$ za kořeny polynomu $P_{2n-i}(t)$. Tuto druhou domněnku dokázal Alexander Grothendieck [12].

3. *Konečná verze Riemannovy hypotézy*. Kořeny polynomu P_i vystupujícího v (11.7) leží na „kritické přímce“ v rovině komplexních čísel z s reálnou částí $i/2$. Tuto třetí a zároveň nejtěžší domněnku dokázal právě Pierre Deligne [4] v roce 1974 (viz též [5]).

4. *Bettiho čísla*. Je-li X redukce modulo p regulární projektivní variety nad tělesem komplexních čísel, pak je stupeň polynomu P_i roven dimenzi i -té homologické grupy této variety, tedy jejímu i -tému Bettiho číslu β_i (viz [18, s. 731–732]).

Jako příklad vezměme hladkou projektivní křivku X rodu g .⁸ V souladu s Weilovou domněnkou

$$\zeta(X, z) = \frac{P(t)}{(1-t)(1-qt)},$$

⁸*Rod* (genus) g je polovina prvního Bettiho čísla β_1 variety X . Pro $g = 0$ je tedy X topologicky dvourozměrná sféra, pro $g = 1$ torus.

kde $P(t)$ je polynom stupně $2g$. Konečná verze Riemannovy hypotézy říká, že kořeny polynomu $P(t)$ leží na přímce komplexních čísel s imaginární částí $1/2$. Podobnost s klasickou Riemannovou hypotézou je důsledkem mnohem hlubší souvislosti.

Připomeňme, že těleso algebraických čísel K je konečné rozšíření tělesa racionálních čísel $\mathbb{Q}$. Každé takové K obsahuje okruh celých algebraických čísel $\mathcal{O}_K$ tvořený prvky $x \in K$ splňujícími rovnici

$$x^k + A_1x^{k-1} + \dots + A_k = 0$$

s nějakými celočíselnými koeficienty $A_1, \dots, A_k \in \mathbb{Z}$. Snadno se přesvědčíme, že $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, což zdůvodňuje názvosloví.

V popsané situaci Richard Dedekind definoval ζ -funkci vztahem

$$\zeta_K(z) = \sum N(I)^{-z},$$

kde součet probíhá všechny ideály I okruhu $\mathcal{O}_K$ a $N(I)$ značí kardinalitu podílového okruhu $\mathcal{O}_K/I$. Podobně jako v klasickém případě (11.3) můžeme ζ -funkci vyjádřit také Eulerovým součinem

$$\zeta_K(z) = \prod \frac{1}{1 - N(\mathfrak{p})^{-z}}$$

přes všechny prvoideály $\mathfrak{p}$ okruhu $\mathcal{O}_K$. Doporučujeme jako cvičení ukázat, že pro $K = \mathbb{Q}$ dostáváme klasickou Riemannovu ζ -funkci z kapitoly 11.4. Artin si povšiml, že Dedekindovu definici lze použít i na okruh regulárních funkcí na varietě X . Vzorec (11.6) je přepis Dedekindovy definice do geometrického jazyka. Plné pochopení podstaty Weilových domněnek inspirovalo objev etálních kohomologií, jednoho z nejdůležitějších pojmů moderní algebraické geometrie.

11.6 Další Deligneovy výsledky

Databáze Mathematical Reviews obsahuje přes 100 Deligneových prací z nejrůznějších matematických oborů. Jeho záběr je opravdu široký: matematická teorie strun a supergravitace, spinory, hyperbolické funkce, homologické algebry, eliptické křivky, modulární formy, konečné grupy, ...

Deligne se snažil rozřešit několik dalších závažných problémů. Uveďme si několik typických příkladů. Deligne se např. zabýval Hodgeovou domněnkou, což je opět jeden ze sedmi problémů pro třetí tisíciletí [8].

Deligne ve své práci [3] také podstatně přispěl k rozřešení a zobecnění 21. Hilbertova problému o existenci diferenciálních rovnic s regulárními singulárními body. Použité důkazové techniky jsou popsány v [13]. Další přehledový článek o jeho příspěvcích k matematice nedávno napsal Gowers [11].

Na úplný závěr zmíníme domněnku formulovanou Delignem v dopise [7] z roku 1993, k jejímuž důkazu přispěl český matematik. Domněnka říká, že struktura Gerstenhaberovy algebry na Hochschildových kohomologiích je generována akcí operády malých disků na kořetězcích. Zobecněním je problém charakterizace homotopického typu operády všech přirozených operací. Tento problém byl v [2] zcela vyřešen Michaellem Bataninem a druhým autorem této kapitoly Martinem Marklem.

L i t e r a t u r a

- [1] ARTIN, E.: *Quadratische Körper im Gebiete der höheren Kongruenzen II. Analytischer Teil.* Math. Z. 19 (1924), 207–246.
- [2] BATANIN, M., MARKL, M.: *Crossed interval groups and operations on the Hochschild cohomology.* Vyjde v Journal of Noncommutative Geometry, 36 stran. Předběžná verze vystavena jako preprint arXiv:0803.2249.
- [3] DELIGNE, P.: *Equations différentielles à points singuliers réguliers.* Lecture Notes in Mathematics 163. Springer, Berlin–Heidelberg–New York 1970.
- [4] DELIGNE, P.: *La conjecture de Weil I.* Publ. Math. Inst. Hautes Etudes Sci. 43 (1974), 273–307.
- [5] DELIGNE, P.: *La conjecture de Weil II.* Publ. Math. Inst. Hautes Etudes Sci. 52 (1980), 137–252.
- [6] DELIGNE, P., SERRE, J.-P.: *Formes modulaires de poids.* Ann. Sci. École Norm. Sup. 7 (1974), 507–530.
- [7] DELIGNE, P.: *A letter to Stasheff, Gerstenhaber, May, Schechtman and Drinfel'd.* 1993.
- [8] DEVLIN, K. J.: *The millenium problems: The seven greatest unsolved mathematical puzzles of our time.* Basic Books, New York 2002; český překlad, Dokořán, Praha 2005.

- [9] DIEUDONNÉ, J.: *The Weil conjectures*. Math. Intelligencer 10 (1975), 7–21.
- [10] DWORK, B.: *On the rationality of the zeta function of an algebraic variety*. Amer. J. Math. 82 (1960), 631–648.
- [11] GOWERS, W. T.: *The work of Pierre Deligne*. Preprint 2013, 1–15.
- [12] GROTHENDIECK, A.: *Tores maximaux, groupe de Weil, sous-groupes de Cartan, centre réductif des schémas en groupes lissés et affines*. Sémin. Géométrie Algébrique, Inst. Hautes Études Sci. 1963/64, Fasc. 4, Exposé 12, 69 pp.
- [13] KATZ, N. M.: *An overview of Deligne’s work on Hilbert’s twenty-first problem*. In: Mathematical Developments Arising from Hilbert Problems, Part 2, Amer. Math. Soc., Providence, 1976, 537–557.
- [14] KRÍŽEK, M., SOMER, L.: *Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup*. PMFA 53 (2008), 177–187.
- [15] KRÍŽEK, M., SOMER, L., MARKL, M., KOWALSKI, O., PUDLÁK, P., VRKOČ, I.: *Prvních deset Abelových cen za matematiku*. JČMF, Praha, 2013.
- [16] KRÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Academia, Praha 2009, 2011.
- [17] MORENO, C. J., WAGSTAFF, S. S.: *Sums of squares of integers*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton 2006.
- [18] OSSERMAN, B.: *The Weil conjectures*. The Princeton Companion to Mathematics, T. Gowers (ed.). Princeton Univ. Press 2008, 729–732.
- [19] RAMANUJAN, S.: *On certain arithmetical functions*. Trans. Cambridge Phil. Soc. XXII (1916), 159–184.
- [20] SERRE, J. -P.: *Analogues kähleriens de certaines conjectures de Weil*. Ann. Math. 71 (1960), 392–394.
- [21] SCHROEDER, M. R.: *Number theory in science and communication*. Springer, Berlin 1984, 1986, 1997, 2006.
- [22] WEIL, A.: *Numbers of solutions of equations in finite fields*. Bull. Amer. Math. Soc. 55 (1949), 497–508.
- [23] <http://www.abelprize.no>

12. Abelovu cenu za matematiku získal v roce 2014 Jakov G. Sinaj

Michal Křížek

12.1 Prolog

Dne 26. března 2014 oznámil předseda Norské akademie věd Nils Christian Stenseth, že Abelovu cenu za rok 2014 získá ruský matematik prof. Jakov G. Sinaj za své *fundamentální příspěvky k teorii dynamických systémů, ergodické teorii a matematické fyzice*.



JAKOV G. SINAJ

V pondělí 19. května 2014 se J. Sinaj nejprve zúčastnil kladení květin a věnců u památníku Nielse Henrika Abela v královské zahradě v Oslu (viz obr. 12.1). Následující den pak laureát převzal Abelovu cenu v hlavní aule univerzity v Oslu. Večer pak Norská akademie věd uspořádala slavnostní banket na počest prof. Sinaje na zámku Akershus.

Dne 21. května J. Sinaj proslovil na univerzitě v Oslu odbornou laureátskou přednášku *Now everything has been started? The origin of deterministic chaos*. Poté následovaly tři abelovské přednášky shrnující laureátovo dílo. První proslovil Gregory Marguli, nositel Fieldsovy medaile, na téma *Kolmogorov–Sinai entropy and homogeneous dynamics*. Jako druhý vystoupil Konstantin M. Chanin s přednáškou *Between mathematics and physics*. Ve třetí přednášce *Mathematical billiards and chaos* se Domokos Szász pokusil odpovědět na otázku, zda může náhodné chování vzniknout v čistě deterministických systémech. O den později pronesl prof. Sinaj ještě další přednášku popularizující matematiku pro studenty na univerzitě ve Stavangeru.

Profesor Sinaj je uznávanou osobností jak mezi matematiky, tak mezi fyziky. Pracuje v Matematickém ústavu na univerzitě v Princetonu a Landauově ústavu pro teoretickou fyziku Ruské akademie věd. Není proto divu, že je autorem stimulujícího článku *Mathematicians and physicists = Cats and dogs?* [14], v jehož závěru se svěří: *Obvykle fyzikům nedůvěřují, dokud nenaleznou svůj vlastní důkaz nebo alespoň objasnění jejich výsledků.*

Jakov Sinaj získal Abelovu cenu mj. za práce svazující teorii deterministických dynamických systémů s teorií stochastických systémů. Je po něm pojmenována celá řada matematických pojmů, např. Kolmogorovova–Sinajova entropie, Sinajův kulečník (billiards), Sinajova náhodná procházka, Sinajova–Ruelleova–Bowenova míra či Pirogovova–Sinajova teorie.

12.2 Stručný životopis

Jakov Grigorjevič Sinaj se narodil 21. září 1935. Oba jeho rodiče byli mikrobiologové. Dědeček z matčiny strany, matematik Veniamin Fjodorovič Kagan, byl vedoucím oddělení diferenciální geometrie na Moskevské státní univerzitě (MGU) a hodně se svému vnuku Jakobovi věnoval.



Obr. 12.1 Socha NIELSE HENRIKA ABELA v Oslu (foto J. E. Vatne)

Jakov Sinaj začal studovat v roce 1952 na Fakultě mechaniky a matematiky MGU. V roce 1957 úspěšně zakončil studium, v roce 1960 získal vědecký titul kandidáta věd a o tři roky později i velký doktorát. Jeho školitelem byl slavný ruský matematik Andrej Nikolajevič Kolmogorov. Na MGU se J. Sinaj aktivně účastnil semináře o ergodické teorii.

Již v roce 1962 měl Sinaj zvanou přednášku na Mezinárodním kongresu matematiků ve Stockholmu (celkem přednášel na těchto kongresech čtyřikrát). V letech 1960–1971 působil jako vědecký pracovník

v laboratoři pravděpodobnostních a statistických metod MGU. Poté se stal profesorem na MGU a vedoucím vědeckým pracovníkem v Landauově ústavu teoretické fyziky Ruské akademie věd. Tento ústav byl založen v roce 1964 ve městě Černogolovka asi 40 km severně od Moskvy.

Profesor Sinaj vyškolil více než 50 Ph.D. studentů. Je velice respektovaným pedagogem na univerzitě v Princetonu. Jeden z jeho studentů o něm prohlásil: *Být v jeho třídě je velice inspirativní . . . Přítomní cítí okamžitou potřebu vstoupit do děje — vyzařuje z něj hmatatelné nadšení, které nás inspiruje.*

V roce 1997 byl Jakov Sinaj oceněn prestižní Wolfovou cenou. V letech 1997–1998 působil na Princetonské univerzitě a v roce 2005 nastoupil na Kalifornský technologický ústav v Pasadeně. V roce 2001 byl zvolen předsedou výboru Mezinárodní matematické unie, který uděloval Fieldsovy medaile další rok na kongresu v Pekingu. V roce 2002 mu byla udělena Nemmersova cena za matematiku. Během života získal mnoho dalších ocenění, např. Diracovu medaili či Boltzmannovu zlatou medaili. Čestný doktorát mu udělila Varšavská univerzita (1993), Budapešťská univerzita (2002), Hebrejská univerzita v Jeruzalémě (2005) a univerzita ve Warwicku (2010). Profesor Sinaj byl zvolen členem, popř. čestným členem mnoha akademií a vědeckých společností, např. Americké akademie umění a věd (1983), Ruské akademie věd (1991), Londýnské matematické společnosti (1992), Maďarské akademie věd (1993), Americké národní akademie věd (1999), Brazílské akademie věd (2000), Academia Europaea (2008), Polské akademie věd (2009) a Londýnské královské společnosti (2009).

12.3 Řád a chaos v dynamických systémech

Pod pojmem dynamický systém chápeme matematický popis a vývoj nějakého fyzikálního systému v čase. Systém má obvykle mnoho přípustných stavů, které tvoří tzv. *fázový prostor*. Cesta ve fázovém prostoru pak popisuje dynamiku uvažovaného systému. Dynamický systém může být čistě deterministický, např. systém diferenciálních rovnic 1. řádu popisující pohyb kyvadla. Ze zadané polohy a rychlosti můžeme jednoznačně vypočítat jeho budoucí stavy. Druhým extrémem je stochastický systém, jehož budoucí vývoj je zcela nejistý, např. házení mincí.

Již od dob Isaaca Newtona používají matematici, fyzici a inženýři diferenciální rovnice, aby vysvětlili rozmanité přírodní jevy a předpověděli, jak se budou vyvíjet v čase. Mnohé z těchto rovnic obsahují též stochastické členy vyjadřující jistou nahodilost. Široké spektrum moderních aplikací deterministických i stochastických evolučních rovnic popisuje pohyby planet, oceánské proudy, fyziologické cykly, populační dynamiku, elektrické obvody aj. Přitom chování některých systémů lze předpovědět s vysokou přesností, zatímco jiné se zdají být chaotické s naprosto nepředvídatelným chováním. Takto je řád a chaos důvěrně spojen. Můžeme najít chaotické chování v deterministických systémech (viz např. [8, s. 202]). Na druhé straně statistická analýza může zase vést k některým definitivním předpovědím (srov. [15]).

U většiny dynamických systémů máme dobrý přehled o tom, co udělá systém na krátkých časových intervalech, zatímco dělat dlouhodobé předpovědi je velice obtížné. Typickým příkladem je problém předpovědi počasí, když máme v pevném čase zadáno rozložení teploty, tlaku, vlhkosti apod., což je bod ve fázovém prostoru. Správná předpověď počasí na 10 minut dopředu je jistě mnohem realističtější než na 10 dní.

V roce 1982 J. Sinaj napsal společně s I. P. Cornfeldem a slavným ruským matematikem S. V. Fominem obsáhlou monografii [3] o ergodické teorii. Sergej Vasiljevič Fomin se bohužel jejího vydání nedožil. Ergodická teorie studuje pohyby v tzv. *měřitelném prostoru* $(M, \mathfrak{S})$, kde M je daný abstraktní prostor a $\mathfrak{S}$ je σ -algebra podmnožin množiny M , tj. neprázdný množinový systém obsahující s každou množinou také její doplněk v M a s každým nejvýše spočetným systémem množin také jeho sjednocení. Na M se obvykle definuje míra μ a pak se uvažuje trojice $(M, \mathfrak{S}, \mu)$, jež se nazývá *prostorem s mírou*.¹ Pokud $\mu(M) = 1$, pak hovoříme o *pravděpodobnostním prostoru* a μ se jmenuje *pravděpodobnostní míra*.

