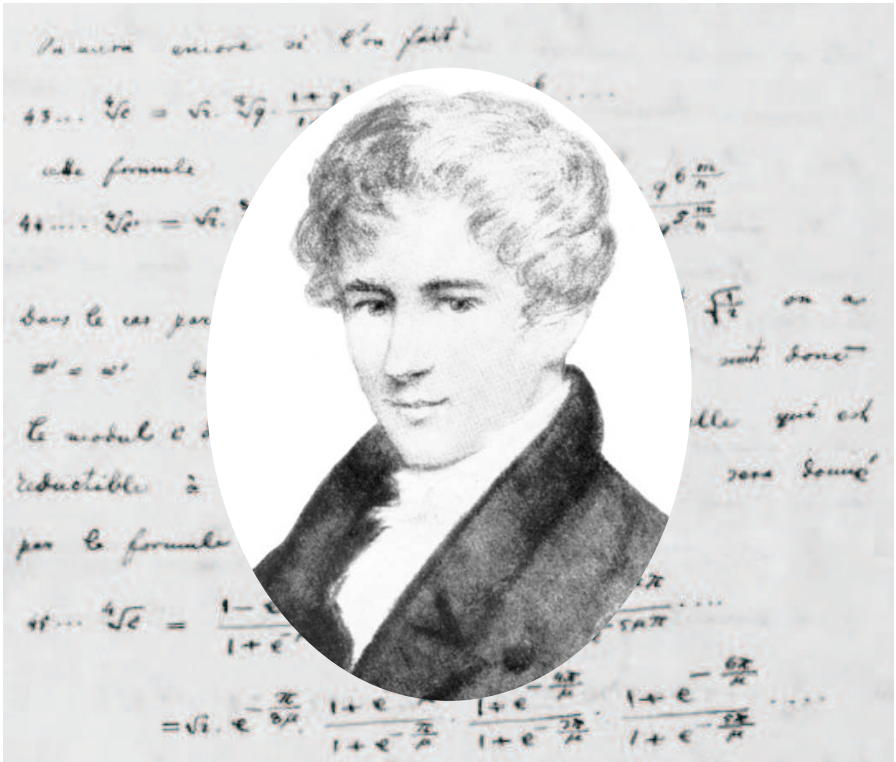
PRVNÍCH DESET ABELOVÝCH CEN ZA MATEMATIKU

Michal Křížek, Lawrence Somer, Martin Markl,

Oldřich Kowalski, Pavel Pudlák, Ivo Vrkoč



Jednota českých matematiků a fyziků

Název: Prvních deset Abelových cen za matematiku
Vydavatel: Jednota českých matematiků a fyziků, Praha
Rok vydání: 2013
Tisk: Petr Beran, Praha
www.pb-tisk.cz
Obálka a sazba: Hana Bílková
První vydání

ISBN 978-80-7015-014-6
EAN 9788070150146

Abelova cena za matematiku

V letech 2004–2012 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: *Prvních deset Abelových cen za matematiku*, JČMF, Praha 2013

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 Mittagem-Lefflerem (1846–1927), žákem Weierstrassovým a zakladatelem časopisu *Acta Mathematica*.

Nejprestižnějším oceněním v matematice byla dříve Fieldsova medaile [10], která se uděluje od roku 1936 (kromě delší přestávky během 2. světové války). Seznam nositelů Fieldsovy medaile je uveden v [6]. Pro matematiky ale existuje celá řada dalších ocenění, např. Fermatova cena[1], Kleinova cena, Lagrangeova cena, Gaussova cena a Wienerova cena za aplikovanou matematiku, ceny společnosti SIAM, Nevanlinnova cena za matematické práce v informatice, Pólyova cena, Steelova cena, Wolfova cena a Wolfskehlova cena [2]. Některé ceny se udělují jen jednorázově, jako např. cena za vyřešení Bealovy domněnky (viz [5]). Připomeňme též vyhlášení sedmi problémů pro 3. tisícletí „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 11 000 dolarů, což je o dva řády menší suma než u Nobelovy ceny. Proto se Norská akademie věd rozhodla zřídit Abelovu cenu (viz `www.abelprisen.no`) na počest geniálního norského matematika Nielse Henrika Abela (1802–1829). Jeho portrét a rukopis jsou na obálce. Abelova cena se uděluje za vynikající vědecké výsledky v oblasti matematiky. Její finanční ohodnocení 6 000 000 norských korun je naprosto rovnocenné s Nobelovou cenou. Předává se v norském Oslu podobně jako Nobelova cena za mír.

[1] Fermatovu 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.

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.

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 pět cen navrhovaných Nobelem. 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 Abelova narození však byla promarněna, i když ji chtěl tehdejší norský král Oscar II. finančně podporovat. Uplynulo dalších sto let, než konečně první Abelovu cenu převzal francouzský matematik Jean-Pierre Serre.

Připomeňme si v krátkosti několik základních údajů o Abelovi. Niels Hendrik Abel se narodil roku 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 [7, 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 vlastní kapsy 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).

Roku 1825 Abel obdržel stipendium od norské vlády ke studijnímu pobytu ve Francii a Německu. Cestoval přes Kodaň, Altonu, Freiberg, Drážďany, Vídeň, s delší

zajížďkou 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 s Augustem Crellem (1780–1855), stavebním inženýrem, který později založil proslulý matematický časopis *Journal für die reine und angewandte Mathematik*. Crelle zůstal Abelovi otcovským přítelem a bez nadsázky lze říci, že jej zachránil pro světovou matematiku. Rozšířenou verzi Abelova článku uveřejnil Crelle v prvním čísle svého časopisu. Abel v něm 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. Později byl nezávisle zobecněn E. Galoisem (1811–1832) na kořeny polynomů libovolného stupně většího než čtyři. Právem jsou proto Abel i Galois považováni za zakladatele teorie grup.

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 a vzájemně různých Fermatových prvočísel (viz [4]). Zde Abel podstatně využil toho, že explicitně vyjádřil délku lemniskáty pomocí eliptických integrálů (viz [8]). V Crellově časopise vyšla též osmdesátistránková stať věnovaná Abelovu výzkumu v oblasti eliptických křivek. Další Abelovy matematické práce lze nalézt v sebraných spisech [9].

Abel strávil spoustu času zajišťováním prostředků na svou obživu. Za jeho života se mu nedostalo uznání. Zemřel 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 poctě s mnoha matematickými 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 Jaroslavu Hančlovi, Františku Katrnoškovi, Martinu Klazarovi, Stanislavu Koukalovi, Pavlovi a Filipovi Křížkovi, Bohdanu Maslowskému, Ivanu Netukovi, Vojtěchu Pravdovi, Aleši Pultrovi, Ivanu Saxlovi, Karlu Segethovi, Jiřímu Vanžurovi, Tomáši Vejchodskému a Václavu Vopravilovi za cenné připomínky k jednotlivým kapitolám. Můj vřelý dík též patří Hance Bílkové za pečlivé technické zpracovaní celého textu a návrh obálky. Publikace vznikla v rámci grantu GA ČR P201/12/G028 a projektu RVO 67985840 Matematického ústavu Akademie věd ČR.

20. 12. 2012

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 [9], 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] Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry.* Springer-Verlag, New York 2001, 2011.

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

[6] Netuka, I.: *Mezinárodní matematické kongresy a Fieldsovy medaile.* PMFA *40* (1995), 124–129.

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

[8] Rosen, M.: *Abel's theorem on the lemniscate.* Amer. Math. Monthly *88* (1981), 387–395.

[9] Sylow, L., Lie, S. (eds): *Œeuvres complètes de Niels Henrik Abel*, vol. I, II, Nouvelle Edition, Oslo 1881, 621 + 341 pp.

[10] 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. Úvod

V červnu r. 2003 převzal Abelovu cenu za matematiku z rukou norského krále Haralda V. francouzský matematik Jean-Pierre Serre. Tento první laureát Abelovy ceny byl oceněn již v roce 1954 Fieldsovu medailí (viz [1]) za práce týkající se homotopických grup sféry 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 velice ráda 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 [4]).

Jean-Pierre Serre

V posledním ročníku středoškolských studií 1943/44 vyhrál celostátní matematickou soutěž „Concours Général“.

V letech 1945–1948 studoval na École Normale Supérieure v Paříži. V dizertační práci se zabýval homotopickými grupami (tehdy ještě nikdo nevěděl, že jsou konečně generované). Již v roce 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 je profesorem algebry na Collège de France v Paříži (v současnosti emeritním). Prof. Serre měl zvanou přednášku na Mezinárodním matematickém kongresu ve Stockholmu v roce 1962. Všeobecně je pokládán za skvělého přednášejícího, jak ostatně bylo patrno i z jeho abelovské přednášky (viz [6]).

V rozhovoru pro časopis Mathematical Intelligencer *8* (1986) mj. uvedl (srov. též [4, s. 243]):

> *I often work at night (in half-sleep), where the fact that you don't have to write anything down gives to the mind a much greater concentration, and makes changing topics easier.*

Jean-Pierre Serre byl zvolen do národních akademií Francie, Nizozemí, 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 [3].

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 registruje přes 250 jeho prací a zhruba stejný počet jich obsahuje i databáze Zentralblatt für Mathematik. V roce 1968 publikoval v *Annals of Mathematics* průlomový článek [10] 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

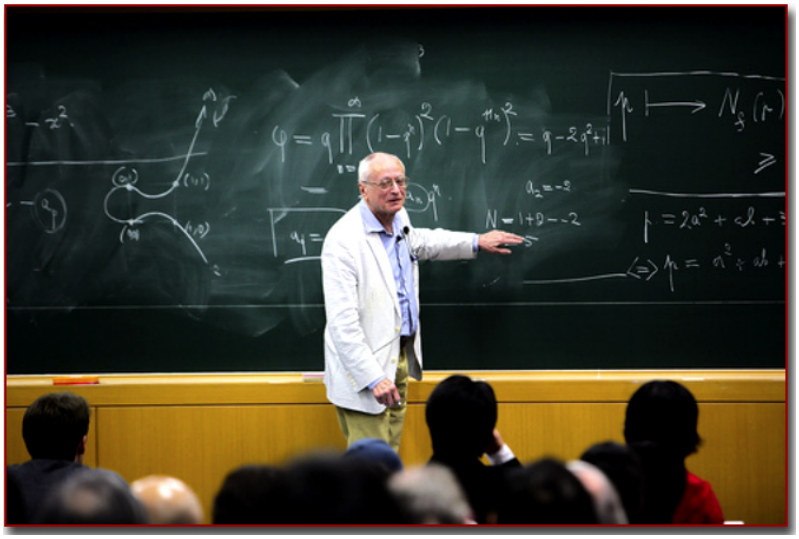
Serre vyvinul nové algebraické metody pro studium topologických objektů. Zejména se zabýval zobrazeními mezi sférami ve vyšších dimenzích. Tato problematika mj. úzce souvisí se známou Poincarého hypotézou (viz [11], [12, s. 276]). Byl jedním z průkopníků algebraické geometrie. V mnoha ohledech tak rozšířil 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 např. částečně přispěl k důkazu Velké Fermatovy věty, kterou dokázal Andrew Wiles společně s Richardem Taylorem [13] v roce 1995 (viz též [5]). Velká Fermatova věta tvrdí, že pro celé $n \geq 3$ neexistuje řešení rovnice

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

v přirozených číslech.[1] Koncem šedesátých let Yves Hellegouarch ve své doktorské dizertační práci přišel s myšlenkou přiřadit případným řešením (a, b, c) rovnice (1.1)

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



Obr. 1.1. Jean-Pierre Serre během své přednášky o eliptických křivkách

zcela jiný objekt a sice *eliptické křivky*. Pokud je ℓ liché prvočíslo a a, b, c jsou přirozená čísla taková, že

$$a^\ell + b^\ell = c^\ell,$$

pak odpovídající *Freyova křivka* je daná rovnicí

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

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

V roce 1982 Gerhard Frey věnoval pozornost neobvyklým vlastnostem těchto křivek, které např. nemusí být modulární. Podle Taniyamaovy-Šimurovy domněnky (viz PMFA *42* (1997), 169–187) je ale každá eliptická křivka modulární (podrobnosti viz [5], [7], [12]). Proto se Frey domníval, že Taniyamaova-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 [9]. V roce 1985 se pokusil dokázat, že Freyova křivka nemusí být modulární, ale předložil jen částečný důkaz tohoto tvrzení. Přesněji řečeno, ukázal, že tzv. semistabilní případ Taniyamaovy-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 Taniyamaova-Šimurova domněnka implikuje Velkou Fermatovu větu. To pak již umožnilo Wilesovi a Taylorovi dokázat Velkou Fermatovu větu v roce 1995.

Již od studentských let se J.-P. Serre intenzívně zabýval teorií grup. Jedna z jeho nejobtížnějších prací v tomto oboru pojednává o otevřených podgrupách profinitních grup. Nejvíce si však cení práce o tenzorovém součinu grupy reprezentací s charakteristikou p. Napsal ji až po šedesátce a věnoval Émilu Borelovi (viz [6]).

Jean-Pierre Serre také podstatným způsobem obohatil topologii právě pomocí teorie grup. Během studií se zabýval Lerayovou teorií fibrovaných prostorů.[2] Napadlo jej, že může použít spektrální posloupnosti ke studiu homotopických grup sfér $\mathbb{S}^n$ a takto dokázal, že většina těchto grup je konečná (viz [8]). Výjimkou je grupa $\pi_n(\mathbb{S}^n) \cong \mathbb{Z}$, $n \geq 1$, a také grupa $\pi_{4n-1}(\mathbb{S}^{2n})$, která je, modulo torze, také izomorfní s množinou celých čísel $\mathbb{Z}$.

V algebraické geometrii Serre přispěl k důkazu Weilových domněnek, které zformuloval André Weil v roce 1949. Tyto hypotézy se týkají generování funkcí získaných z počtu řešení systému polynomiálních 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, než 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 roce 1944.