Ergodická teorie se používá k řešení celé řady problémů. Jako příklad uveďme následující užitečné tvrzení z teorie čísel, které lze dokázat právě pomocí ergodické teorie (viz [3, s. 159]). K tomuto účelu nejprve připomeňme, že posloupnost reálných čísel $x_1, x_2, \dots$, $0 \leq x_n \leq 1$, je *rovnoměrně rozložená* v uzavřeném intervalu $[0, 1]$,

¹Prostor s mírou (angl. measure space) je tedy speciálním případem měřitelného prostoru (angl. measurable space).

jestliže pro každou spojitou funkci f z prostoru $C([0, 1])$ platí následující rovnost

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n f(x_j) = \int_0^1 f(x) dx.$$

Označme ještě

$$\{x\} = x - [x],$$

kde $[x]$ je celá část reálného čísla x .

Věta. *Necht' $m \geq 1$ a $P(x) = a_0x^m + a_1x^{m-1} + \dots + a_m$ je polynom s reálnými koeficienty, z nichž alespoň jeden koeficient a_k je iracionální pro $0 \leq k < m$. Pak je posloupnost $x_n = \{P(n)\}$ pro $n = 1, 2, \dots$ rovnoměrně rozložená v intervalu $[0, 1]$.*

Kdyby všechny koeficienty a_k pro $0 \leq k < m$ byly racionální čísla, potom by podobné tvrzení evidentně neplatilo.

Jakov Sinaj učinil mnoho fundamentálních objevů v oblasti dynamických systémů a našel překvapivé souvislosti mezi řádem a chaosem (podobně jako desátý laureát Abelovy ceny Endre Szemerédi, viz [7, s. 78]). Podstatně tak obohatil ergodickou teorii,² která vyšetřuje tendenci dynamického systému projít všemi svými možnými stavy podle určité časové statistiky. Ve statistické mechanice zase zkoumal chování velkého systému částic (např. molekul v plynu).

První důležitý Sinajův výsledek byl inspirován jeho školitelem Kolmogorovem. Jednalo se o nalezení jistého invariantu dynamického systému, který později dostal jméno *Kolmogorovova–Sinajova entropie*. Tento pojem nyní hraje důležitou roli při studiu složitosti systému pomocí teoretického popisu trajektorií založeného na pojmu míry. Sinaj tak jako první položil základy ke klasifikaci složitosti daného dynamického systému. Kolmogorovova–Sinajova entropie měří nepředvídatelnost chování daného dynamického systému. Čím je nepředvídatelnost systému vyšší, tím je vyšší i jeho entropie.

Pojem Kolmogorovova–Sinajova entropie zobecňuje Shannonovu entropii, známou z teorie informace, kde zpráva je nekonečná posloupnost symbolů z dané abecedy (tj. fázového prostoru). Posun v řetězci

²Ergodické teorii se věnovala také Maryam Mirzakhaniová (1977–2017) ze Stanfordovy univerzity (viz [9]), která v roce 2014 jako první žena v historii získala Fieldsovu medaili za matematiku. Byla snachou bývalého předsedy České astronomické společnosti Jana Vondráka.

o jeden symbol vpřed určuje dynamiku systému. Shannonova entropie měří, jaký symbol můžeme předvídat v následujícím kroku. Nepředpověditelnost následujícího symbolu je tak vlastně ekvivalentní nové informaci.

12.4 Entropie binárních posloupností

Uvažujme dynamický systém, jehož stavový prostor se skládá ze všech nekonečných binárních posloupností, tj. posloupností nul a jedniček. Jeho dynamika bude dána operátorem posunutí. Tento systém se nazývá *Bernoulliovo schéma* po velkém matematikovi 17. století Jacobu Bernoulliovi.

Jako konkrétní příklad budeme vyšetřovat následující konečnou binární posloupnost délky 50:

$$11010010001010111011011000101010100011100110100011. \quad (12.1)$$

Položme si otázku, zda byla posloupnost (12.1) vygenerována náhodně.

Nejprve uveďme několik zjevných skutečností:

1. Uvažovaná posloupnost obsahuje 25 nul a stejný počet jedniček.
2. Na 30 místech se mění 0 na 1 nebo naopak. Na 19 místech je cifra stejná jako na předchozí pozici. Ve zcela náhodné posloupnosti by se tyto počty měly k sobě blížit.
3. Posloupnost (12.1) obsahuje 6 podposloupností tří stejných cifer, ale žádnou podposloupnost čtyř stejných cifer, tj. 0000 nebo 1111. Přitom v náhodně generované binární posloupnosti délky 50 bude existovat podposloupnost se čtyřmi stejnými ciframi s pravděpodobností cca 98 %. Tento fakt naznačuje, že posloupnost (1) patrně nebyla náhodně vygenerována.

Pravda je taková, že posloupnost (12.1) byla vytvořena zkusmo tak, aby vypadala jako náhodná. Jak ale ukazuje předchozí analýza, změna cifer probíhala příliš často.

Pokud vygenerujeme binární posloupnost zcela náhodně,³ pak výskyt 0 či 1 má zřejmě pravděpodobnost $p = \frac{1}{2}$. V uvažovaném příkladu

³Statistické vlastnosti generátorů náhodných čísel jsou například studovány v článku [1].

se skutečně zdá, že výskyt 0 a 1 má stejnou pravděpodobnost. Četnost výskytu dvojic 01 a 10 je 60 %, zatímco jen 40 % připadá na dvojice 00 a 11. Tento rozdíl v předpovědi je kvantifikován v entropii systému. Jak již bylo řečeno, čím je chování systému méně předvídatelné, tím má systém větší entropii. Zcela náhodná binární posloupnost má entropii $\ln 2 = 0.693147\dots$. Entropie posloupnosti (12.1) je 0.673, což je jen o trochu menší hodnota. Entropie obecného Bernoulliho schématu se dvěma hodnotami s pravděpodobnostmi p a $1 - p$ je dána vztahem

$$E = -p \ln p - (1 - p) \ln(1 - p).$$

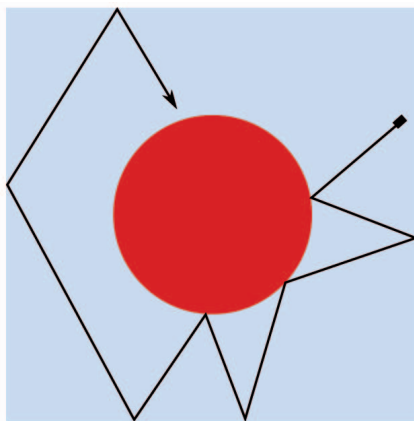
Bernoulliho schéma může mít více hodnot. Například množina všech nekonečných posloupností z velkých písmen anglické abecedy jich má 26. Známý matematik John von Neumann si kladl záludnou otázku, zda je možné, aby dvě strukturně odlišná Bernoulliho schémata dávala stejné výsledky. Jako příklad uvažujme dvě Bernoulliho schémata $BS(\frac{1}{2}, \frac{1}{2})$ a $BS(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, kde zlomek označuje pravděpodobnost výskytu příslušného písmena abecedy v Bernoulliho schématu $BS(\dots)$.

Problém vyřešil Donald Ornstein [10] v roce 1970. Odpověď na von Neumannovu otázku zní NE, a tedy dvě strukturně různá Bernoulliho schémata dávají odlišné výsledky. Základem pro toto tvrzení⁴ je Sinajova a Kolmogorovova idea z roku 1959. Zde je třeba poznamenat, že Kolmogorovova–Sinajova entropie je právě to, co separuje různá Bernoulliho schémata.

12.5 Sinajův kulečník

Dynamický kulečník je matematická idealizace skutečného kulečníku, kde stůl nemusí mít jen obdélníkový tvar a může být navíc vícerozměrný (viz [3, s. 143] pro polyedrické či polytopické oblasti). Přesněji řečeno, příslušný dynamický systém popisuje trajektorii pohybujícího se nehmotného bodu v ohraničené oblasti s hranicí po částech hladkou. Mimo hranici se částice pohybuje přímočaře stále stejnou konstantní rychlostí. Při nárazu na hladkou část hranice se odrazí podle klasického zákona odrazu, kdy úhel odrazu je stejný jako úhel dopadu.

⁴Ornsteinova věta o izomorfismu Bernoulliových automorfismů se stejnou entropií je elegantněji dokázána v monografii [3]. Zde uváděný důkaz se liší od původního Ornsteinova důkazu [10].



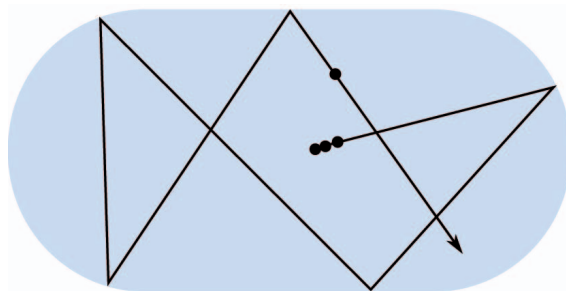
Obr. 12.2 Sinajův kulečnick (nakreslila H. Bílková)

Pravděpodobnost dopadu částice na vrchol, hranu apod. je rovna nule. Tento případ je třeba vyšetřovat individuálně (viz [3, s. 138]).

Sinajův kulečnick (viz např. [3], [11]) je znázorněn na obr. 12.2. Tento zjednodušený model vznikl při studiu chování molekul ideálního plynu v uzavřené nádobě. Sinaj jej navrhl jako příklad interagujícího hamiltonovského systému, který znázorňuje jisté termodynamické vlastnosti (má kladné Ljapunovovy exponenty a všechny trajektorie jsou ergodické), a proto se mu někdy též říká Lorentzův plyn. Systém má zdánlivě chaotické chování. Pomocí tohoto modelu Sinaj objevil, že chování molekul ideálního plynu se řídí trajektoriemi Hadamardova dynamického systému z článku z roku 1898. To byla první práce, která se systematicky zabývala matematickým chaosem.

Dynamický kulečnick lze zobecňovat různými způsoby. Místo rovinného kulečnicku můžeme uvažovat i dvojrozměrnou varietu s nenulovou křivostí (např. hemisféru). Přímočaré pohyby nehmotného bodu jsou pak nahrazeny rovnoměrným pohybem podél geodetik, což jsou zhruba řečeno nejkratší spojnice mezi dvěma různými body. Jedná se však stále o deterministický systém, protože trajektorie je jednoznačně určena počáteční polohou a směrem.

V klasickém obdélníkovém kulečnicku žádné chaotické chování nenastává. Malá změna počátečních podmínek způsobí podstatnou odchylku v trajektorii na určitém časovém intervalu, kde ale odchylka bude lineární funkcí času. Chaotické chování je však charakterizováno exponenciálním růstem odchylky, což právě Sinajův kulečnick splňuje.



Obr. 12.3 Bunimovičův kulečnick (nakreslila H. Bílková)

Původně existovala hypotéza, že chaotické chování je způsobeno konkávním tvarem vnitřní hranice (viz obr. 12.2). Pak ale v roce 1979 Leonid Bunimovič [2] dokázal, že pro konvexní kulečnick ve tvaru atletického stadionu (viz obr. 12.3) také dostáváme chaotické chování trajektorií.

12.6 Několik poznámek na závěr

Koncem 50. let minulého století organizoval Andrej N. Kolmogorov (1903–1987) na MGU sérii seminářů věnovaných dynamickým systémům. Během nich často padala otázka, zda je možno najít strukturální podobnost dvou různých dynamických systémů. Mladý účastník semináře Jakov Sinaj tehdy vyřešil kladně tento problém pomocí pojmu entropie dynamického systému. I svými dalšími výsledky významně obohatil teorii dynamických systémů. Pomocí pojmu entropie umožnil jejich klasifikaci a lepší chápání jejich složitosti. Jeho manželka Jelena B. Vulová je také matematicka a fyzička. Společně napsali několik prací publikovaných v renomovaných mezinárodních časopisech.

Převážná většina Sinajových prací se týká řešení problémů matematické fyziky, Schrödingerovy rovnice, Navierových–Stokesových rovnic, Lorentzova plynu, Markovových procesů, kulečnickových trajektorií, invariantních a Gibbsových měr, stochastických operátorů, diferenciální geometrie, teorie čísel, teorie chaosu, teorie stochastických modelů dynamiky tekutin (srov. též [4]), ergodické teorie a dynamických systémů. Na tato témata napsal několik monografií (viz např. [3], [12], [13]) a přes 200 vědeckých článků, evidovaných databází Mathematical Reviews a Zentralblatt für Mathematik.

L i t e r a t u r a

- [1] BALKOVÁ, Ľ., HLADKÝ, J.: *Generátory pseudonáhodných čísel založené na nekonečných slovech*. PMFA 59 (2014), 211–222.
- [2] BUNIMOVICH, L. A.: *On the ergodic properties of nowhere dispersing billiards*. Comm. Math. Phys. 65 (1979), 295–312.
- [3] CORNFELD, I. P., FOMIN, S. V., SINAI, Y. G.: *Ergodic theory*. Springer-Verlag, New York, Heidelberg, Berlin 1982.
- [4] FLANDOLI, F., MASLOWSKI, B.: *Ergodicity of the 2-D Navier–Stokes equation under random perturbations*. Comm. Math. Phys. 171 (1995), 119–141.
- [5] HOLDEN, H., RIENE, R. (Eds): *The Abel Prize 2003–2007. The first five years*. Springer-Verlag, Berlin, New York 2009.
- [6] KRÍŽEK, M., MARKL, M., SOMER, L.: *V roce 2013 získal Abelovu cenu Pierre Deligne za fundamentální práce svazující algebru a geometrii*. PMFA 58 (2013), 265–273.
- [7] KRÍŽEK, M., SOMER, L., MARKL, M., KOWALSKI, O., PUDLÁK, P., VRKOČ, I.: *Prvních deset Abelových cen za matematiku*. JČMF, Praha 2013.
- [8] KRÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Academia, Praha 2009; druhé vydání 2011.
- [9] MIRZAKHANI, M.: *Ergodic theory of the earthquake flow*. Int. Math. Res. Not. (2008), Art. ID rnm16, 39 pp.
- [10] ORNSTEIN, D.: *Bernoulli shifts with the same entropy are isomorphic*. Adv. Math. 4 (1970), 337–352.
- [11] SINAI, Y. G.: *Dynamical systems with elastic reflections. Ergodic properties of dispersing billiards* (Russian). Uspechi Mat. Nauk 25 (1970), 141–192.
- [12] SINAI, Y. G.: *Introduction to ergodic theory*. Math. Notes 18, Princeton Univ., NJ 1976.
- [13] SINAI, Y. G.: *Theory of phase transitions (Russian)*. Nauka, Moskva 1980.

- [14] SINAI, Y. G.: *Mathematicians and physicists = Cats and dogs?* Bull. Amer. Math. Soc. *43* (2006), 563–565; český překlad viz PMFA *59* (2014), 274–276.
- [15] VEJCHODSKÝ, T.: *Stochastické modely v biochemii. Je život jen náhoda?* PMFA *59* (2014), 277–284.
- [16] <http://www.abelprisen.no/en/>

13. Abelovu cenu za matematiku získali v roce 2015 John F. Nash a Louis Nirenberg

Michal Křížek

13.1 Prolog

Dne 25. března 2015 oznámila prezidentka Norské akademie věd Kristi S. Bullová, že v pořadí již třináctou Abelovu cenu¹ získají američtí matematici John F. Nash a Louis Nirenberg za překvapivé a původní



JOHN F. NASH a LOUIS NIRENBERG

¹O předchozích Abelových cenách pojednávají též práce [5], [6], [7] a [12].

příspěvky k teorii nelineárních parciálních diferenciálních rovnic a její aplikace na geometrickou analýzu (viz [25]). V pondělí 18. května byli oba laureáti pozváni do královského paláce v Oslu. Následující den pak převzali Abelovu cenu² od Jeho Veličenstva norského krále Harald V. v hlavní aule univerzity v Oslu. Večer se konal slavnostní banket na zámku v Akershusu, kam je pozval norský ministr pro vzdělávání a vědu Torbjørn Røe Isaksen. Výběrová komise pro Abelovu cenu se skládala z pěti vynikajících matematiků, byla stejná jako v roce 2014.