I když se Serre zabýval především tzv. čistou matematikou, některé jeho výsledky mají důležité aplikace. Vyvinul např. 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 zásadním způsobem ovlivnili matematiku minulého století a zcela změnili strukturu některých důležitých partií. Řada jeho vět totiž uvádí do souvislosti topologii, geometrii a analýzu.

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.: *Fibrované variety a kvantová teorie.* PMFA *28* (1983), 121–147.

[3] Chern, S. S., Hirzebruch, F. (eds.): *Jean-Pierre Serre.* In: *Wolf Prize in Mathematics*, Vol. II, World Sci. Publ. Co. 2001, 523–551.

[4] Chong, C. T., Leong, Y. K.: *Rozhovor s Jeanem-Pierrem Serrem.* PMFA *33* (1988), 241–248.

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

[6] Raussen, M., Skau, C.: *Rozmluva s Jeanem-Pierrem Serrem, prvním nositelem Abelovy ceny.* PMFA *49* 2004, 114–121.

[7] Ribenboim, P.: *Fermat's Last Theorem for amateurs.* Springer, New York, 1999.

[8] Serre, J.-P.: *Homologie singulière des espaces fibrés. Applications.* Ann of Math. *54 (2)* (1951), 425–505.

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

[10] Serre, J.-P., Tate, J.: *Good reduction of abelian varieties.* Ann of Math. *88* (1968), 492–517.

[11] Smale, S.: *Mathematical problems for the next century.* Math. Intelligencer *20 (2)* (1998), 7–15.

[12] Stillwell, J.: *Příběh stodvacetistěnu v* $\mathbb{R}^4$. PMFA *46* (2001), 265–280.

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

[2] O fibrovaných varietách pojednávají články [2] a [6] uveřejněné v PMFA (viz též kap. 2.4 a 9.4).

2. Atiyah a Singer získali Abelovu cenu za rok 2004

Michal Křížek, Martin Markl

2.1. Úvod

Norská Akademie věd se rozhodla udělit Abelovu cenu za rok 2004 Siru Michaelu Francisi Atiyahovi z Uviversity of Edinburgh a Isadoru M. Singerovi z Massachusetts Institute of Technology. Cenu získali „*za objev a důkaz věty o indexu, která uvádí do souvislosti topologii, geometrii a analýzu, a za svou 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 hluboce ovlivnil pokrok v nejdůležitějších oblastech topologie, diferenciální geometrie a kvantové 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

Sir Michael Francis Atiyah Isadore Manuel Singer

stala jednou z nejvíce fascinujících výzkumných činností několika posledních desetiletí. S formulací věty o indexu se seznámíme v kap. 2.4. Atiyah a Singer společně s Patodim 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 se též vysoce cení. 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-teorie[1] mělo řadu aplikací v klasických problémech topologie a 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 jádrech“[2] (angl. heat kernels). I tento objev měl velký dopad.

2.2. Stručná biografie Michaela F. Atiyaha

Michael F. Atiyah[3] se narodil v Londýně v roce 1929. Titul B.A. a později doktorát získal na Trinity College v Cambridge. Podstatnou část své akademické dráhy strávil v Cambridge a Oxfordu. Zastával mnoho význačných funkcí, mezi jinými vysoce prestižní Savilian Chair of Geometry v Oxfordu a Master of Trinity College v Cambridge. Byl také profesorem matematiky v Institute for Advanced Study v Princetonu.

Během svého působení v Oxfordu a Cambridge se Atiyah stal představitelem nové generace mladých matematiků. Byl vedoucí osobností při budování Isaac Newton Institute for Mathematical Sciences v Cambridge a stal se jeho prvním ředitelem. Nyní je Atiyah v důchodu a je čestným profesorem na University of Edinburgh.

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 Royal Medal v r. 1968 a Copley Medal v r. 1988. Prezidentem Royal Society byl v letech 1990–1995 a prezidentem London Mathematical Society v letech 1974–1976. Hrál též významnou roli při utváření dnešní Evropské matematické společnosti (European Mathematical Society).

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

Z mnoha cen, které mu byly uděleny, jmenujme Feltrinelli Prize (Accademia Nazzionale dei Lincei, 1981) a King Faisal International Prize for Science (1987). V roce 1983 byl Atiyah pasován na rytíře a v roce 1992 byl zvolen členem Order of Merit.

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

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

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

2.3. Stručná biografie Isadora M. Singera

Isadore Manuel Singer se narodil v roce 1924 v Detroitu a v roce 1944 ukončil studia na University of Michigan. Po získání doktorátu (Ph.D.) na University of Chicago v roce 1950, přešel na Massachusetts Institute of Technology (MIT). Zde strávil většinu svého profesionálního života a v současné době je zde profesorem (Institute Professor).

Singer je členem American Academy of Arts and Sciences, American Philosphical Society a National Academy of Sciences (NAS). Působil v Radě NAS, v Řídicí správě 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 Böcher Prize (1969) a Steele Prize (2000) za celoživotní úspěchy. Obě dostal od Americké matematické společnosti. Dále obdržel Eugene Wigner Medal (1988) a National Medal of Science (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

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

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

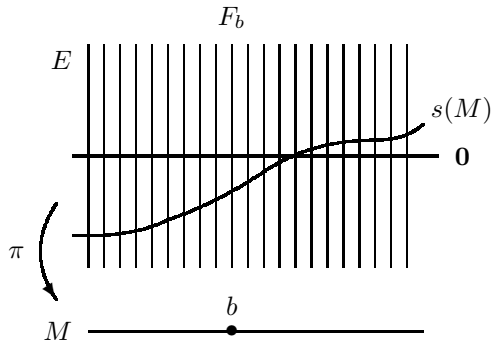
$$\mathrm{rk}(D) := \max\{i_1 + \cdots + i_n \mid F_{i_1,\dots,i_n} \neq 0\}.$$

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

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

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

$$\Delta := \frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}, \tag{2.2}$$



Obr. 2.1. Představa fíbrace jako spojité rodiny vektorových prostorů.

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

$$\Box := -\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2} \tag{2.3}$$

eliptický není.

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

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

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 $v \mapsto \phi(x, v)$ izomorfizmem komplexních vektorových prostorů $\mathbb{C}^k$ a F_x.

Podmínka (i) vyjadřuje komutativitu diagramu

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

v němž p_1 je projekce na první faktor. Prostory M, resp. E, se nazývají *báze*, resp. *totální prostor* fíbrace $\pi : E \to M$. Na zobrazení π se budeme odkazovat jako na *fíbrující zobrazení*.

[4] Anglicky *smooth vector bundle*.

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

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

Vektorová fíbrace $\pi : E \to M$ je *hladká*, jestliže π je hladké zobrazení hladkých variet.[5] V dalším textu budeme hladkost předpokládat automaticky. *Řez* fíbrace $\pi : E \to M$ je pravá inverze fíbrujícího zobrazení, tedy hladké zobrazení $s : M \to E$, 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 fíbrace 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 $\Box$ připomenuté v (2.2), resp. (2.3) můžeme nyní chápat jako lineární zobrazení $\Gamma(U\times\mathbb{C}, U) \to \Gamma(U\times\mathbb{C}, U)$.

Na vektorové fibrace lze ‚po fíbrech' aplikovat stejné operace jako na vektorové prostory. Každá vektorová fíbrace $E \to M$ má proto svuj *duál* $E^* \to M$, jehož fíbr F_b^* nad $b \in M$ je lineární duál fíbru F_b puvodní fíbrace.[6] Podobně můžeme utvořit *součet*

$$E' \oplus E'' \to B \tag{2.5}$$

fíbrací $E' \to B$ a $E'' \to B$ se stejnou bází B. Fíbry součtu (2.5) tvoří přímé součty $F'_b \oplus F''_b$ fíbrů jednotlivých konstituentů.

Ve formulaci věty o indexu upotřebíme i následující konstrukci. Pro hladké zobrazení $p : B \to M$ a fíbraci $\pi : E \to M$ definujeme *indukovanou* fíbraci[7] $p^*E \to M$ fíbrace π podél zobrazení p jako fíbraci s totálním prostorem

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

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

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

s obvyklou univerzální vlastností kategoriálních kartézských čtverců.

Vraťme se nyní k definici diferenciálních operátorů v potřebné obecnosti. Uvažujme vektorové fibrace $\pi' : E' \to M$ a $\pi'' : E'' \to M$ nad stejnou bází. Diferenciální

[5] O hladkých varietách pojednáme též v kap. 9.3.

[6] Pokud není třeba, vynecháváme symbol pro fíbrující zobrazení.

[7] Anglicky *pullback*.

operátor je lineární zobrazení $D : \Gamma(E', M) \to \Gamma(E'', M)$ 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

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

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

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

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

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

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

jsou (komplexní) *de Rhamovy formy* stupně i. Ty, spolu s *de Rhamovým diferenciálem* $d^i : \Omega^i(M) \to \Omega^{i+1}(M)$, tvoří (komplexifikovaný) de Rhamův komplex $(\Omega(M), d)$ variety M. Jeho kohomologie $H\big(\Omega(M), d\big)$ jsou shodné s kohomologiemi $H(M; \mathbb{C})$ variety M s komplexními koeficienty.

Pomocí Riemannovy metriky lze sestrojit operátor $d^{i\,*} : \Omega^{i+1}(M) \to \Omega^i(M)$ *sdružený* k operátoru d^i. Operátory d^i a $d^{i\,*}$ jsou příklady diferenciálních operátorů na řezech fíbrace $\wedge^i_{\mathbb{C}}(M)$ s hodnotami v řezech fíbrace $\wedge^{i+1}_{\mathbb{C}}(M)$, resp. $\wedge^{i-1}_{\mathbb{C}}(M)$. Označme

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

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

$$d := \sum_{j \ge 0} d^{2j} : \Gamma(E', M) \to \Gamma(E'', M) \ \text{ a } d^* := \sum_{j \ge 0} d^{2j+1\,*} : \Gamma(E', M) \to \Gamma(E'', M)\,,$$

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

Dále se soustředíme na vektorové fíbrace 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

$$Ind_A(D) := \dim Ker(D) - \dim coKer(D), \tag{2.6}$$

kde $Ker(D)$, resp. $coKer(D)$, značí jádro, resp. kojádro, lineárního zobrazení D.

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

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

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

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

$$Ind_T(D) := ch(D)\mathscr{T}(M)[M]. \tag{2.7}$$

Jeho úplné vysvětlení přesahuje možnosti tohoto článku, proto jenom naznačíme definice jednotlivých členů bez nároků na úplnou přesnost, na detaily odkazujeme čtenáře k [4]. Začněmě s veličinou $ch(D)$.

Množina všech (nikoliv nutně hladkých) vektorových fibrací s danou bází B je komutativní pologrupa[11] $\mathcal{E}(B)$ s operací + danou součtem (2.5) a neutrálním prvkem 0 tvořeným identitou $B \to B$. 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* $TM \to M$ a duální *kotečnou fibraci* $p\colon T^*M \to M$. V totálním prostoru kotečné fibrace vezměme podprostor $B(M) \subset T^*M$ vektorů délky nepřesahující 1 a sestrojme indukované fibrace

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

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

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

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 isomorfismus. Indukované fibrace p^*E' resp. p^*E'' náleží pologrupě $\mathcal{E}\big(B(M)\big)$, můžeme proto vzít jejich rozdíl

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

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

Uveďme následující posloupnost tvořenou standardními objekty algebraické topologie:

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

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

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

[11] To je množina s komutativní asociativní operací + a neutrálním prvkem 0.

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

$$\mathscr{T}(M) = 1 + \frac{c_1}{2} + \frac{c_2 + c_1^2}{12} + \frac{c_1 c_2}{24} + \frac{-c_1^4 + 4c_2c_1^2 + 3c_2^2 + c_3c_1 - c_4}{720} + \cdots \in H(M;\mathbb{Q}),$$

ve které $c_1, c_2, c_3, \ldots \in H^*(M;\mathbb{Q})$ jsou Chernovy třídy komplexifikované tečné fibrace variety M. Topologický index (2.7) je racionální číslo dané evaluací součinu $ch(D)\mathscr{T}(M) \in H(M;\mathbb{Q})$ 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 topologickemu indexu, tedy*

$$Ind_A(D) = Ind_T(D).$$

Hloubka věty je v porovnávání veličin rozdílného charakteru. Zatímco analytický index je celé číslo sestrojené prostředky funkcionální analýzy, topologický index je geometrická veličina. Okamžitý dusledek je, že $Ind_T(D)$ je také celé číslo, zatímco jeho definice říká pouze, že je to číslo racionální – povšimněmě si, že vzorec pro Todduv rod obsahuje racionální koeficienty![12] 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) definující $Ind_A(D)$ konečný a (protože (2.8) není izomorfizmus) nelze sestrojit ani rozdílový element $d(D)$ potřebný pro definici $Ind_T(D)$.

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

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

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

$$Ind_T(D) = \chi(M)[M].$$

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 $\overline{\partial} + \overline{\partial}^*$ pusobící 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).

[12] Stejná poznámka platí i pro Chernuv charakter, jež je v podstatě exponenciání funkcí Chernových tříd.

3. Abelovu cenu v roce 2005 získal Peter Lax

Michal Křížek

3.1. Úvod

Norská akademie věd se rozhodla udělit Abelovu cenu za rok 2005 význačnému 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 dne 18. května 2005 společně s peněžitou odměnou 980 000 USD. Týž den pak proslovil Abelovu přednášku na půdě univerzity v Oslu.

Peter David Lax

Peter David Lax se narodil 1. května 1926 v Budapešti. V roce 1941 se s rodiči přestěhoval do New Yorku. Zde v roce 1949 získal titul Ph.D. pod vedením Richarda Couranta, zakladatele metody konečných prvků. O rok později začal Lax pracovat v Los Alamos jako konzultant. Od roku 1951 P. Lax byl zaměstnán v Courantově ústavu matematických věd (University of New York), kde v letech 1972–1980 působil ve funkci ředitele. 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. Např. 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 [2]).