13.2 Stručný životopis Johna F. Nashe

John Forbes Nash junior se narodil 13. června 1928 v Bluefieldu v západní Virginii. V době dospívání absolvoval Carnegie Institute of Technology v Pittsburghu. Svůj první článek *The bargaining problem* [13] napsal jako student druhého semestru na Princetonské univerzitě.

Většinu své profesionální kariéry strávil John Nash na Princetonské univerzitě a na Massachusetském technologickém ústavu (MIT). Byl uznáván zejména za práce v oblasti teorie her a diferenciální geometrie. V roce 1994 získal Nobelovu cenu za ekonomii, kterou společně s ním dostali i další dva matematici, Reinhard Selten a John Harsanyi. Nobelovský výbor ocenil zejména Nashovy práce týkající se tzv. Nashovy rovnováhy, o níž se zmíníme v následující kapitole. Mezi další jeho významná ocenění patří Neumannova cena (John von Neumann Theory Prize, 1978) a Steelova cena Americké matematické společnosti (1999).

Nashův životní příběh je zachycen v oscarovém filmu *A Beautiful Mind*, který čeští diváci mohli zhlédnout pod názvem *Čistá duše*. Film vypráví o jeho boji s paranoidní schizofrenií. V roce 2001 jej natočil režisér Ron Howard podle scénáře Akivy Goldsmana. Role Nashe se zhostil herec Russell Crowe.

John Nash bohužel nešťastně zemřel společně se svou manželkou Alicí dne 23. května krátce po převzetí Abelovy ceny. Při cestě z Norska domů měli těžkou havárii v taxíku v New Jersey [20]. V době nehody manželé neměli zapnuté bezpečnostní pásy.

²Ocenění bylo spojeno s peněžitou odměnou 3 milionů norských korun pro každého laureáta.

13.3 Vybrané vědecké výsledky Johna F. Nashe

Nobelovu cenu získal John F. Nash zejména za práce týkající se teorie her, které mají uplatnění v ekonomii a sociologii. Existují hry pro více hráčů takové, že prohrává ten, kdo je první na tahu. Mějme například řadu 13 kamenů a každý ze dvou hráčů z ní bere 1, 2 nebo 3 kameny. Oba hráči se střídají a prohrává ten, kdo sebere poslední kámen. Vítězná strategie druhého hráče je tato:

Jestliže první hráč vezme $x \in \{1, 2, 3\}$ kamenů, pak druhý musí vzít $4 - x$ kamenů. Potom zřejmě první hráč prohraje, jak plyne z diagramu:

• • • • • | • • • • • | • • • • • | •

To pak vyvolává jakousi přirozenou rovnováhu, protože při zahájení hry nikdo nechce táhnout jako první, aby neprohrál.

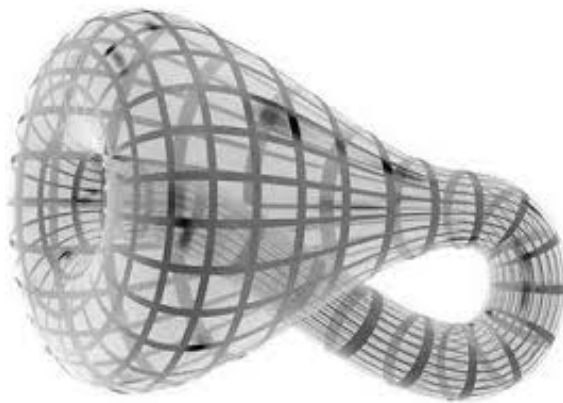
Nashova rovnováha je v teorii her taková situace, kdy žádný z hráčů nemůže jednostrannou změnou zvolené strategie vylepšit svoji situaci [14]. Současně se jedná i o koncept řešení nekooperativních her více hráčů [15]. John Nash dokázal, že každá konečná hra má alespoň jedno takové řešení.

Abelovu cenu získal J. Nash za práce o teorii nelineárních parciálních diferenciálních rovnic a její aplikace na geometrickou analýzu. V roce 1954 publikoval v *Annals of Mathematics* zcela zásadní článek [16]. Jeho na tehdejší dobu velice překvapivé výsledky se týkají izometrických³ vnoření (angl. immersion) a vložení⁴ (angl. imbedding) Riemannových variet s pozitivně definitní metrikou do k -rozměrných eukleidovských prostorů $\mathbb{E}^k$. Na ukázkou uveďme některé důležité matematické výsledky z Nashovy práce [16]:

Věta 1. *Pro každou uzavřenou n -rozměrnou Riemannovu varietu existuje izometrické C^1 -vložení do $\mathbb{E}^{2n}$.*

³Izometrie je zobrazení zachovávající vzdálenosti.

⁴Příslušné definice lze najít v kap. 7.3 a v [11, s. 137–138]. Poznamenejme, že při vložení je vzor difeomorfní se svým obrazem. Přitom každé vložení je zároveň vnoření, ale obrácená inkluze neplatí. Při vnoření je vzor pouze lokálně difeomorfní a obecně nemusí jít o vzájemně jednoznačné zobrazení globálně. Například známou Kleinovu láhev (ale i všechny další dvourozměrné neorientovatelné uzavřené plochy) lze vnořit do $\mathbb{E}^3$, kde se tato plocha protíná, ale nelze ji vložit do $\mathbb{E}^3$ (viz obr. 13.1).



Obr. 13.1 Kleinova láhev je uzavřená neorientovatelná plocha ve čtyřrozměrném eukleidovském prostoru $\mathbb{E}^4$, kterou lze vnořit do trojrozměrného prostoru $\mathbb{E}^3$. Nelze ji ale vložit do $\mathbb{E}^3$ (zdroj Wikipedia).

Věta 2. Pro každou n -rozměrnou Riemannovu varietu existuje izometrické C^1 -vnoření do $\mathbb{E}^{2n}$ a izometrické C^1 -vložení do $\mathbb{E}^{2n+1}$.

Věta 3. Pokud pro uzavřenou n -rozměrnou Riemannovu varietu existuje C^∞ -vnoření (resp. vložení) do $\mathbb{E}^k$ pro nějaké $k \geq n + 2$, pak existuje izometrické vnoření (resp. vložení) do $\mathbb{E}^k$.

Tato tvrzení rozšířil J. Nash na C^3 -vložení v pokračování [17] uveřejněném rovněž v Annals of Mathematics.

Dále popíšeme jednu úlohu z oblasti nelineárních parciálních diferenciálních rovnic, kterou se John Nash podrobně zabýval. Zatímco teorie lineárních parciálních rovnic je v podstatě uzavřenou disciplínou, teorie nelineárních rovnic se stále buduje. Každá třída nelineárních problémů se totiž musí vyšetřovat individuálně. K tomuto účelu je třeba vyvinout speciální důkazové techniky využívající příslušný tvar nelinearity. V článku [19] John Nash vyšetřuje nelineární úlohu proudění viskózní tepelně vodivé stlačitelné tekutiny

$$\begin{aligned} \frac{d\rho}{dt} &= -\rho \nabla \cdot v, \\ \frac{dv}{dt} &= -\frac{\nabla p}{\rho} + \frac{1}{\rho} \frac{\partial \sigma'_{ik}}{\partial x_k} + F(x, t), \\ \rho T \frac{dS}{dt} &= \nabla \cdot (\kappa \nabla T) + \frac{\eta}{2} \left[\frac{\partial v_i}{\partial x_k} + \frac{\partial v_k}{\partial x_i} + \frac{2}{3} \delta_{ik} \frac{\partial v_l}{\partial x_l} \right] \zeta (\nabla \cdot v)^2, \end{aligned} \tag{13.1}$$

kde

$$\sigma'_{ik} = \eta \left(\frac{\partial v_i}{\partial x_k} + \frac{\partial v_k}{\partial x_i} \right) + \left(\zeta - \frac{2}{3} \eta \right) \delta_{ik} \frac{\partial v_l}{\partial x_l},$$

T je teplota a ρ hustota tekutiny, $v = (v_1, v_2, v_3)$ je její rychlost, p je tlak, F je hustota vnějších objemových sil, η a ζ jsou koeficienty viskozity⁵, S je entropie a $d/dt = \partial/\partial t + v_k \partial/\partial x_k$ je lagrangeovská časová derivace se standardní Einsteinovou sumační konvencí. Nash předpokládá, že entropie závisí na hustotě i teplotě (tj. $S = S(\rho, T)$). Pro teplotu pak odvozuje další parciální diferenciální rovnici, kterou využije k důkazu existence a jednoznačnosti řešení soustavy (13.1) za jistých předpokladů na data úlohy.

13.4 Stručný životopis Louise Nirenberga

Louis Nirenberg se narodil dne 28. února 1925 v kanadském Hamiltonu. Matematiku a fyziku studoval na McGillově univerzitě v Montrealu a získal titul bakaláře. Magisterský titul obdržel na Newyorské státní univerzitě. Na konci války působil v National Research Council of Canada, kde pracoval v matematickém oddělení, které založil fyzik Ernest Courant, syn slavného matematika Richarda Couranta. Nirenberg pak získal místo v Courantově matematickém ústavu Newyorské státní univerzity. V roce 1957 se stal profesorem a v letech 1970–1972 působil ve funkci ředitele Courantova ústavu. Připomeňme, že laureáti Abelovy ceny P. Lax, Š. Varadhan a M. Gromov též pracovali v Courantově ústavu.

L. Nirenberg má za sebou dlouhou a úspěšnou matematickou kariéru. Mnoho výsledků nese jeho jméno, např. Gagliardovy–Nirenbergovy interpolační nerovnosti, Nirenbergova teorie pseudodiferenciálních operátorů, Caffarelliovy–Kohnovy–Nirenbergovy nerovnosti, Johnova–Nirenbergova nerovnost či Johnův–Nirenbergův prostor. Za své matematické výsledky získal L. Nirenberg Bôcherovu medaili Americké matematické společnosti (1959), Crafoordovu cenu Švédské královské akademie věd (1982), Jefferyovu–Williamsovu cenu (1987), Steelovu cenu Americké matematické společnosti (1994, 2014), Chernovu medaili od Mezinárodní matematické unie (2010) aj. Další životopisné údaje lze nalézt v článku [8].

⁵Koeficient η se anglicky nazývá shear viscosity a ζ bulk viscosity.

13.5 Vybrané vědecké výsledky Louise Nirenberga

Mezi nejdůležitější Nirenbergovy práce patří článek [21], který sepsal se svým studentem Augustem Newlanderem o komplexních strukturách a který vyšel v *Annals of Mathematics* v roce 1957. V článku [1] z roku 1959 Louis Nirenberg se Shmuelem Agmonem a Avronem Douglisem vytvořil teorii regularity řešení eliptických rovnic. Pak v roce 1961 společně s Fritzem Johnem zavedl v [9] nové speciální funkcionální prostory (*functions with bounded mean oscillation*). V další významné práci [10] z roku 1978 se Nirenberg s Davidem Kinderlehrerem a Joelem Spruckem zabýval regularitou řešení okrajových problémů s volnou hranicí.

O rok později napsal Louis Nirenberg s Basilisem Gidasem a Wei Ming Niem zcela zásadní článek o symetriích řešení nelineárních parciálních diferenciálních rovnic [4], který získal okolo tisíce citací. Na ukázkou si z něj uveďme typickou větu.

Věta 4. *Nechť $u \in C^2(\overline{\Omega})$ je řešení úlohy*

$$\Delta u + f(u) = 0 \quad \text{a} \quad u = 0 \quad \text{pro} \quad |x| = R,$$

kde $\Omega = \{x \in \mathbb{R}^n; |x| < R\}$ je koule a f je třídy C^1 . Je-li $u > 0$ na Ω , pak řešení u je sféricky symetrické a $\partial u / \partial r < 0$ pro všechna $r \in (0, R)$.

Autoři tuto větu dále zobecňují na prstencové oblasti a také na evoluční parabolické úlohy typu

$$-\frac{du}{dt} + \Delta u + f(t, r, u) = 0 \quad \text{a} \quad u = 0 \quad \text{pro} \quad |x| = R$$

s vhodnými počátečními podmínkami.

V roce 1983 napsal Louis Nirenberg s Haïmem Brezisem další důležitý článek⁶ o kladných řešeních nelineárních parciálních diferenciálních rovnic [2], který rovněž získal okolo tisíce citací. Jeho autoři uvažují na ohraničené oblasti $\Omega \subset \mathbb{R}^n$ pro $n \geq 3$ nelineární eliptickou okrajovou úlohu

$$-\Delta u = u^p + f(x, u) \quad \text{v} \quad \Omega, \quad u > 0 \quad \text{v} \quad \Omega, \quad u = 0 \quad \text{na} \quad \partial\Omega, \quad (13.2)$$

⁶Profesor Brezis přednášel o těchto výsledcích i v Matematickém ústavu ČSAV v Praze.

kde $p = (n + 2)/(n - 2)$, $f(x, 0) = 0$ a $f(x, u)$ je perturbace nízkého stupně vzhledem k u^p , tj.

$$\lim_{u \rightarrow \infty} \frac{f(x, u)}{u^p} = 0.$$

Variační řešení úlohy (13.2) se hledá v Sobolevově prostoru

$$H_0^1(\Omega) = \{v \in L^2(\Omega) ; \nabla v \in (L^2(\Omega))^n, v|_{\partial\Omega} = 0\}$$

a převádí se na minimalizaci funkcionálu

$$\Phi(u) = \int_{\Omega} \left(\frac{1}{2} |\nabla u|^2 - \frac{1}{p+1} |u|^{p+1} - F(x, u) \right) dx,$$

kde $F(x, u) = \int_0^u f(x, v) dv$. Poznamenejme, že pro exponent $p + 1 = 2n/(n - 2)$ není vnoření $H_0^1(\Omega) \subset L^{p+1}(\Omega)$ kompaktní, což je hlavním zdrojem potíží. Není totiž splněna Palaisova–Smaleova podmínka zaručující existenci kritických bodů funkcionálu Φ . Označíme-li λ_1 nejmenší vlastní číslo operátoru $-\Delta$ s homogenními okrajovými podmínkami, pak platí následující tvrzení [2]:

Věta 5. *Pro každé $n \geq 4$ a $\lambda \in (0, \lambda_1)$ má úloha (13.2) variační řešení pro $f(x, u) = \lambda u$.*

Věta 6. *Nechť $\Omega \subset \mathbb{E}^3$ je koule a $f(x, u) = \lambda u$. Pak má úloha (13.2) variační řešení právě tehdy, když $\lambda \in (\frac{1}{4}\lambda_1, \lambda_1)$.*

Hlavní výsledek obsáhlého článku [3] o lokální regularitě řešení Navierových–Stokesových rovnic

$$\begin{aligned} \frac{du}{dt} + u \cdot \nabla u - \Delta u + \nabla p &= f, \\ \nabla \cdot u &= 0 \end{aligned}$$

pro dané počáteční a okrajové podmínky na parabolickém válci

$$Q_r(x, t) = \{(y, \tau) ; |y - x| < r, t - r^2 < \tau < t\}$$

lze formulovat přibližně takto: pokud pro rychlost u a tlak p existují konstanty ε_1 a $\varepsilon_2 = \varepsilon_2(q)$ takové, že

$$\int \int_{Q_1} (|u|^3 + |u||p|) dx dt + \int_{-1}^0 \left(\int_{|x|<1} |p| dx \right)^{5/4} dt \leq \varepsilon_1$$

a

$$\iint_{Q_1} |f|^q \leq \varepsilon_2$$

pro nějaké $q > 5/2$, pak u je hladké na $Q_{1/2}$. Za tento článek získal Louis Nirenberg se spoluautory Luísem A. Caffarellim a Robertem V. Kohnem v roce 2014 Steelovu cenu Americké matematické společnosti za klíčový příspěvek k výzkumu.