3.2. Laxovo-Milgramovo lemma

Celá řada úloh z technické praxe vede na okrajové úlohy pro parciální (popř. obyčejné) diferenciální rovnice eliptického typu. Typickými 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 [3]) 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.*

$$\exists C > 0 \quad \forall v, w \in V \quad |a(v,w)| \le C\|v\|\|w\|, \tag{3.1}$$

a V-eliptická, tj.

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

Pak problém:

Najít $u \in V$ takové, že

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

má právě jedno řešení.

Ukažme si použití Laxova-Milgramova lemmatu na jednoduchém příkladě. Nechť $\Omega \subset R^d$ ($d \in \{1,2,3,\dots\}$) je omezená oblast, jejíž hranice $\partial\Omega$ je lipschitzovsky spojitá (viz [5]). Klasické řešení Poissonovy rovnice s Dirichletovou okrajovou podmínkou

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

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

kde Δ 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.

Zaveďme prostor testovacích funkcí

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

kde parciální derivace chápeme ve smyslu distribucí a rovnici $v = 0$ na hranici $\partial\Omega$ ve smyslu stop (viz [1] nebo [5]). 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

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

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

$$\int_\Omega \nabla u \cdot \nabla v \,\mathrm{d}x = \int_\Omega f v \,\mathrm{d}x \quad \forall v \in V; \tag{3.7}$$

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

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

je Hilbertův, že F je lineární spojitý funkcionál na V a že $a(\cdot, \cdot)$ je bilineární spojitá forma. Její V-eliptičnost (3.2) plyne z Friedrichsovy nerovnosti (viz [5]). 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 v nějakém konečněrozměrném neprázdném podprostoru $V_h \subset V$, kde h charakterizuje míru diskretizace. Existence a jednoznačnost takového $u_h \in V_h$ je pak opět zaručena Laxovým-Milgramovým lemmatem.

Laxovo-Milgramovo lemma zobecňuje známou Rieszovu větu[1] o reprezentaci lineárních spojitých funkcionálů pomocí skalárního součinu. Forma $a(\cdot, \cdot)$ ale není skalárním součinem, pokud není symetrická. S nesymetrickými formami je zapotřebí pracovat v úlohách proudění, při výpočtu elektromagnetického pole aj. Hilbertův prostor V vystupující v Laxově-Milgramově lemmatu může být i nad komplexními čísly. Pak je ale třeba dát levou stranu nerovnosti (3.2) do absolutní hodnoty.

[1] **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 $v \in V$.*

3.3. Konvergence numerických schémat

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

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

$$u(0) = u_0, \tag{3.9}$$

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 [4]). 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]).

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.

3.4. 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

Obr. 3.1. Diederik J. Korteweg a Gustav de Vries

do vzdálenosti několika kilometrů. Později nizozemský matematik Diederik Johannes Korteweg a jeho student Gustav de Vries (viz obr. 3.1) odvodili evoluční parciální diferenciální rovnici, která tento jev popisuje:

$$\frac{\partial u}{\partial t} = 6u\frac{\partial u}{\partial x} - \frac{\partial^3 u}{\partial x^3}, \tag{3.10}$$

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 (3.10) 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, ale i při modelování vln cunami (viz [6]).

3.5. Závěr

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 [2].

P. Lax je velký příznivec využití počítačů v matematice. Tvrdí, že úloha počítačů v matematice je srovnatelná s významem dalekohledů v astronomii či mikroskopů v biologii. Mladým studentům doporučuje, aby si trénovali matematické dovednosti na řešení nějakého 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] Lax, P. D.: *Selected papers, volume I and II.* Eds. A. J. Majda and P. Sarnak, Springer, New York 2005.

[3] Lax, P. D., Richtmyer, R. D.: *Survey of the stability of linear difference equations.* Comm. Pure Appl. Math. *9* (1956), 267–293.

[4] Lax, P. D., Richtmyer, R. D.: *Survey of the stability of linear finite difference equations.* Comm. Pure Appl. Math. *9* (1956), 267–293.

[5] Nečas, J., Hlaváček, I.: *Mathematical theory of elastic and elasto-plastic bodies: an introduction.* Elsevier, Amsterdam 1981.

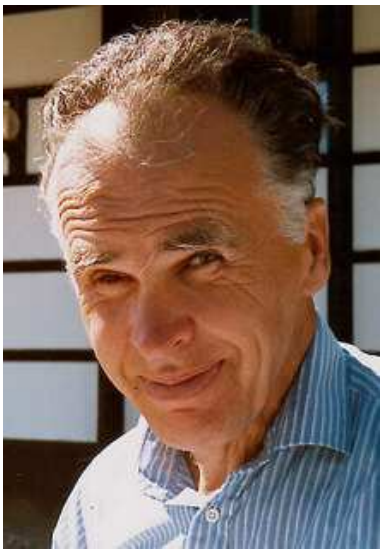
[6] Švadlenka, K.: *Matematické modely a numerická simulace vln cunami.* PMFA *57* (2012), 177–185.

4. Abelovu cenu za rok 2006 získal Lennart Carleson

Michal Křížek

4.1. Úvod

V úterý 23. května 2006 obdržel profesor Lennart Carleson Abelovu cenu za rok 2006 z rukou Jeho Veličenstva norského krále Haralda V. na universitě v Oslo. Podle vyjádření komise pro výběr kandidátů na Abelovu cenu ji dostal za *své hluboké a 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.



Lennart Carleson

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 později byl též profesorem na kalifornské univerzitě v Los Angeles a v Královském technologickém institutu ve Stockholmu (viz [16]).

V období 1968–84 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 matematické centrum, 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 profesoři. V letech 1978–82 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 toho jednou měl plenární přednášku, což se považuje za jedno z nejvyšších ocenění v mezinárodní matematické komunitě. Obdržel čestný doktorát na několika univerzitách 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 význačných ocenění za svou práci, např. v roce 1984 Steelovu 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 roku 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]) problém přesně zformuloval ruský matematik Nikolaj N. Luzin (1883–1950), ale nebyl schopen jej dokázat. Po něm byl nazván *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 věta uvedená níže. 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 systému $\{\mathrm{e}^{\mathrm{i}nx}\}_{n=-\infty}^{\infty}$) jsou definovány takto:

$$\hat{f}(m) = \frac{1}{2\pi}\int_0^{2\pi} f(t)\mathrm{e}^{-\mathrm{i}mt}\mathrm{d}t, \quad s_n(x) = \sum_{m=-n}^{n} \hat{f}(m)\mathrm{e}^{\mathrm{i}mx}.$$

Označíme-li

$$a_m = 2\mathrm{Re}\hat{f}(m) = \frac{1}{\pi}\int_0^{2\pi} f(t)\cos mt\,\mathrm{d}t,$$
$$b_m = 2\mathrm{Im}\hat{f}(m) = \frac{1}{\pi}\int_0^{2\pi} f(t)\sin mt\,\mathrm{d}t,$$

pak $\hat{f}(m) = (a_m - \mathrm{i}b_m)/2$ 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 $n \to \infty$ skoro všude.*