13.6 Závěrečné poznámky

V důsledku vážné Nashovy choroby databáze Mathematical Reviews eviduje pouze 26 jeho vědeckých prací, které však získaly přes 1 600 citací. To je naprosto vynikající průměr na jednu práci. Přitom šest prací bylo publikováno v *Annals of Mathematics*. Každý z článků [15] a [18] získal kolem 300 citací. I když Nash nenapsal s Nirenbergem žádnou společnou práci, byl jím podstatně ovlivněn (viz např. [18]). John Nash psal většinou sám. Na druhé straně Louis Nirenberg psal hlavně se spoluautory. Publikoval přes 170 vědeckých článků, které eviduje databáze Mathematical Reviews. Získal na ně neuvěřitelných 10 000 citací od 5 800 autorů. K nejvíce citovaným článkům patří např. [2], [3], [4], [22], [23] a [24].

L i t e r a t u r a

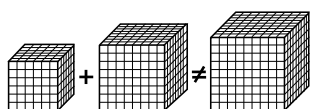
- [1] AGMON, S., DOUGLIS, A., NIRENBERG, L.: *Estimates near the boundary for solutions of elliptic partial differential equations satisfying general boundary conditions I*. Comm. Pure Appl. Math. 12 (1959), 623–727.
- [2] BRÉZIS, H., NIRENBERG, L.: *Positive solutions of nonlinear elliptic equations involving critical Sobolev exponents*. Comm. Pure Appl. Math. 36 (1983), 437–477.
- [3] CAFFARELLI, L., KOHN, R., NIRENBERG, L.: *Partial regularity of suitable weak solutions of the Navier–Stokes equations*. Comm. Pure Appl. Math. 35 (1982), 771–831.
- [4] GIDAS, B., NI, W. M., NIRENBERG, L.: *Symmetry and related properties via the maximum principle*. Comm. Math. Phys. 68 (1979), 209–243.

- [5] HELSVIG, K.: *The Abel Prize: The missing Nobel in mathematics?*
- [6] HOLDEN, H., RIENE, R. (Eds): *The Abel Prize 2003–2007. The first five years.* Springer-Verlag, Berlin, New York, 2009.
- [7] HOLDEN, H., RIENE, R. (Eds): *The Abel Prize 2008–2012.* Springer-Verlag, Berlin, New York, 2014.
- [8] JACKSONOVÁ, A.: *Rozhovor s Louisem Nirenbergem.* PMFA 60 (2015), 284–293.
- [9] JOHN, F., NIRENBERG, L.: *On functions of bounded mean oscillation.* Comm. Pure Appl. Math. 14 (1961), 415–426.
- [10] KINDERLEHRER, D., NIRENBERG, L., SPRUCK, J.: *Regularity in elliptic free boundary problems.* J. Anal. Math. 34 (1978), 86–119.
- [11] KOWALSKI, O., KŘÍŽEK, M., PRAVDA, V.: *Nejsymetričtější variety.* PMFA 59 (2014), 135–145.
- [12] KŘÍŽEK, M., SOMER, L., MARKL, M., KOWALSKI, O., PUDLÁK, P., VRKOČ, I.: *Prvních deset Abelových cen za matematiku.* JČMF, Praha, 2013.
- [13] NASH, J.: *The bargaining problem.* Econometrica 18 (1950), 155–162.
- [14] NASH, J.: *Equilibrium points in n -person games.* Proc. Natl. Acad. Sci. USA 36 (1950), 48–49.
- [15] NASH, J.: *Non-cooperative games.* Ann. of Math. 54 (1951), 286–295.
- [16] NASH, J.: *C^1 isometric imbeddings.* Ann. of Math. 60 (1954), 383–396.
- [17] NASH, J.: *The imbedding problem for Riemannian manifolds.* Ann. of Math. 63 (1956), 20–63.
- [18] NASH, J.: *Continuity of solutions of parabolic and elliptic equations.* Amer. J. Math. 80 (1958), 931–954.
- [19] NASH, J.: *Le problème de Cauchy pour les équations différentielles d'un fluide général.* Bull. Soc. Math. France 90 (1962), 487–497.
- [20] *Nash and Nirenberg awarded 2015 Abel Prize.* Notices Amer. Math. Soc. 62 (2015), 670–672.

- [21] NEWLANDER, A., NIRENBERG, L.: *Complex analysis coordinates in almost complex manifolds*. Ann. of Math. 65 (1957), 391–404.
- [22] NIRENBERG, L.: *On elliptic partial differential equations*. Ann. Scuola Norm. Sup. Pisa 13 (1959), 115–162.
- [23] NIRENBERG, L.: *Topics in nonlinear functional analysis*. With a chapter by E. Zehnder. Notes by R. A. Artino. Lecture Notes, 1973–1974. Courant Institute of Mathematical Sciences, New York University, New York, 1974, viii+259 pp.
- [24] NIRENBERG, L.: *Topics in nonlinear functional analysis*. Chapter 6 by E. Zehnder. Notes by R. A. Artino. Revised reprint of the 1974 original. Courant Lecture Notes in Mathematics, 6. New York University, Courant Institute of Mathematical Sciences, New York; American Mathematical Society, Providence, RI, 2001, xii+145 pp.
- [25] <http://www.abelprisen.no/en/>

14. Abelova cena v roce 2016 udělena za důkaz Velké Fermatovy věty

Michal Krížek, Lawrence Somer



*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...*

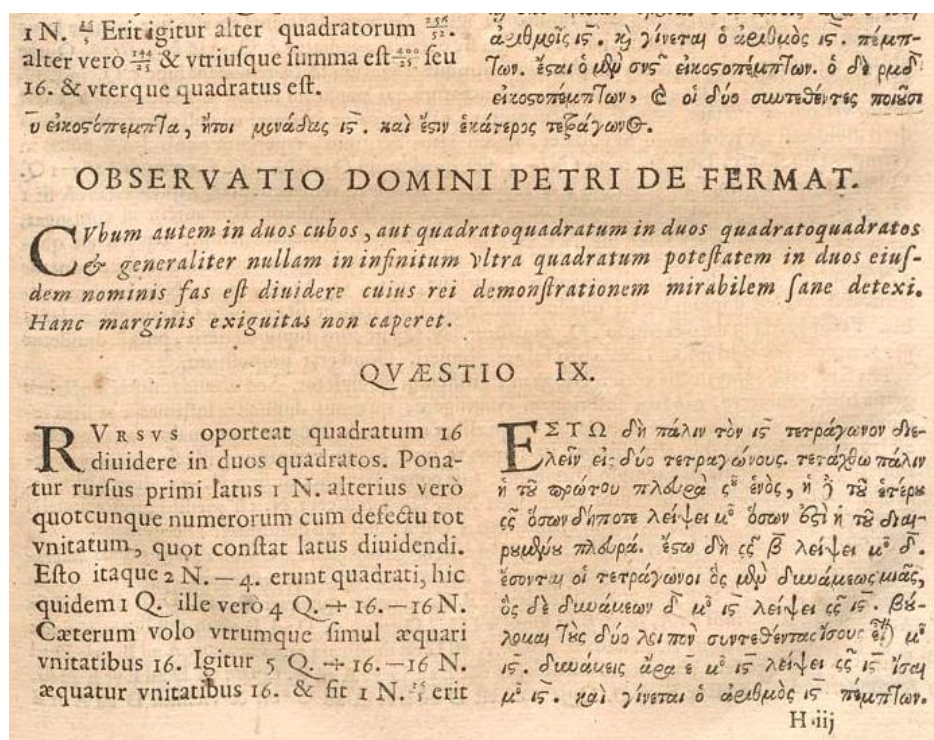
PIERRE DE FERMAT

14.1 Prolog

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



ANDREW WILES



Obr. 14.1 Ukázka z rozšířeného vydání Diofantovy *Aritmetiky* se slavnou poznámkou Pierra de Fermata (zdroj Wikipedia)

modulární domněnky pro semistabilní eliptické křivky a za otevření nové epochy výzkumu v teorii čísel [41].

Francouzský matematik Pierre de Fermat (1601–1665) si v roce 1637 připsal na okraj svého exempláře¹ Bachetova vydání Diofantovy *Aritmetiky* poznámku, kterou uvádíme v záhlaví této kapitoly.² Za ní pak připsal: ... *cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet*, což volně přeloženo zna-

¹V roce 1670 Samuel de Fermat, syn Pierra de Fermata, publikoval ve francouzském Toulouse monografii *Diophanti Alexandrini arithmeticonum*, prvně vydanou v Paříži (Sebastiani Cramoisy) v roce 1921, kterou rozšířil právě o poznámky svého otce, viz obr. 14.1.

²Je 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.)



Obr. 14.2 Hlavní aula univerzity v Oslu se nachází v blízkosti královského paláce a sochy N. H. Abela (foto S. Korotov).

mená: *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*

$$x^n + y^n = z^n. \quad (14.1)$$

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

V úterý 24. května 2016 A. Wiles převzal Abelovu cenu z rukou norského korunního prince Haakona Magnuse v hlavní aule na univerzitě v Oslu (viz obr. 14.2 a 14.3). 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.

³Ve Fermatově pozůstalosti zmíněný důkaz nalezen nebyl.



Obr. 14.3 Sir Andrew Wiles (vlevo) a norský korunní princ Haakon Magnus (vpravo) při předávání Abelovy ceny (zdroj <http://www.abelprize.no/>)

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. 14.4 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. Henri Darmon posluchačům vysvětlil koncept Heckeho algeber, který byl k důkazu použit (viz [38]).

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 7 problémů tisíciletí. Na vyřešení každého z nich vypsal Clayův matematický ústav odměnu 1 000 000 dolarů.

Birchova–Swinnertonova–Dyerova domněnka zhruba řečeno tvrdí,⁴ že pro eliptickou křivku E hodnoty r je $\prod_{p \leq x} N_p/p \sim c(\log x)^r$, kde N_p označuje počet bodů na $E \pmod{p}$. 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. (14.13) 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. [34]). Během svého vystoupení zdůraznil, že jediná diofantická rovnice $x^2 + y^2 = z^2$ má nekonečně mnoho řešení (srov. (14.8) níže), zatímco nekonečně mnoho diofantických rovnic $x^n + y^n = z^n$ pro $n \geq 3$ 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 zámekem 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, 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 ...*

14.2 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.

⁴V kapitole 14.4 se budeme věnovat grupě racionálních bodů na eliptických křivkách. Hodnota takové křivky je maximální počet nezávislých bodů $V_1, \dots, V_r$ nekonečného řádu. Zhruba řečeno, pokud $n_1 V_1 \oplus \dots \oplus n_r V_r = V_0$, kde $n_1, \dots, n_r$ jsou celá nezáporná čísla a V_0 je neutrální prvek vyšetřované grupy, pak platí $n_1 = \dots = n_r = 0$ (podrobnosti viz [33]). Nejvyšší známá hodnota je v současnosti 28. Body konečného řádu se nazývají *torzní*, protože po konečném počtu sčítání dostaneme neutrální prvek V_0 .



Obr. 14.4 Přednášející zleva: Simon Singh, sir Andrew Wiles, Manjul Bhargava a Henri Darmon (foto M. Křížek).

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 pracoval v Institutu des hautes études scientifiques v blízkosti Paříže a na École normale supérieure. Od roku 1988 do 1990 působil na přechodnou dobu jako profesor v oblasti výzkumu (angl. 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 ve-

řejně čítárně na Milton Road, kde našel 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 -domněnky⁵ pocházející od Kennetha Alana Ribeta z roku 1986, kterou již předtím Gerhard Frey spojil se slavnou Fermatovou rovnicí (14.1), viz kap. 14.6. 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 nezmiňoval⁶ 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 John 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 *Elíptické 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 dvoustetstránkový důkaz do časopisu *Inventiones Mathematicae*, jehož redaktor Barry Mazur z Harvardovy univerzity 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

⁵Této domněnce se dnes říká Ribetova věta, viz věta 5. Opírá se o Galoisovy reprezentace odpovídající modulárním formám (viz kap. 14.5). Jako první ji zformuloval Jean-Pierre Serre, pozdější nositel první Abelovy ceny.

⁶A. Wiles k otázce práce v ustraní prohlásil: *Zjistil jsem, že cokoliv souvisí s Velkou Fermatovou větou, vzbuzuje příliš mnoho zájmu. Pak se nemůžete dlouhodobě plně koncentrovat, protože by vás hodně zájemců vyrušovalo.*

dosti pravděpodobné, že se nějaká závažná chyba objeví. Po více než roce usilovné práce, když už chtěl Wiles odstraňování chyby vzdát, jej 19. září 1994 napadla hlavní myšlenka, jak důkaz opravit. Tehdy požádal o pomoc svého bývalého studenta Richarda Taylora⁷. Přepřacovaný důkaz („jen“ 130 stránek) pak vyšel v květnu 1995 ve dvou článcích [40] a [38] 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 cenu (1995), Wolfovu cenu (1995/96), Coleovu cenu (1997), Wolfskehlovu cenu⁸ (1997), stříbrnou plaketu Mezinárodní matematické unie (1998), Pythagorovu cenu (2004) a Shawovu cenu (2005). Budova univerzity v Oxfordu, v níž sídlí matematický ústav, byla po něm pojmenována a asteroid č. 9999 nese od roku 1999 jméno Wiles. V roce 1989 se A. Wiles stal spolupracovníkem Královské společnosti a v roce 2000 byl povýšen na rytíře Řádu Britského impéria. Jeho podrobný životopis je uveřejněn v knize Simona Singha [34].

14.3 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], [26], [28], [29], [34]. Také v PMFA byla tomuto tématu věnována velká pozornost, viz [11], [16], [22], [35] a [36].

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 (14.1) řešení pro nějaké $n = pq$, kde p je liché prvočíslo a $q > 1$, pak

$$x^{pq} + y^{pq} = (x^q)^p + (y^q)^p = (z^q)^p = z^{pq}. \quad (14.2)$$

Tudíž stačí položit $x' = x^q$, $y' = y^q$, $z' = z^q$ a vidíme, že rovnice (14.1) má řešení i pro $n = p$.

⁷R. Taylor obhájil Ph.D. v roce 1988 na univerzitě v Princetonu. Byl také jedním ze šestice recenzentů původního chybného Wilesova důkazu.

⁸V roce 1908 německý průmyslník Paul Wolfskehl vypsál odměnu 100 000 zlatých marek tomu, kdo jako první dokáže Velkou Fermatovu větu.

Podobně zjistíme, že pokud by existovalo nějaké řešení rovnice (14.1) pro $n = 2^k$, kde $k > 2$, pak by muselo existovat řešení i pro $n = 4$, neboť

$$x^{2^k} + y^{2^k} = \left(x^{2^{k-2}}\right)^4 + \left(y^{2^{k-2}}\right)^4 = \left(z^{2^{k-2}}\right)^4 = z^{2^k}. \quad (14.3)$$

Sám Fermat dokázal neexistenci řešení (14.1) jen pro $n = 4$, z čehož podle (14.3) okamžitě plyne, že rovnice (14.1) nemá řešení ani pro $n = 8, 16, 32, \dots$. Použil k tomu svoji oblíbenou metodu nekonečného sestupu (franc. descente infinie).

Věta 2 (Fermatova). *Bikvadratická rovnice*

$$x^4 + y^4 = z^4 \quad (14.4)$$

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 (14.4), 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

$$w^2 = z^4 - y^4 \quad (14.5)$$

v množině přirozených čísel. Nechť navíc řešení rovnice (14.5) je takové, že $z \in \mathbb{N}$ je nejmenší možné číslo. Takové z zřejmě existuje, neboť množina přirozených čísel je dobře uspořádaná, tj. každá její neprázdna podmnožina má minimální prvek. Pak pro největší společný dělitel čísel y a z platí

$$\gcd(y, z) = 1. \quad (14.6)$$

Kdyby totiž nějaké prvočíslo p dělilo y i z , pak bychom mohli rovnici $(p^2 w')^2 = (p z')^4 - (p y')^4$, 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 (14.6) 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

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

Obě čísla s a t musí být lichá, protože

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

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

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

Protože s a t jsou lichá, platí

$$\gcd(u, v) = 1. \quad (14.7)$$

Jelikož $uv = (s^2 - t^2)/4 = y^2/2$, máme $y^2 = 2uv$. Odtud podle vztahu (14.7) tedy existují $j, m \in \mathbb{N}$ tak, že platí buď

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

anebo

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

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 $k > l$ tak, že (viz např. [17, s. 54])

$$2j^2 = u = 2kl, \quad m^2 = v = k^2 - l^2, \quad z = k^2 + l^2. \quad (14.8)$$

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

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

a podle (14.8) tedy platí $m^2 = d^4 - e^4$. Ukázali jsme, že čísla $d, e, m \in \mathbb{N}$ rovněž splňují rovnici (14.5), 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 (14.5) a (14.6) je $\langle w, y^2, z^2 \rangle$ pythagorejská trojice nesoudělných čísel. Podobně jako v (14.8) existují nesoudělná přirozená čísla $k > l$ tak, že

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

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

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

Důkaz. Necht' $a, b \in \mathbb{N}$ jsou délky odvěsen pythagorejského trojúhelníka a necht' 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 (14.5) nemá celočíselné řešení, což je spor. $\square$

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.⁹*

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

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

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

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 $n = 3$.

⁹Přitom pravoúhlý trojúhelník s délkami odvěsen 3 a 4 má celočíselný obsah 6.

V jeho důkazu z roku 1770 však byla nalezena meze, kterou se naštěstí později podařilo zaplnit (viz [29, s. 30]). Případu $n = 3$ se věnovali i Christian Huygens, Karel Rychlík a mnoho dalších autorů¹⁰, viz např. [12], [21, s. 86], [28, s. 39], [39, s. 90].

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

$$x^3 + y^3 + z^3 = 0 \quad (14.9)$$

nemá řešení v množině nenulových celých čísel.

Důkaz. Předpokládejme naopak, že existují po dvou nesoudělná čísla x, y, z , pro něž platí (14.9), kde bez újmy na obecnosti jsou x a y lichá, z je sudé a $|z|$ je nejmenší možné. Pak

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

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

$$-z^3 = x^3 + y^3 = (a + b)^3 + (a - b)^3 = 2a(a^2 + 3b^2). \quad (14.10)$$

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. Rozlišujeme dva případy.

Případ 1: $\gcd(2a, a^2 + 3b^2) = 1$.

Podle (14.10) jsou $2a$ a $a^2 + 3b^2$ třetí mocniny

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

kde s je liché. Podle Eulera [7] pak existují¹¹ celá čísla u, v taková, že platí (viz [28, s. 40–42])

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

¹⁰Vlastní elegantní důkaz nedávno předložil středoškolský student Vojtěch Suchánek [37]. 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 (14.1) pro $n = 3$. Je-li totiž $x \equiv r \pmod{9}$, kde $r \in \{0, 1, \dots, 8\}$, pak $x^3 \equiv 0$ nebo $\pm 1 \pmod{9}$, což implikuje onu vlastnost.

¹¹Položíme-li $M = \{a^2 + 3b^2 \mid a, b \in \mathbb{Z}\} = \{0, 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, 25, 27, \dots\}$, 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 [28, s. 39]), že pokud $s^3 = a^2 + 3b^2 \in M$ pro nesoudělná čísla a a b , pak samotné s je stejného tvaru $s = u^2 + 3v^2 \in M$.

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

$$2u = -k^3, \quad u - 3v = l^3, \quad u + 3v = m^3,$$

kde celá čísla k, l, m jsou nenulová (protože jsou po dvou nesoudělná). Tedy

$$k^3 + l^3 + m^3 = 0,$$

kde k je sudé. Protože navíc $b \neq 0$ a $3 \nmid u$, z (14.10) 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 (14.10) máme

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

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

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

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

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

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

$$2v = -k^3, \quad u + v = l^3, \quad u - v = -m^3.$$

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

$$\begin{aligned} |z|^3 &= 18|c|(3c^2 + b^2) = 54|v(u^2 - v^2)|(3c^2 + b^2) = \\ &= 27|k|^3|u^2 - v^2|(3c^2 + b^2) \geq 27|k|^3 > |k|^3, \end{aligned}$$

což je opět ve sporu s minimalitou $|z|$. $\square$

Francouzská matematička Sophie Germainová [10] v roce 1819 dokázala, že rovnice (14.1) 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. (14.2)) nedělí žádného čitatele Bernoulliových čísel $B_0, B_1, \dots, B_{p-3}$ (viz též [36]). 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 (14.1).

V roce 1983 Gerd Faltings [8] dokázal slavnou *Mordellovu domněnku* (viz [28, s. 214], [36, s. 318]) z roku 1922, která tvrdí, že rovnice (14.1) 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 (14.1), je podán v článku [39].

Bylo nutno najít nějakou zcela novou metodu, která by zahrnovala všechny prvočíselné exponenty v (14.1) současně. V následujících třech kapitolách se stručně seznámíme se základními ingrediencemi Wilesova důkazu.

14.4 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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (14.11)$$

kde koeficienty a_i jsou racionální čísla.¹² Studium těchto křivek se matematikové věnují už dlouho, protože se mj. používají k vyjádření délky eliptických oblouků¹³ (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 (14.11) zjednodušit na tvar

$$y^2 = x^3 + b_2x^2 + 2b_4x + b_6, \quad (14.12)$$

kde b_i jsou vhodná racionální čísla. Pomocí další substituce $x \mapsto x - b_2/3$ reprezentující jen posunutí lze rovnici (14.12) zjednodušit na tvar (podobně jako při řešení kubických rovnic [27, s. 39])

$$y^2 = x^3 + Ax + B. \quad (14.13)$$

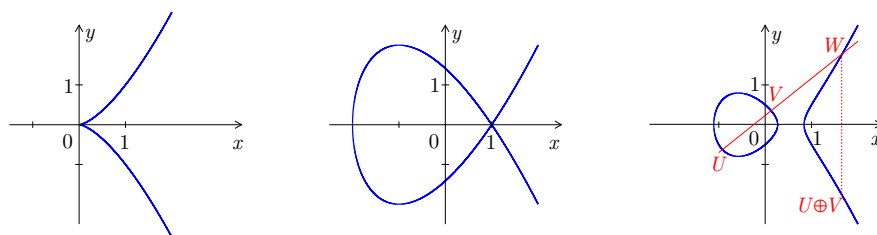
Odpovídající *diskriminant*

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

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. 14.5 vlevo). Je-li $\Delta = 0$ a $A \neq 0$, pak eliptická křivka (14.13) protíná sama sebe (viz obr. 14.5 uprostřed). Pokud $\Delta \neq 0$, pak má monický polynom $p(x) = x^3 + Ax + B$ tři různé kořeny; v opačném

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

¹³Vznik 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 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 [32].



Obr. 14.5 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 $U \oplus V$ (nakreslil F. Křížek).

případě má vícenásobný kořen. Je-li $\Delta < 0$, pak existuje jeden reálný a dva komplexně sdružené kořeny a eliptická křivka je souvislá (viz např. $y^2 = x^3 + 2$ nebo obr. 14.5 vlevo). Je-li $\Delta > 0$, pak existují jen reálné kořeny a eliptická křivka má dvě komponenty (viz obr. 14.5 vpravo).

Na bodech eliptické křivky (14.13) lze pro $\Delta \neq 0$ definovat grupu s operací $\oplus$ (viz obr. 14.5 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 kap. 8.4.

Je velice obtížné stanovit všechna celočíselná řešení $(x, y) \in \mathbb{Z}^2$ rovnice (14.11), viz [16, s. 94]. Na konkrétním příkladě si nyní ukážeme, jak lze eliptické křivky charakterizovat. Uvažujme eliptickou křivku

$$x^3 - x^2 = y^2 + y. \quad (14.14)$$

Její celočíselná řešení jsou

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

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

$$x^3 - x^2 \equiv y^2 + y \pmod{5} \quad (14.15)$$

navíc splněna pro

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

Snadno lze ověřit, že kongruence (14.15) 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 (14.14) tak můžeme jednoznačně přiřadit nekonečnou posloupnost

$$E_2 = 4, E_3 = 4, E_4 = 8, E_5 = 4, E_6 = 16, E_7 = 9, E_8 = 16, \dots \quad (14.16)$$

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 (14.13) 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. 14.5 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 [33], 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.

Uveďme si ještě překvapivou Mazurovu větu z [23] a [24] o torzních grupách na eliptických křivkách nad racionálními čísly. Nejprve však připomeňme několik definic.

Nechť e je neutrální prvek netriviální grupy G a nechť $g \in G$. Nejmenší přirozené číslo r takové, že $g^r = e$, se nazývá *řád prvku g* . Pokud takové r neexistuje, pak g má nekonečný řád.

Řekneme, že grupa G je direktním součtem grup G_1 a G_2 , tj. $G = G_1 \oplus G_2$, jestliže

1. G_1 a G_2 jsou normální podgrupy G (viz kap. 6.4),
2. $G_1 \cap G_2 = \{e\}$,
3. G je generována G_1 a G_2 , tj. pro každé $g \in G$ existuje právě jedna dvojice $g_1 \in G_1$ a $g_2 \in G_2$ tak, že $g = g_1 \cdot g_2 = g_2 \cdot g_1$.

Můžeme například snadno ověřit, že C_6 je izomorfní s grupou $C_2 \oplus C_3$, kde C_n označuje cyklickou grupu řádu n . Naproti tomu C_4 není izomorfní s grupou $C_2 \oplus C_2$, protože $C_2 \oplus C_2$ neobsahuje prvek řádu 4.

Nechť E je eliptická křivka. Uvažujme Abelovu grupu $E(\mathbb{Q})$ racionálních bodů na E . *Torzní podgrupa* $T(\mathbb{Q})$ grupy $E(\mathbb{Q})$ obsahuje všechny racionální body z E , které mají konečný řád v $E(\mathbb{Q})$.

Věta 4 (Mazurova). *Nechť E je eliptická křivka nad $\mathbb{Q}$. Pak torzní grupa $T(\mathbb{Q})$ je izomorfní s právě jednou z následujících 15 grup:*

$$\begin{aligned} C_n \text{ pro } n \in \{1, 2, \dots, 10\} \cup \{12\}, \\ C_2 \oplus C_{2m} \text{ pro } m \in \{1, 2, 3, 4\}, \end{aligned} \quad (14.17)$$

kde $\oplus$ označuje direktní součet.

Poznamenejme ještě, že cyklická grupa C_n je také izomorfní s podílovou grupou $\mathbb{Z}/n\mathbb{Z}$ a $C_2 \oplus C_{2m}$ je izomorfní s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$.

Eliptické křivky našly v poslední době i řadu praktických uplatnění. Používají se např. pro stanovení veřejného šifrovacího klíče v kryptografii, při testování prvočíslnosti velkých přirozených čísel nebo jejich rozkladu na prvočinitele. Například Henri Lenstra vyvinul efektivní metodu pro nalezení nejmenšího prvočinitele p (angl. elliptic curve factorization method) daného přirozeného čísla n . Její výpočetní složitost je úměrná délce prvočinitele p , a nikoliv délce n .

14.5 Modulární formy

Modulární formy jsou mnohem abstraktnější matematické objekty než eliptické křivky. Jsou to jistá zobrazení vykazující neuvěřitelně mnoho symetrií (viz např. kap. 11.3, (14.19) a (14.20) 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 $z \in \mathbb{C}$ definujeme tzv. *akci* gz pomocí komplexní racionální funkce (viz např. [14, s. 98])

$$gz = \frac{az + b}{cz + d}. \quad (14.18)$$

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

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

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

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

dostaneme

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

Každému prvku grupy $g \in SL_2(\mathbb{Z})$ lze tedy pomocí (14.18) přiřadit transformaci $H \rightarrow H$.

Definice. Nechť $k \in \mathbb{Z}$ a nechť funkce f meromorfní¹⁴ v horní polorovině H splňuje vztah

$$f(gz) = (cz + d)^k f(z) \quad \forall g \in SL_2(\mathbb{Z}). \quad (14.19)$$

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

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

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

Ze vztahu (14.19) je patrná vysoká symetrie modulárních forem. Zvolíme-li např. $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, pak

$$f(z+1) = f(z). \quad (14.20)$$

Podobně pro $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ dostaneme

$$f(-1/z) = (-z)^k f(z). \quad (14.21)$$

Nyní stručně popíšeme, co znamená, že eliptická křivka je modulární. Nechť $E(\mathbb{Q})$ je eliptická křivka nad racionálními čísly s konduktorem N . Konduktor N je jistý invariant, který dělí diskriminant křivky $E(\mathbb{Q})$. Nechť N_p označuje počet bodů ležících na eliptické křivce E nad konečným tělesem F_p s p prvky, kde p je prvočíslo. Položme $a_p = p+1 - N_p$ pro $p \nmid N$ a $a_p = \pm 1$, pokud $p \mid N$ a $p^2 \nmid N$. Přitom znaménko $a_p \in \mathbb{Z}$ závisí na chování eliptické křivky nad F_p . Dále nechť $a_1 = 1$ a pro nesoudělná celá čísla a_m a a_n klademe $a_{mn} = a_m a_n$. Pro $s \in \mathbb{C}$ a $E(\mathbb{Q})$ definujeme L -funkci $L(s, E)$ vztahem (viz [2, s. 210])

$$L(s, E) = \prod_p L_p(s, E)^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

kde pro dané prvočíslo p je

$$L_p(s, E) = \begin{cases} 1 - a_p p^{-s} + p^{1-2s} & \text{pro } p \nmid N, \\ 1 - a_p p^{-s} & \text{pro } p \mid N \text{ a } p^2 \nmid N, \\ 1 & \text{pro } p^2 \mid N. \end{cases}$$

Eliptická křivka se nazývá *modulární*, jestliže funkce

$$f(q, E) = \sum_{n=1}^{\infty} a_n q^n,$$

kde $q = e^{2\pi i \tau}$ a $\tau \in \mathbb{C}$, je modulární.

V padesátých letech minulého století japonský matematik Jutaka Tanijama¹⁶ vyslovil domněnku o souvislosti eliptických křivek a modulárních forem. Další japonský matematik Goró Šimura mu ji pak pomohl zpřesnit. Proto se jí dnes většinou říká Tanijamova–Šimurova.

¹⁶J. Tanijama spáchal ve svých 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 [35].

Tanijamova–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. (14.16). J. Tanijama 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 shodují. 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 $j = 2, 3, \dots$. Tak vznikla Tanijamova–Šimurova domněnka.¹⁸

14.6 Wilesova–Taylorova věta

Propojení mezi Tanijamovou–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. (14.2)), potom by racionální eliptická křivka, tzv. *Freyova křivka*¹⁹ tvaru (14.12),

$$y^2 = x(x - a^p)(x + b^p) \quad (14.22)$$

dávala protipříklad na Tanijamovu–Šimurovu domněnku.

Ve stejném roce Jean-Pierre Serre podal částečný důkaz toho, proč Freyova křivka nemůže být modulární. Jinými slovy, pokud by platila Tanijamova–Šimurova domněnka, pak by Freyova křivka (14.22)

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

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

¹⁹Tuto křivku uvedl předtím ve své doktorské dizertaci Yves Hellegouarch. Případnému řešení diofantické rovnice (14.1) tak přiřadil zcela jiný matematický objekt: eliptickou křivku.

byla tak bizarní, že by nemohla existovat, tj. množina racionálních řešení rovnice (14.22) by byla prázdná. Kenneth Ribet pak v roce 1990 v článku [30] podal úplný důkaz toho, že Frey měl pravdu.

Věta 5 (Ribetova). *Jestliže platí Tanijamova–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 Tanijamovy–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) Tanijamovu–Šimurovu domněnku pro tzv. semistabilní eliptické křivky²⁰, ale naštěstí tento speciální případ v sobě stále ještě zahrnuje Velkou Fermatovu větu.

Věta 6 (Wilesova–Taylorova). *Každá semistabilní racionální eliptická křivka je modulární.*

K důkazu Andrew Wiles použil Iwasawovu teorii společně s Kolyvaginovou–Flachovou metodou [34, s. 161]. Semistabilní eliptické křivky vyjádřil pomocí Galoisových reprezentací a ukázal, že se shodují s Galoisovými reprezentacemi příslušných modulárních forem. Galoisovou reprezentací se 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].