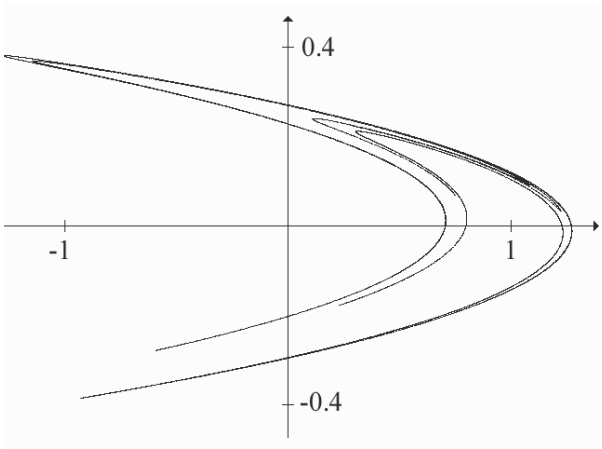
Tato věta byla později zobecněna Richardem A. Huntem na funkce integrovatelné s p-tou mocninou pro $p > 1$ – tzv. Carlesonova-Huntova věta (viz [14, s. 127]).

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 Massachusetts Institute of Technology 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



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

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 došlo 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 křídly motýla v březnu někde v Pekingu může způsobit v srpnu změnu směru hurikánu v Atlantickém 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 Lorenzův systém. Hénon definoval zobrazení T roviny do roviny 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 $n = 0, 1, 2, \ldots$ 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 týž atraktor. Pokud ale vystartujeme z bodu $(0, 0.2919)$, odpo-

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

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

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 dokázali jako první 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].

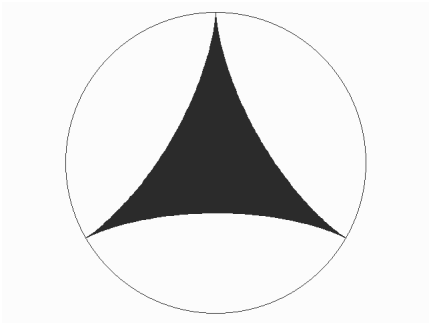
4.5. Závěrečné poznámky

Lennart Carleson přispěl k řešení mnoha dalších problémů. V roce 1917 japonský matematik Sôichi Kakeya 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?*

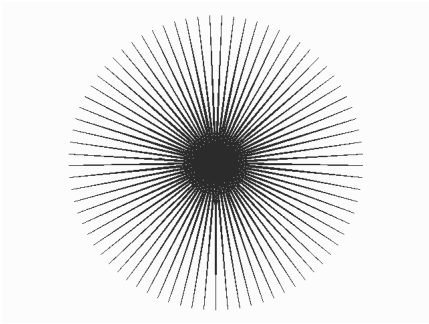
Můžeme si rovněž klást otázky: *Jak posunovat a otáčet jehlou tak, aby obarvená plocha byla minimální? Existuje vůbec taková plocha o minimálním obsahu?* Uvidíme, že na poslední dvě otázky existuje negativní odpověď.

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 Kakeya domníval, že je minimální (viz obr. 4.2). V roce 1928 ale ruský matematik Abram S. Bezikovič (1891–1970) překvapivě dokázal,

[1] Již 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.



Obr. 4.3. Plocha složená z mnoha dlouhých a úzkých trojúhelníků.

že obarvenou plochu můžeme udělat libovolně malou (viz [2, 3]). Jeho plocha se skládá z velkého množství úzkých trojúhelníků podobných jehličkám na vánočním stromečku (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 S. 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. Mothly *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 Srinivasa Varadhan

Michal Křížek, Ivo Vrkoč

5.1. Úvod

Dne 22. května 2007 obdržel Abelovu cenu profesor Srinivasa 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 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 S. Varadhan Abelovu cenu ze *své fundamentální příspěvky k teorii pravděpodobnosti, zejména za vytvoření sjednocené teorie velkých odchylek.*

Srinivasa S. R. Varadhan

Komisi předsedal Kristian Seip. Abelovu cenu pak udělila Norská akademie věd. Slavnostnímu aktu v aule univerzity v Oslo 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 Oslo a Trondheimu a zúčastnil se matematického cirkusu organizovaného pro děti. Abelova cena je spojena s peněžitou odměnou 6 000 000 norských korun.

5.2. Proslov prof. Varadhana při udělení Abelovy ceny

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

Chci začít vyjádřením velkých díků norské vládě a lidem, kteří se zasloužili o zřízení Abelovy nadace, která podporuje tuto cenu. Abel ve svém velice krátkém životě učinil obrovský přínos „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 mě 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 fundamentálními 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 formování jako osoby i jako matematika se podílelo mnoho osobností. Můj otec byl učitel a později ředitel na střední škole. Vzdělání mělo vždy vysokou prioritu v našem domově a já jsem v tomto směru měl trvalou podporu od obou svých rodičů.

Na střední škole jsem měl výborného profesora matematiky, od něhož jsem pochytil, 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 měl velké 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 můj skvělý kolega a věrný rádce. 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 mí kolegové Stroock, Papanicolaou a H. T. Yau v různých obdobích a dále Kipnis, Olla a Landim, kteří dlouhodobě navští-

vili náš ústav. Během těch let jsem měl kolem třiceti studentů. Spolupráce s nimi byla velice povzbuzující a byli to oni, kdo přispěli a obohatili můj profesionální život.

Newyorská univerzita a především Courantův ústav je báječná instituce v tom smyslu, že získává studenty k vědeckému bádání a umožňuje 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 Gopal[1] *a že nemůže se mnou prožívat tento okamžik.*

Končím díky adresovanými Norské akademii věd, Abelově nadaci a výběrové komisi za to, co se dnes stalo, a přeji každému dobrý den.

5.3. Stručný životopis

Srinivasa 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 disertace 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 Kolmogorovovi představit svého vynikajícího studenta. A nutno dodat, že Kolmogorov nebyl zklamán.

S. Varadhan začal svoji akademickou kariéru v Courantově ústavu v New Yorku již jako postdoc (1963–67). V letech 1966–68 zde působil jako asistent a poté jako docent (angl. Associate Professor). V roce 1972 byl jmenován profesorem a ještě v témže roce odcestoval do švédského Mittag-Lefflerova ústavu na delší studijní pobyt. V období 1976–77 přijal nabídku pracovat na Standfordské univerzitě. V letech 1980–84 vystřídal ve funkci ředitele Courantova ústavu P. Laxe. Později (1991–92) byl také zaměstnán v prestižním Ústavu pro pokročilá studia (Institute for Advanced Study) a po návratu se stal opět ředitelem Courantova ústavu (1992–94).