V roce 1995 A. Wiles zveřejnil v *Annals of Mathematics* (viz [40]) úplný důkaz věty 6, ze kterého Velká Fermatova věta vyplývá (viz obr. 14.6), přičemž část důkazu je ve společném článku [38] s Richardem Taylorem. Předložený důkaz se ale opírá o celou řadu dalších netriviálních tvrzení publikovaných jinde (viz např. [8], [30]). Metody,

²⁰Tyto křivky mají bezkvadrátový konduktor. Na obr. 14.5 vlevo je příklad křivky, která není semistabilní. Zbývající dvě křivky semistabilní jsou. Podrobnosti viz [1].



Obr. 14.6 V jihofrancouzském Beaumont-de-Lomagne, rodišti Pierra de Fermata, v říjnu 1996: *Velká Fermatova věta byla tedy skutečně dokázána?*, ptají se vesničané Andrewa Wilese (foto J.-B. Hiriart-Urruty).

které Wiles použil, jsou podrobně vysvětleny např. v knize [13] či v článku [25].

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

Věta 7 (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.

14.7 Bealova domněnka a domněnka abc

Před rokem 1995 se někteří matematikové domnívali, že Fermatova hypotéza je nerozhodnutelné tvrzení. Sir Andrew Wiles však našel po-

stup, jak Velkou Fermatovu větu²¹ 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 5 (viz [30, s. 120, 128]) není omezující, neboť jej vtipně doplňují Fermatova věta 2 a Fermatova–Eulerova věta 3. Vzhledem ke vztahům (14.2) a (14.3) tak Velká Fermatova věta 1 platí pro všechny exponenty $n \geq 3$.

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 .

²¹V 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 $m = 0, 1, 2, \dots$ obsahuje jen konečně mnoho prvočísel [15].

Smysl předchozí nerovnosti je zhruba tento. Pokud například $a = 2^m$, $b = 3^n$ pro velká m a n , pak domněnka říká, že c musí mít velký prvočíselný dělitel nebo velké množství prvočinitelů tak, aby r bylo velké.²²

V případě rovnice (14.1) stačí zvolit $\varepsilon = \frac{1}{2}$. Pak podle domněnky abc je $z^n < Cr^{3/2}$, kde

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

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

L i t e r a t u r a

- [1] ASH, A., GROSS, R.: *Fearless symmetry: Exposing the hidden patterns of numbers*. Princeton Univ. Press, 2008.
- [2] ASH, A., GROSS, R.: *Elliptic tales*. Princeton Univ. Press, Princeton, Oxford, 2012.
- [3] BREUIL, C., CONRAD, B., DIAMOND, F., TAYLOR, R.: *On the modularity of elliptic curves over $\mathbb{Q}$: 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 arithmeticoarum 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.

²²Existuje 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 $r^{1+\varepsilon} < c$.

- [8] FALTINGS, G.: *Finiteness 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] KRÍŽEK, 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] KRÍŽEK, M., SOMER, L.: *John Tate získal Abelovu cenu za rok 2010*. PMFA 55 (2010), 89–96.
- [17] KRÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. 2. vydání, Academia, Praha, 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] MAZUR, B.: *Modular curves and the Eisenstein ideal*. IHES Publ. Math. 47 (1977), 33–186.
- [24] MAZUR, B.: *Rational isogenies of prime degree*. Invent. Math. 44 (1978), 129–162.
- [25] NEKOVÁŘ, J.: *Modulární křivky a Fermatova věta*. Math. Bohem. 119 (1994), 79–96.
- [26] VAN DER POORTEN, A.: *Notes on Fermat's Last Theorem*. John Wiley, New York, 1996.
- [27] REKTORYS, K.: *Přehled užití matematiky I*. Prometheus, Praha, 1995.
- [28] RIBENBOIM, P.: *13 lectures on Fermat's last theorem*. Springer, New York, 1979.
- [29] RIBENBOIM, P.: *Fermat's last theorem for amateurs*. Springer, New York, 1999.
- [30] RIBET, K. A.: *From the Taniyama–Shimura conjecture to Fermat's last theorem*. Ann. Fac. Sci. Toulouse Math. 11 (1990), 116–139.
- [31] 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.
- [32] RICE, A., BROWN, E.: *Why ellipses are not elliptic curves*. Math. Mag. 85 (2012), 163–176.
- [33] SILVERMAN, J. H., TATE, J.: *Rational points on elliptic curves*. Springer-Verlag, 1992.
- [34] SINGH, S.: *Velká Fermatova věta*. Academia, Praha, 2000.
- [35] SINGH, S., MILLSON, R.: *Velká Fermatova věta (Pořad Horizon stanice BBC)*. PMFA 42 (1997), 169–183.
- [36] SKULA, L.: *Některé historické aspekty Fermatova problému*. PMFA 39 (1994), 318–330.

- [37] SUCHÁNEK, V.: *Důkaz Velké Fermatovy věty pro $n = 3$* . SOČ, Brno, 2015, 1–20.
- [38] TAYLOR, R., WILES, A.: *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. *141* (1995), 553–572.
- [39] TERJANIAN, G.: *Velká Fermatova věta*. Cah. CEFRES *28* (2002), 87–106.
- [40] WILES, A.: *Modular elliptic curves and Fermat’s last theorem*. Ann. of Math. *141* (1995), 443–551.
- [41] http://abelprisen.no/en/c67107/seksjon/vis.html?tid=671088&struk_tid=67107

15. Abelova cena v roce 2017 udělena za teorii waveletů

Michal Krížek

15.1 Prolog

V roce 2017 Norská akademie věd rozhodla, že patnáctou Abelovu cenu získá prof. Yves Meyer z École normale supérieure Paris-Saclay za klíčovou roli při rozvoji matematické teorie waveletů. Meyerovy výsledky mají využití jak v čistě teoretických disciplínách, tak i ve



YVES MEYER

výpočtové matematice, informačních technologiích a při vytváření počítačového softwaru. Yves Meyer převzal Abelovu cenu dne 23. května z rukou norského krále Harald V. v hlavní aule univerzity v Oslu.

Následující den pak Yves F. Meyer proslovil laureátskou přednáškou: *Detection of gravitational waves and time-frequency wavelets*. V ní mj. konstatoval, že Sergej Klimenko sestavil algoritmus pro detekci gravitačních vln [7], který je založen na výsledcích Ingrid Daubechiesové, Stéphana Jaffarda a Jean-Lina Journého z roku 1990. Na konkrétním příkladu Meyer demonstroval, proč k detekci nelze použít klasickou Fourierovu analýzu a proč právě wavelety jsou vhodným nástrojem pro analýzu gravitačních vln, které byly zachyceny v roce 2015 dvěma detektory LIGO, vzdálenými od sebe 3 002 km (viz [1]). Signály z průchodu gravitační vlny oběma detektory jsou tak korelované, zatímco všudypřítomný bílý šum na obou detektorech by korelovaný být neměl. Waveletová analýza umožnila odhalit gravitační vlnu se vzrůstající frekvencí a amplitudou na krátkém časovém intervalu. Přitom nebyl vzat do úvahy gravitační červený posuv.

Po Meyerově vystoupení zaznely další tři abelovské přednášky¹ o teorii waveletů:

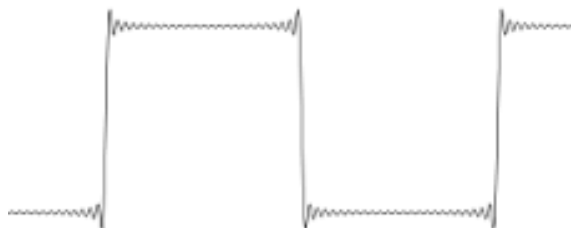
Stéphane G. Mallat: *A wavelet zoom to analyze multiscale world*,

Ingrid Daubechiesová: *Wavelet bases: roots, surprises and applications*,

Emmanuel Jean Candès: *Wavelets, sparsity and its consequences*.

Teorie waveletů (vlnek) navazuje na poměrně dlouhou historii sahající až do roku 1807, kdy Abelův současník Jean Baptiste Joseph Fourier přišel s myšlenkou, že pomocí spočetného ortonormálního systému složeného z jednoduchých trigonometrických funkcí lze popsat některé základní prostory reálných funkcí [18]. Termín *wavelet* použil již v roce 1951 Vladimír Vand pro elementární trigonometrické polynomy $\sin nx$, $\cos nx$, $n = 1, 2, \dots$. Na svém samočinném mechanickém počítači dokázal sečíst až 100 těchto waveletových funkcí vynásobených příslušnými Fourierovými koeficienty (viz [21]). Bouřlivý rozmach teorie waveletů nastal v osmdesátých letech minulého století při digitálním zpracování signálů. Místo trigonometrických polynomů [8] se začaly používat wavelety, které jsou více lokalizovány v prostorových souřadnicích. Navíc jsou obvykle méně hladké a mají

¹ Jejich záznamy jsou volně k dispozici na webové stránce [24].

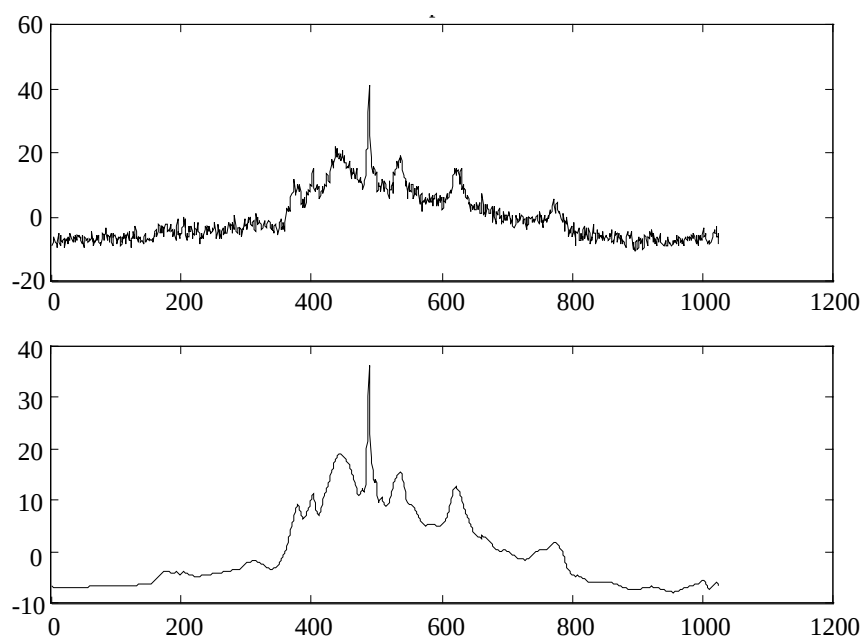


Obr. 15.1 Při aproximaci skokové funkce konečnou trigonometrickou řadou vznikají nežádoucí oscilace v blízkosti bodů nespojitosti. I když budeme zvyšovat počet členů řady, amplituda oscilací se nezmenší (tzv. Gibbsův jev). Waveletová řada však tyto nežádoucí artefakty umožňuje odstranit (zdroj Wikipedia).

kompaktní nosič nebo rychle ubývají do nekonečna. To umožňuje lépe aproximovat funkce, jež jsou nespojité nebo jejichž grafy mají ostré hroty (srov. obr. 15.1). Signál je rozložen pomocí waveletové báze do řady, čímž získáme příslušné waveletové koeficienty. Waveletovou reprezentaci lze použít např. k odstraňování šumu, což se provádí tak, že se z řady vypustí členy odpovídající vysokým frekvencím a malým amplitudám (nežádoucí bílý šum), viz obr. 15.2.

15.2 Vědecký životopis

Yves F. Meyer se narodil 19. července 1939 v Paříži. Od mládí vyrůstal v Tunisu, kde také absolvoval střední školu. Pak vyhrál studentskou soutěž v matematice *Concours général* a v roce 1957 byl přijat na École normale supérieure v Paříži. V letech 1960–1963 absolvoval vojenskou službu na Prytanée national militaire, kde vyučoval matematiku. V roce 1966 obhájil doktorskou dizertační práci. Jeho školitelem byl Jean-Pierre Kahane. Potom působil jako asistent na univerzitě ve Štrasburku a v letech 1966–1980 byl profesorem na univerzitě Paris-Sud. Poté až do roku 1986 přednášel na slavné École polytechnique a do roku 1995 na univerzitě Paris-Dauphine. Pět let (1995–1999) také pracoval v CNRS (Centre national de la recherche scientifique), což je obdoba naší Akademie věd. V období 1999–2003 byl zaměstnán na École normale supérieure, kde od roku 2004 dodnes působí jako emeritní profesor. Podnítil celou řadu mladých lidí k výzkumu v teorii waveletů a pod jeho vedením obhájilo titul Ph.D. kolem 50 studentů.

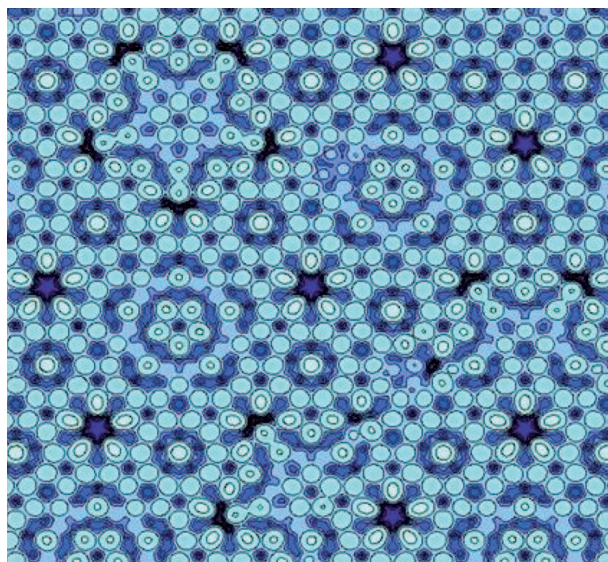


Obr. 15.2 Odstranění bílého šumu: nahoře je původní signál pozměněný nežádoucím šumem a dole je rekonstrukce signálu pomocí teorie waveletů (zdroj Wikipedia).

Na počátku své vědecké kariéry se Yves Meyer zabýval především teorií čísel. Byl okouzlen matematickými objekty, které vykazují pravidelnost a perfektní symetrii, jako jsou například krystalické mřížky. Podrobným studiem rozložení Pisotových čísel (mezi něž patří např. zlatý řez) pak vybudoval teorii [10], jak lze ze zcela pravidelných periodických krystalových mřížek ve vícerozměrném prostoru získat vhodnými projekcemi aperiodická dláždění vykazující jen lokální pětičetnou symetrii (viz obr. 15.3). Inspirován aperiodickým dlážděním² Rogera Penrose z roku 1974 (viz např. [9, s. 312]) se tak dostal až k matematickému popisu kvazikrystalů (viz [11], [15]). Meyer zavedl množiny, které dnes nesou jeho jméno (*Meyer sets*) a slouží právě k popisu kvazikrystalů.

Meyer se dále zabýval harmonickou analýzou. Tak se dostal k problému rozkladu složitých oscilujících matematických funkcí na jednodušší funkce. Této myšlenky využil i při řešení parciálních diferenciál-

²Aperiodická dláždění vykazující lokální pětičetnou symetrii znal již český stavitel Jan Blažej Santini Aichel (1677–1723), viz obr. 15.4.

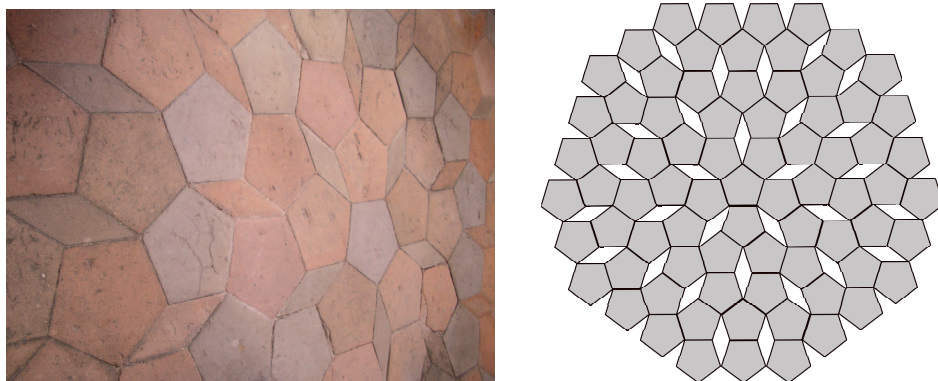


Obr. 15.3 Speciální projekcí pravidelné periodické hyperkrychlové krystalické mřížky v $\mathbb{R}^5$ do vhodně nakloněné dvojrozměrné roviny lze získat aperiodické dláždění vykazující lokální pětičetnou symetrii kvazikrystalu Al-Pd-Mn. Sklon roviny je určen zlatým řezem, což je iracionální číslo (zdroj Wikipedia).

ních rovnic, např. v problému proudění. Zabýval se především problémem turbulence při řešení Navierových–Stokesových rovnic a zkoumal, jak se transformuje energie z malých škál na velké.

Počátkem osmdesátých let se soustředil na teorii waveletů, což okomentoval slovy: *Jednou jsem jel ranním vlakem do Marseille, kde jsem potkal Ingrid Daubechiesovou, Alexe Grossmanna a Jeana Morleta. Bylo to jako v pohádce. Cítil jsem, že jsem konečně našel svůj domov.* Později s nimi Meyer úzce spolupracoval na tom, jak lze pomocí jediné waveletové funkce definovat ortonormální bázi v nekonečněrozměrných prostorech funkcí, což vypadá jako malý zázrak (viz kap. 15.3). Jeden typ waveletů dokonce nese Meyerovo jméno (viz obr. 15.6, [17, s. 82], [23]).

Yves Meyer získal během svého života celou řadu významných ocenění. Třikrát byl zvaným přednášejícím na mezinárodních kongresech matematiků (v Nice v r. 1970, ve Varšavě v r. 1983 a v Kjótu v r. 1990). Za své práce z teorie čísel obdržel v roce 1970 Salemovu cenu. Od roku 1993 je řádným členem Francouzské akademie věd.



Obr. 15.4 Santiniho aperiodické dlážďení v kostele na Zelené hoře u Žďáru nad Sázavou. Dláždění má lokální pětičetnou symetrii, ale nemá globální translační symetrii. Rombická dlaždice je shodná s Penroseovou dlaždicí (vyfotografoval a nakreslil F. Křížek).

V roce 2010 získal prestižní Gaussovu cenu od Německé matematické společnosti za fundamentální přínos k teorii čísel, teorii operátorů, harmonické analýze a za průkopnickou úlohu při vývoji matematické teorie waveletů a multirezoluční (tj. víceškálové) analýzy. Je čestným členem Americké akademie umění a věd. V roce 2012 jej Americká matematická společnost poctila titulem Fellow.

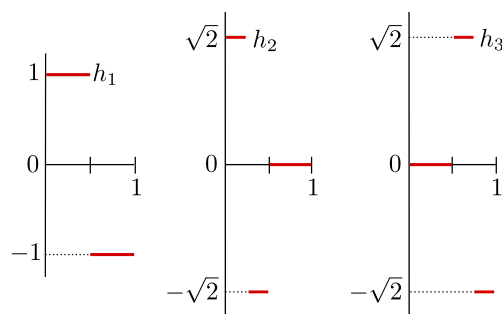
15.3 Hlavní myšlenka teorie waveletů

V roce 1909 maďarský matematik Alfréd Haar zkonstruoval ortonormální systém funkcí pomocí celočíselných translací a dyadických dilatací jediné skokové funkce $h : \mathbb{R} \rightarrow \mathbb{R}$, definované vztahem (viz obr. 15.5)

$$h(x) = \begin{cases} 1 & \text{pro } x \in [0, \frac{1}{2}), \\ -1 & \text{pro } x \in [\frac{1}{2}, 1), \\ 0 & \text{jinde.} \end{cases}$$

Dnes jí říkáme *Haarův wavelet*. *Dyadickou dilatací* rozumíme násobení argumentu x dané funkce nějakou celočíselnou mocninou čísla 2. Pro celá čísla $j \geq 0$, $0 \leq k < 2^j$ a $n = 2^j + k$ pak Haar definoval funkce (srov. obr. 15.5)

$$h_n(x) = 2^{j/2} h(2^j x - k).$$



Obr. 15.5 Ortonormální Haarovy báze funkce $h_1 = h$, h_2 a h_3 z prostoru $L^2([0, 1])$ (nakreslila H. Bílková).

Jestliže dále položíme

$$h_0 \equiv 1,$$

lze dokázat, že systém funkcí $\{h_n\}_{n=0}^\infty$ zúžených na interval $[0, 1]$ tvoří ortonormální bázi v prostoru funkcí lebesgueovsky integrovatelných s kvadrátem $L^2([0, 1])$. Faktor $2^{j/2}$ zaručuje, že L^2 norma funkce h_n je rovna jedné.

Haarův systém $\{h_n\}$ báze funkcí se však v praxi nepoužívá, protože po částech konstantní funkce mají špatné aproximační vlastnosti. Tento systém slouží hlavně pro ilustraci hlavní myšlenky teorie waveletů. Pomocí primitivních funkcí k h_n lze ale definovat jiný ortonormální systém spojitých po částech lineárních funkcí [18].

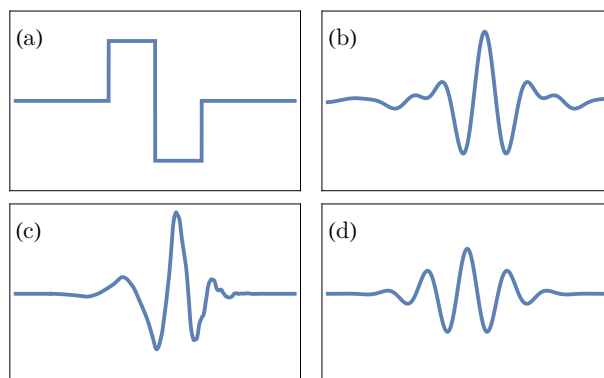
Dále si ukážeme, jaké vlastnosti požadujeme od waveletových báze funkcí. Pro jednoduchost se omezíme na Lebesgueův prostor $L^2(\mathbb{R})$. Uvažujme pevnou funkci $\psi \in L^2(\mathbb{R})$ a její translace a dyadické dilatace definované vztahy

$$\psi_{jk}(x) = 2^{j/2}\psi(2^jx - k), \quad x \in \mathbb{R}, \quad j, k \in \mathbb{Z}.$$

Jestliže systém funkcí $\{\psi_{jk}\}_{j,k \in \mathbb{Z}}$ tvoří ortonormální bázi prostoru $L^2(\mathbb{R})$, pak funkci ψ nazveme *waveletem*³ (viz obr. 15.6). Každou funkci $f \in L^2(\mathbb{R})$ lze zřejmě vyjádřit ve tvaru řady

$$f = \sum_{j \in \mathbb{Z}} \sum_{k \in \mathbb{Z}} (f, \psi_{jk}) \psi_{jk},$$

³Anglicky se takové funkci říká mother wavelet.



Obr. 15.6 Příklady několika typických waveletů: (a) Haarův wavelet, (b) Meyerův wavelet, (c) wavelet Daubechiesové, (d) Morletův wavelet (nakreslil A. Slavík).

kde rovnost platí skoro všude a

$$(f, g) = \int_{-\infty}^{\infty} f(x)g(x)dx$$

označuje skalární součin v $L^2(\mathbb{R})$. Přitom je skoro všude též splněna známá *Parsevalova rovnost*

$$\int_{-\infty}^{\infty} |f(x)|^2 dx = \sum_{j \in \mathbb{Z}} \sum_{k \in \mathbb{Z}} (f, \psi_{jk})^2.$$

Pro wavelet ψ většinou požadujeme, aby $\psi \in L^1(\mathbb{R})$,

$$\int_{-\infty}^{\infty} \psi(x) dx = 0 \quad \text{a} \quad \int_{-\infty}^{\infty} \psi^2(x) dx = 1.$$

Dále je výhodné omezit se na wavelety mající též nulové momenty vyšších řádů než $m = 0$, tj.

$$\int_{-\infty}^{\infty} x^m \psi(x) dx = 0 \quad \text{pro } m = 1, 2, \dots, M,$$

kde M je vhodné přirozené číslo. Jinými slovy, wavelet je kolmý na polynomy nižších stupňů.

Popsaná konstrukce umožňuje velice snadno a rychle provádět výpočty se zadanou funkcí f popisující signál, neboť pro hladké části

signálu jsou příslušné koeficienty malé. Pro dané $\varepsilon > 0$ se pak celkový signál aproximuje jako

$$\tilde{f} = \sum_{| \langle f, \psi_{jk} \rangle | > \varepsilon} \langle f, \psi_{jk} \rangle \psi_{jk}.$$

Malé koeficienty $\langle f, \psi_{jk} \rangle$ se tak zanedbávají a uchovávají se pouze koeficienty velké v absolutní hodnotě. Nejvíce informací o signálu je obvykle uloženo jen v relativně malém počtu koeficientů. Přitom výpočet skalárních součinů $\langle f, \psi_{jk} \rangle$ se obvykle neobejde bez numerické integrace (viz [12], [17, s. 162]).

Pomocí vybraných bázeových funkcí ψ_{jk} lze pak analyzovat signál na různých úrovních rozlišení. Pokud nejsme spokojeni s výsledkem, můžeme díky ortonormalitě snadno přidávat další bázeové funkce, aniž bychom řešili (na rozdíl od metody konečných prvků) rozsáhlé soustavy algebraických rovnic. Bázeové funkce můžeme též ubírat nebo vybírat různé frekvenční kanály.⁴

Teorie waveletů se opírá o tzv. *multirozklad prostoru* $L^2(\mathbb{R})$, čímž rozumíme posloupnost do sebe vnořených⁵ podprostorů $\cdots \subset V_{j-1} \subset V_j \subset V_{j+1} \subset \cdots$, $j \in \mathbb{Z}$, které splňují následující podmínky:

- (i) uzávěr jejich sjednocení je $L^2(\mathbb{R})$,
- (ii) průnik všech prostorů V_j obsahuje jen nulovou funkci,
- (iii) $f(x) \in V_j \iff f(2x) \in V_{j+1}$ a $f(x) \in V_0 \iff f(x+1) \in V_0$,
- (iv) existuje $\varphi \in V_0$ tak, že $\{\varphi(x-k)\}_{k \in \mathbb{Z}}$ je báze V_0 .

Podmínka (i) vlastně říká, že každou funkci $f \in L^2(\mathbb{R})$ lze libovolně přesně aproximovat posloupností funkcí $f_n \in \bigcup_{j \in \mathbb{Z}} V_j$ v L^2 -normě $\|\cdot\|$, tj.

$$\lim_{n \rightarrow \infty} \|f_n - f\| = 0.$$

⁴Pásmové filtry připomínající Fourierovu analýzu zvukového signálu dobře zvládá i hlemýžď ve vnitřním uchu ve spolupráci s naším mozkem. Umíme totiž rozlišit jednotlivé zdroje zvuku, pokud současně slyšíme např. hluk jedoucí tramvaje, hlášení řidiče a k tomu ještě posloucháme hudbu.

⁵Tato vnoření připomínají známou numerickou metodu více sítí (angl. multigrid method) pro řešení parciálních diferenciálních rovnic.

Poznamenejme, že celočíselná translace z podmínky (iii) se pro některé úlohy nepožaduje. Podmínky podobné (i)–(iv) lze nalézt např. v [17]. Pokud báze funkce nejsou ortogonální, často se používá známý Gramův–Schmidtův ortonormalizační proces k vytvoření nové báze.⁶ Bohužel některé příznivé vlastnosti waveletů nelze splnit současně. Lze např. dokázat [17, s. 95], že neexistují nekonečně hladké wavelety s kompaktním nosičem. Proto slavné wavelety Ingrid Daubechiesové [3] s kompaktním nosičem nejsou třídy C^∞ . Na druhé straně Morletův wavelet z obr. 15.6 je nekonečně hladký, ale zase nemá kompaktní nosič. Pokud bychom zhladili Haarovy báze funkce regularizační metodou z [19, s. 58], tak vzniklé funkce sice budou mít kompaktní nosič a budou nekonečně hladké, ale nebudou ortogonální.

15.4 Praktické použití waveletů

Teorie waveletů má obrovské množství nejrůznějších aplikací, srov. [3], [6], [22], [23]. Používá se především ke kompresi dat, jejich archivaci a odstraňování šumu. Kupříkladu bezztrátové bitové mapy otisků prstů jedné osoby vyžadují cca 6 MB paměti počítače, zatímco po úpravě ztrátovou waveletovou transformací stačí paměť 26krát menší a výsledný obrázek je téměř k nerozeznání od bitové mapy (viz obr. 15.7 a [5, s. 12]). Proto FBI k uchovávání a analýze otisků prstů používá formát opírající se o wavelety [2]. Kompresi pomocí standardního JPEG formátu není totiž vhodná, protože se obraz rozkládá na čtverečky 8×8 pixelů a ty se zpracovávají samostatně. Na otiscích se pak zřetelně projevují nežádoucí artefakty JPEG formátu (viz [5, s. 5]).

V současnosti se pomocí waveletové reprezentace běžně analyzují jednorozměrná, dvourozměrná⁷ či vícerozměrná data, například seismické vlny, změny kurzů na finančních trzích, řeč, hudba, rozma-

⁶Báze běžně používané v metodě konečných prvků pro řešení diferenciálních rovnic obvykle nejsou ortogonální, ale vedou na řídké matice. Přidáním jedné báze funkce je proto třeba znovu vyřešit celou soustavu algebraických rovnic pro neznámé koeficienty báze funkcí. Existují však výjimky. Například Szabó a Babuška [20, s. 38] konstruují ortonormální bázi v Sobolevově prostoru $H_0^1((-1, 1))$ se skalárním součinem $(v', w')_{L^2((-1, 1))}$ tak, že integrují Legendreovy polynomy, které jsou ortogonální v $L^2((-1, 1))$.

⁷Dvourozměrné (vícerozměrné) wavelety lze zkonstruovat pomocí jednorozměrných waveletů, viz např. přednášky v [24].



Obr. 15.7 Vlevo je bitová mapa otisku prstu, vpravo její waveletový obraz, který má 26krát menší nároky na paměť počítače (foto Chris Brislawn, Los Alamos National Laboratory).

nitě obrázky či video. Waveletová redukce umožňuje sledovat filmy v různých stupních rozlišení. Wavelety umožňují dokonce detekovat detaily, které nemohou být našimi smysly rozlišeny, protože analyzují signál na mnoha úrovních rozlišení současně. Mají tak rozsáhlé použití v lékařství při rekonstrukci obrazu např. pomocí magnetické rezonance. Podstatně totiž urychlují výpočet, protože vznikají řídké struktury, které lze úsporně ukládat. Nový obor počítačového vidění využívá wavelety k digitalizaci zraku navrhovaných inteligentních robotů. S wavelety se setkáváme také ve skenerech.

Teorie waveletů se používá i k řešení diferenciálních a integrálních rovnic například Galerkinovou metodou (viz [5] a [17]). Slouží též k detekci hran či ostrých hrotů, k rozpoznávání obrazců, ke zjišťování dlouhodobých trendů (např. sezónní oscilace) či k počítačovému modelování křivek a ploch. Pomocí teorie waveletů lze analyzovat struktury s velice komplikovaným tvarem (např. multifraktály). Wavelety přispěly i k současným úspěchům mise Herschelova vesmírného dalekohledu a k objevu gravitačních vln [1].