I když je práce S. Varadhana motivována problémy matematické fyziky a teorií parciálních diferenciálních rovnic, zabývá se především teorií pravděpodobnosti. Když nastoupil do Courantova ústavu, nalezl 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 processes* [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 Varadhan zvaným řečníkem na Mezinárodním matematickém kongresu a v roce 1994 zde měl plenární přednášku. Během svého plodného života prof. Varadhan získal řadu ocenění a uznání. Připomeňme například Birkhoffovu cenu (1994)

[1] *Pozn. redakce:* Gopal je Varadhanův prvorozený syn, který tragicky zahynul 11. září 2001 při teroristickém útoku v New Yorku.

[2] Andrej 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.

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 a v r. 2004 do Indické akademie věd. Databáze Mathematical Reviews eviduje 135 recenzí na práce S. Varadhana. Jeho stručná vědecká biografie 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 de Fermata s Balaisem 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. $\ell = 2$ 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 Jakob 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 $\frac{p}{10^6}$, kde p udává počet, kolikrát padl orel, se bude jen velice málo lišit od pravděpodobnosti $\frac{1}{2}$.

A. N. Kolmogorov vyjádřil zákon velkých čísel následující matematickou větou:

Nechť $X_1, X_2, \ldots$ je posloupnost nezávislých stejně rozdělených náhodných veličin s konečnou střední hodnotou μ a konečným rozptylem.[3] *Pak*

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

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. 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 velkým 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 se vyhnuli velkým odchylkám, pak si

[3] Poznamenejme, 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 $(X_1 + \cdots + X_n)/n$ neohraničená [13].

vaše pojištění nikdo nekoupí. Přitom taková velká odchylka nastane jen velmi zřídka. Pojišťovací společnost proto potřebuje spočítat pravděpodobnost velkých odchylek různých velikostí, aby nalezla rozumnou míru rizika. 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 velkých 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 Monroe 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

$$L(t,\omega(.),y) = \frac{1}{t}\lambda\{s : 0 \le s \le t,\, \omega(s) \le y\},$$

kde λ je Lebesgueova míra na $\mathbb{R}^1$, $\omega(.)$ je realizace Brownova pohybu. Hodnota $L(t,\omega(.),y)$ tedy vyjadřuje relativní dobu, po kterou realizace $\omega(.)$ 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

$$\lim_{t\to\infty} \frac{1}{t} \log E_x \left[\exp\left\{-t\Phi(L(t,\omega(.),.))\right\}\right],$$

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 $L(t,\omega(.),y)$. V tomto případě byla limita nalezena jako extremní 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

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

kde C je podmnožina pravděpodobnostních měr, L_t je definována vztahem

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

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]).

Uvedené 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 výsledky S. Varadhana

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 difúzní proces v $\mathbb{R}^d$, $d \in \{1, 2, \dots\}$, který je popsán evoluční parabolickou parciální diferenciální rovnicí

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

kde koeficienty difúze a_{ij} jsou spojité a omezené 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])

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

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 difúzních 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 Kolmogorovovou 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

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

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

[4] Andrej 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].

martingal vůči pravděpodobnosti P a σ-algebrám $\mathcal{F}_s$, 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 spojité a omezené, 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 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.* Current 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 Křížek, Lawrence Somer

6.1. Úvod

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 30. května 2008 v hlavní aule univerzity v Oslo. Abelova cena byla tentokrát spojena s částkou 1 200 000 USD. Podle vyjádření prof. Kristiana Seipa, předsedy výběrové komise, cenu dostali za *své hluboké výsledky v algebře a hlavně za zformování moderní teorie grup.*

J. G. Thompson působí od r. 1993 jako Graduate Research Professor na University of Florida a je emeritním profesorem na Univerzity of Cambridge v Anglii. Narodil se 13. října 1932 v Kansasu. Na slavné Yale University začal studovat teologii. Po roce však přešel na matematiku a udělal dobře. Saunders Mac Lane jej totiž pozval, aby

John Griggs Thompson

Jacques Tits

si udělal doktorát na University of Chicago. Zde se začal intenzívně věnovat konečným grupám symetrií a získal v roce 1959 titul Ph.D. Poté rok působil na Institute for Defense Analysis a dva roky na Harvardově univerzitě. Pak se vrátil do Chicaga a v období 1962–1968 zde byl již profesorem. V roce 1970, kdy ještě nedosáhl ani 40 let, byla Thompsonova práce oceněna Fieldsovou medailí. V letech 1970–1993 pak působil na univerzitě v Cambridge. Získal 4 čestné doktoráty, Wolfovu cenu, Coleovu cenu, Sylvesterovu medaili, Poincarého medaili aj.

J. Tits je emeritním profesorem na Collège de France, ale je původem z Belgie. Narodil se 12. srpna 1930 v Uccle na předměstí Bruselu. Považovali jej za zázračné dítě. Už jako tříletý uměl počítat a později mu bylo umožněno, že přeskočil několik tříd školní docházky. Ve svých čtrnácti letech tak úspěšně vykonal přijímací zkoušky na Free University of Brussels. 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.

V tomto článku bychom chtěli seznámit čtenáře se základy moderní teorie konečných grup. V závěrečné kapitole se pak stručně zmíníme o hlavních výsledcích obou laureátů v této oblasti a jejich přínosu ke sporadickým grupám (viz též [15]).

6.2. Stručně o teorii grup

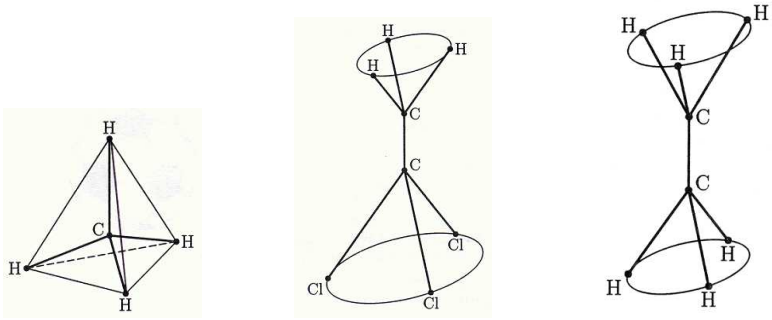
Připomeňme si nejprve některé základní pojmy. *Grupa* G je množina, na které je definována asociativní binární operace $\circ : G \times G \to G$ s neutrálním prvkem e a v níž ke každému prvku $g \in G$ existuje právě jeden prvek inverzní $g^{-1} \in G$ tak, že $g \circ g^{-1} = g^{-1} \circ g = e$.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

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

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

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

[1] Někdy 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. 6.1. Symetrie molekuly metanu CH_4 tvoří grupu o $4! = 24$ prvcích, která je izomorfní[2] 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 trichloretanu H_3C–CCl tvoří cyklickou grupu C_3 o třech prvcích. Dihedrální grupa D_3 se skládá ze šesti přímých symetrií molekuly etanu C_2H_6.

Teorie grup má obrovské množství nejrůznějších praktických aplikací, např. při klasifikaci krystalů, uzlů, symetrií molekul (viz obr. 6.1), popisu silných, slabých a elektromagnetických interakcí, skládání Lorentzových transformací, v teorii kódování[3] (viz [17], [20], [21], [27]). Díky symetriím se značně zjednodušují některé výpočty. S grupami se setkáváme i při řešení různých hlavolamů (viz např. obr. 6.2).