15.5 Meyerův odkaz

Yves Meyer je specialista na klasickou harmonickou analýzu, což mu umožnilo rozšířit teorii waveletů o mnohé výsledky z teorie operátorů. Zabýval se jak spojitou, tak diskrétní waveletovou transformací. Společně s Ronaldem R. Coifmanem vybudoval Calderónovu–

Zygmundovu teorii v harmonické analýze [16]. Yves Meyer s Ingrid Daubechiesovou a Alanem Grossmannem v polovině osmdesátých let minulého století zkonstruovali speciální báze Hilbertových prostorů funkcí s využitím dilatačních a translačních technik [4]. V roce 1988 Y. Meyer se Stéphanem G. Mallatem publikovali své první průkopnické práce o konstrukci ortonormálních waveletovýchází. Meyer též vyvinul rychlou waveletovou transformaci využívající pyramidální multirezoluční algoritmus. Ukázal rovněž, že wavelety jsou vysoce účinným nástrojem k řešení singulárních integrálních rovnic.

Yves Meyer je autorem několika monografií (viz např. [10], [11], [13], [14], [16]). První dvě jsou o teorii čísel, které se Meyer věnoval v sedmdesátých letech minulého století. Další se už zabývají teorií waveletů. Databáze Mathematical Reviews eviduje přes 200 Meyerových vědeckých prací, na něž získal kolem 5 000 citací.

L i t e r a t u r a

- [1] ABBOTT, B. P., et al.: *Observation of gravitational waves from a binary black hole merger*. Phys. Rev. Lett. 116 (2016), paper No. 061102, 1–16.
- [2] BRISLAWN, C. M.: *Fingerprints go digital*. Notices Amer. Math. Soc. 42 (1995), 1278–1283.
- [3] DAUBECHIES, I.: *Ten lectures on wavelets*. SIAM, CBMS Lecture Notes 61 (1992).
- [4] DAUBECHIES, I., GROSSMANN, A., MEYER, Y.: *Painless nonorthogonal expansions*. J. Math. Phys. 27 (1986), 1271–1283.
- [5] FRAZIER, M. W.: *An introduction to wavelets through linear algebra*. Springer, New York, 1999.
- [6] GRAPS, A.: *An introduction to wavelets*. IEEE, 1995.
- [7] KLIMENKO, S., et al.: *Method for detection and reconstruction of gravitational wave transient with networks of advanced detectors*. Phys. Rev. D 93 (2016), paper No. 042004.
- [8] KOUKAL, S., KŘÍŽEK, M., POTŮČEK, R.: *Fourierovy trigonometrické řady a metoda konečných prvků v komplexním oboru*. Academia, Praha, 2002.

- [9] KŘÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Academia, Praha, 2011.
- [10] MEYER, Y.: *Nombres de Pisot, nombres de Salem et analyse harmonique*. Lecture Notes in Math. 117, Springer-Verlag, 1970.
- [11] MEYER, Y.: *Algebraic numbers and harmonic analysis*. North-Holland, Amsterdam, 1972.
- [12] MEYER, Y.: *Wavelets, quadrature mirror filters and numerical image processing* (in French). Les ondelettes en 1989 (Orsay, 1989), Lecture Notes in Math. 1438, Springer, Berlin, 1990, 14–25, 196–197.
- [13] MEYER, Y.: *Wavelets and operators*. Cambridge Stud. Adv. Math. 37, Cambridge Univ. Press, Cambridge, 1992.
- [14] MEYER, Y.: *Wavelets. Algorithms & applications*. SIAM, Philadelphia, 1993.
- [15] MEYER, Y.: *Quasicrystals, Diophantine approximation and algebraic numbers*. Beyond Quasicrystals. F. Axel, D. Gratias (Eds), Les Editions de Physique, Springer, 1995, 3–16.
- [16] MEYER, Y., COIFMAN, R.: *Wavelets. Calderón–Zygmund and multilinear operators*. Cambridge Stud. Adv. Math. 48, Cambridge Univ. Press, Cambridge, 1997.
- [17] NAJZAR, K.: *Základy teorie waveletů*. Karolinum, Praha, 2004.
- [18] NAJZAR, K., HOLMAN, P.: *Wavelets*. PMFA 44 (1999), 294–303.
- [19] NEČAS, J.: *Les méthodes directes en théorie des équations elliptiques*. Academia, Prague, 1967.
- [20] SZABÓ, B., BABUŠKA, I.: *Finite element analysis*. John Wiley, New York, 1991.
- [21] VAND, V.: *Magnifying 100 million times*. The Meccano Magazine 36 (1951), 247.
- [22] WALNUT, F.W.: *An introduction to wavelet theory*. Appl. Numer. Harmon. Anal., Birkhäuser, Boston, 2002.
- [23] WOJTASZCZYK, P.: *Mathematical introduction to wavelets*. Cambridge Univ. Press, Cambridge, 1997.
- [24] <http://www.abelprize.no>

The Abel Prize — the Highest Achievement in Mathematics

*Michal Křížek, Lawrence Somer, Martin Markl, Oldřich Kowalski,
Pavel Pudlák, Ivo Vrkoč*

The Abel Prize for mathematics is an international prize presented by the King of Norway for outstanding results in mathematics. It is named after the well-known Norwegian mathematician Niels Henrik Abel (1802–1829) who found that there is no explicit formula for the roots of a general polynomial of degree five. The financial support of the Abel Prize is comparable with the Nobel Prize, i.e., about one million American dollars.

Already in 1899, another famous Norwegian mathematician Sophus Lie proposed to establish an Abel Prize, when he learned that Alfred Nobel would not include a prize in mathematics among his five proposed Nobel Prizes. The first Nobel Prize for Physics was awarded in 1901 to Wilhelm Conrad Röntgen. Therefore, there was an attempt to organize the Abel Prize in 1902 to commemorate 100 years of Abel's birth, but it was unsuccessful. One hundred years later the Norwegian government announced that the prize would be awarded in 2002 for the two-hundredth anniversary of Abel's birth. However, the first laureate got the Abel Prize one year later. It is awarded by the Norwegian Academy of Sciences and Letters.

In this essay we survey the major results of the recipients of the first fifteen Abel Prizes from 2003–2017. Each chapter contains a short biographical sketch of a particular laureate and his contribution to various fields of mathematics.

In the list below of Abel Prize winners, we also include the most recent winner, Robert Langlands, who was awarded the Abel Prize in 2018.

1. Jean-Pierre Serre (2003) – topology, algebraic geometry, and number theory
2. Michael F. Atiyah and Isadore M. Singer (2004) – topology, geometry, and analysis
3. Peter D. Lax (2005) – numerical and applied mathematics
4. Lennart Carleson (2006) – harmonic analysis and dynamical systems
5. Srinivasa S. R. Varadhan (2007) – theory of probability and statistics
6. John G. Thompson and Jacques Tits (2008) – algebra and theory of groups
7. Mikhail L. Gromov (2009) – differential geometry
8. John T. Tate (2010) – algebraic number theory
9. John Milnor (2011) – differential topology, geometry, and algebra
10. Endre Szemerédi (2012) – discrete mathematics and theoretical computer science
11. Pierre R. Deligne (2013) – algebra and geometry
12. Yakov G. Sinai (2014) – dynamical systems, ergodic theory, and mathematical physics
13. John F. Nash and Louis Nirenberg (2015) – partial differential equations and geometric analysis
14. Andrew J. Wiles (2016) – number theory
15. Yves Meyer (2017) – theory of wavelets
16. Robert P. Langlands (2018) – number theory and harmonic analysis

Jmenný rejstřík

- Abel N. H. 9, 11–15, 59, 73, 151, 152, 174, 186, 201, 213
Adleman L. M. 110
Agmon S. 167
Ajtai M. 133, 135
Akiba T. 116
Albert II. 140
Artin E. 102, 107, 110, 145, 147
Atiyah M. F. 26, 27, 102, 214
- Babuška I. 209
Balasubramanian R. 129
Batanin T. 148
Beal A. 195
Beck M. T. 10
Bell E. T. 178
Benedicks M. 53
Bernoulli J. 63, 156
Beurling A. 49
Bezikovič A. S. 55
Bhargava M. 175, 177
Bolyai J. 90, 127
Borel É. 21, 60
Bourbaki N. 139
Breuil Ch. 194
Brezis H. 167
Buhler J. 110
Bullová K. S. 162
Bunimovič L. 195
Burnside W. 79
- Caffarelli L. A. 169
Candès E. J. 201
de Carcavi P. 182
Carleson L. 48–51, 53–55, 214
Cauchy A.-L. 74
Coates J. 176, 178
- Coifman R. R. 210
Conrad B. 194
Conway J. H. 78, 79, 83
Cornfeld I. P. 154
Courant E. 166
Courant R. 38, 166
Cramér H. 64
Crelle A. 13, 14
Crowe R. 163
- Čech E. 22
Čchen Ť. 128
- Darmon H. 175, 177
Daubechiesová I. 88, 201, 204, 207, 211
Dedekind R. 147
Deligne P. R. 24, 138–142, 144, 146–148, 214
Diamond F. 194
Digby K. 182
Diofantos 108, 129, 173
Dirichlet G. P. L. 185
Djupedal Ø. 58
Donsker M. 60, 65
Douglass A. 167
Dwork B. 146
- Einstein A. 66, 92, 93
Enge A. 102
Erdős P. 127, 130–132
Eukleides 104
Euler L. 89, 128, 182, 183
- Faltings G. 185, 188
Fáry I. 115
Fatou P. 53

Feit W. 83	Hadamard J. 142
Fejér L. 127	Hajnal A. 127
Fermat P. 19, 62, 104, 173, 180, 182, 194	Hall M. 84
Fermat S. 173	Halvorsenová K. 127
Fiala J. 53	Harald V. 17, 48, 58, 70, 88, 102, 114, 127, 139, 163, 201
Fischer B. 78, 79, 83	Harsanyi J. 163
Folkman J. 116	Harten A. 43
Fomin S. V. 154	Hellegouarch Y. 19, 192
Fourier J. B. J. 50, 201	Hencke E. 107
de Fournival R. 62	Hénon M. 52
Fox R. 115	Hirzebruch F. 27
Freedman M. H. 93	Hölder O. 77
Frey G. 20, 178, 192, 193	Holmboe B. M. 12
Friedrichs K. O. 38	Hopkins M. 114
Frobenius G. 79	Howard R. 163
	Hunt R. A. 51
	Huygens Ch. 62, 183
Galileo G. 62	
Galois E. 13, 72, 75, 77	Chanin K. M. 151
Gauss C. F. 14, 63, 89, 142	Chevalley C. 107
Gelfand I. 128	Chvátal V. 135
Germainová S. 185	
Ghys E. 114	
Gidas B. 167	
Goldbach Ch. 128	Isaksen T. R. 163
Goldsman A. 163	
Gorenstein D. 78	Jacobi C. G. J. 14
Gowers T. 127, 133, 148	Jaffard S. 201
Green B. 131	John F. 167
Griess R. L. 79	Janko Z. 78, 81
Griffiths P. 140	Jordan C. 23, 73
Gromov M. L. 87, 88, 94, 95, 97, 166, 214	Journé J.-L. 201
Gross B. 110	Julia G. 53
Grossmann A. 204, 211	
Grossmann M. 127	Kadison R. V. 27
Grothendieck A. 24, 139, 146	Kagan V. F. 151
	Kahane J.-P. 202
	Takeja S. 54
Haar A. 127, 205, 207	Kakutani Š. 55

Katz N. 178	Markov A. A. 67
Kervaire M. A. 120, 121	Masser D. 195
Kinderlehrer D. 167	Mather J. 116
Kingman J. 88	Mathieu É. L. 78, 80
Klein F. 90	Mazur B. 178
Klimenko S. 201	McKean H. P. 60
Kohn R. V. 169	McMullen C. 114
Kolmogorov A. N. 60, 61, 63, 152, 155, 159	Mersenne M. 104
Kolyvagin V. A. 108	Meyer Y. 200–204, 207, 210, 211, 214
Komlós J. 133, 135	Milnor J. 113, 114, 116, 117, 120–122, 124, 214
Korteweg D. J. 44	Mirzakhaniová M. 155
Kummer E. E. 185	Mittag-Leffler G. 10, 49
	de Moivre A. 63
Lagrange J. L. 129	Morlet J. 204, 207
Lamé G. 185	Mumford D. 26, 140
Lampakis E. 109	
Lang S. 108	Nash J. F. 162–166, 214
Langlands R. 193, 214	Nečas J. 44
Lanzcos C. 127	von Neumann J. 127, 157
Lax P. D. 37, 38, 43–46, 58, 59, 61, 89, 127, 166, 214	Newlander A. 167
Lebesgue V. A. 185	Newton I. 154
Leech J. 81	Ni W. M. 167
Legendre A. M. 185	Nirenberg L. 59, 162, 166, 167, 169, 214
Lenstra H. 189	Nobel A. 10, 11, 213
Lie S. 11, 90, 213	Novikov S. 88
Lind E.-C. 108	
Lobačevskij N. I. 90	Oesterlé J. 195
Lorenz E. 51, 52	Ornstein D. 157
Lovász L. 127	Oscar II. 12
Lyons R. 78	Østerud Ø. 113
Luzin N. N. 50	Ottersen O. P. 114, 174
MacLane S. 71	Palis J. 26
Magnus H. 174, 175	Pascal B. 62
Mallat S. G. 201, 211	Patodi V. K. 27
Marguli G. 151	Pekar S. I. 66
Markl M. 124, 148	

- Penrose R. 203
 Perelman G. J. 93, 117
 Péterová R. 127
 Piene R. 127
 Pólya G. 127
 Pomerance C. 110
 Pudlák P. 135

 Rámanudžan Š. 141
 Rao C. R. 59, 60
 Regan R. 38
 Rejewski M. 73
 Rényi A. 127
 Ribet K. 20, 110, 178, 193
 Riemann B. 90, 143
 Riesz M. 127
 Rödl V. 133, 135
 Rognes J. 175
 Rochlin V. A. 88
 Röntgen W. C. 11, 213
 Roth K. F. 131
 Rozycki J. 73
 Rubin K. 108
 Rumely R. S. 110
 Russell J. S. 44
 Rychlík K. 183

 Santini Aichel J. B. 203
 Seip K. 58, 70, 88, 102
 Sejersted O. M. 172
 Selmer E. S. 108
 Selten R. 163
 Serre J.-P. 17–24, 87, 111, 139, 178, 192, 214
 Schwarzschild K. 92
 Siebenmann L. C. 116
 Silverman 110
 Sinaj J. G. 150–155, 158, 159, 214
 Singer I. M. 26–29, 214

 Singh S. 176, 177, 179
 Sjölin P. 55
 Solomon R. 78
 Solymosi J. 132
 Sondow J. 116
 Sóssová V. T. 127
 Spivak M. 116
 Spruck J. 167
 Stasheff J. 124
 Steinberg R. 84
 Stenseth N. Ch. 102, 127, 150
 Størmer E. 26
 Strang G. 26
 Stroock D. W. 61, 66
 Suchánek V. 183
 Süli E. 127
 Sylow L. 74
 Szabó B. 209
 Szász D. 151
 Szemerédi E. 126–128, 131–133, 135, 155, 214

 Šafarevič I. R. 108
 Šimura G. 191
 Štěpánek F. 50

 Tanijama J. 191, 192
 Tao T. 128, 131
 Tate J. 19, 101–103, 105, 107–111, 188, 214
 Taylor R. 10, 19, 21, 102, 110, 179, 193–195
 Thompson J. G. 70, 71, 78, 83, 214
 Thurston W. P. 99
 Tits J. 70, 71, 138, 214
 Trudinger N. 88
 Turán P. 127, 130
 Turing A. 73

de la Vallée Poussin Ch.-J. 142
 Vand V. 201
 Varadhan G. 60, 61
 Varadhan Š.S.R. 57–62, 65, 66,
 89, 166, 214
 Vinogradov I. M. 128
 Vondrák J. 155
 de Vries G. 44
 Vulová J. B. 159

 Waring E. 129
 Weierstrass K. 10
 Weil A. 23, 145, 146, 192
 Wendroff B. 42
 Wieferich A. 129
 Wigderson A. 127
 Wiles A. 10, 19, 21, 102, 110, 111,
 172, 174–179, 193–195, 214
 Wiles M. F. 176
 Wilesová P. 176
 Wolf J. 94
 Wolfskehl P. 179

 Yau H. T. 60

 Zagier D. 26
 Zelmanov E. 88
 Zsigmondy K. 127
 Zygałski H. 73