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. 6.2. Známá hra *patnáctka* (vlevo) neumožňuje prohodit 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?

6.3. 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 $\circ$ ale zúženou na $H \times H$, s týmž neutrálním prvkem e jako má G a splňující axiomy grupy. Nazývá se *vlastní*, je-li $H \neq G$, a *triviální*, je-li $H = \{e\}$.

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

[3]Například 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.

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

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 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.*

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, též molekuly fullerenu C_{60} či klasického fotbalového míče.

6.4. 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 $n = 1, 2, \ldots$ 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 patrno z Galoisovy věty).

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

Protože všechny cyklické grupy[6] 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. Žádná z nich ale není normální.

Jednoduché grupy tvoří jakési stavební kameny všech grup podobně jako chemické prvky, resp. prvočísla jsou stavebními kameny molekul, resp. 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

[5] Grupa všech přímých symetrií krychle je S_4.

[6] *Cyklická grupa* je grupa generovaná jediným prvkem.

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 $G_1/G_2, G_2/G_3, \ldots, G_n/G_{n+1}$ 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 $\{e\} = G_{n+1} \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 = G$ 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 permutace*[7] *π prvků $1, \ldots, n+1$ taková, že G_i/G_{i+1} je izomorfní $H_{\pi(i)}/H_{\pi(i+1)}$ pro $i = 1, \ldots, n$.*

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 typu*[8] *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 článcích od přibližně 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

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

[8] Lieovy 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.

[9] Poznamenejme, že jedna grupa z třídy 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	$\lvert B\rvert \approx 4 \cdot 10^{34}$, viz (6.3)
Monster	M	$\lvert M\rvert \approx 8 \cdot 10^{54}$, viz (6.1)

Tab. 6.1 Sporadické grupy

do Amer. Math. Soc. 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. Conway[10] 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]):

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

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. Např. 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. Např. existují dvě neabelovské grupy řádu $3^3 = 27$.

6.5. Sporadické grupy

Největší sporadická grupa se nazývá *Monstrum* a označuje se M. Jde o zcela výjimečný matematický objekt. 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 jej pak v roce 1983 zkonstruoval jako konečnou grupu rotací v eukleidovském prostoru $\mathbb{R}^{196883}$. Řád M je vskutku úctyhodný,

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

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

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040 \tag{6.2}$$

je sice větší[11] než $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7920$, ale lze ji 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]):

$$g_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 12 \end{bmatrix},$$

$$g_2 = \begin{bmatrix} 1 & 12 & 2 & 11 & 3 & 6 & 4 & 8 & 5 & 9 & 7 & 10 \\ 12 & 1 & 11 & 2 & 6 & 3 & 8 & 4 & 9 & 5 & 10 & 7 \end{bmatrix},$$

$$g_3 = \begin{bmatrix} 1 & 2 & 3 & 7 & 11 & 8 & 9 & 10 & 5 & 6 & 4 & 12 \\ 1 & 2 & 7 & 11 & 8 & 3 & 9 & 5 & 6 & 4 & 10 & 12 \end{bmatrix}.$$

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 $\{1, 2, \ldots, 12\}$ existuje permutace

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

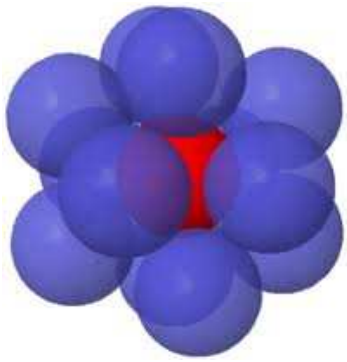
[12] Každá 6-tranzitivní grupa je už buď symetrická, nebo alternující (viz [27]).

$s \in M_{12}$ 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: *These apparently sporadic simple groups would probably repay a closer examinantion than they have yet received.* Podle Burnsidovy věty musí být řád každé sporadické grupy číslo složené z vícera prvočinitelů (srov. tab. 6.1).

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.

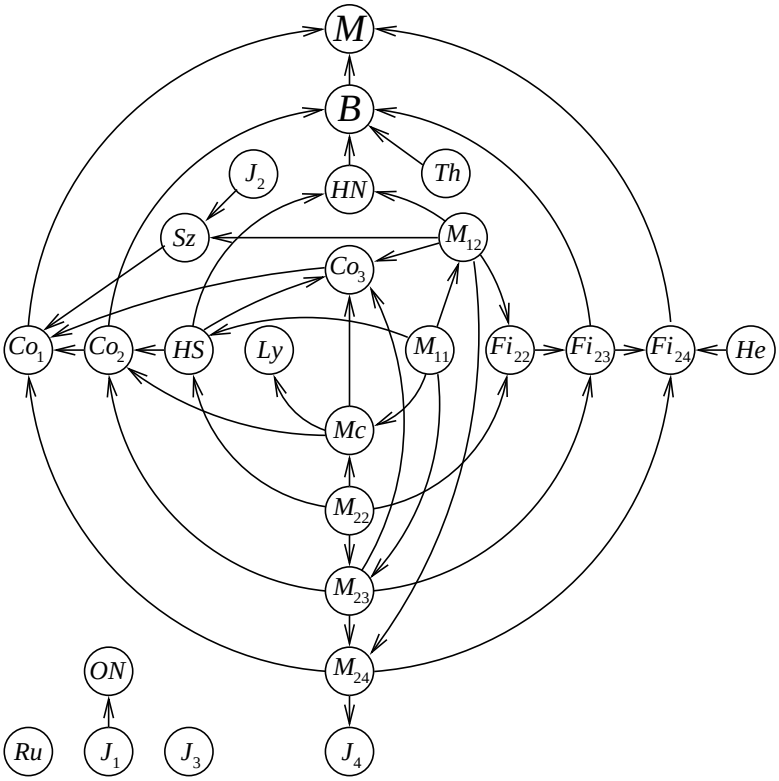
Několik sporadických grup bylo zkonstruováno pomocí tzv. Leechovy mřížky (viz [25]). Při nejhustším uspořádání stejně velkých kruhů v rovině se každý kruh dotýká svých šesti sousedů. Pro pravidelná periodická uspořádání stejně velkých koulí v d-rozměrném prostoru označme maximální počet dotyků vybrané centrální koule se sousedními koulemi symbolem $K(d)$ (angl. *kissing number*). Pak $K(1) = 2$, $K(2) = 6$, $K(3) = 12$ (viz obr. 6.3), $K(4) = 24$ 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]).



Obr. 6.3. Dvanáct koulí obklopujících centrální kouli v třírozměrném prostoru.

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

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



Obr. 6.4. Orientovaný graf ukazuje vztahy mezi všemi 26 sporadickými grupami (šipka $H \to G$ 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 (6.1).

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.[14]

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

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

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

[14] Odtud mj. plyne, že bod o souřadnicích $(0, 1, 2, \ldots, 23, 24, 70)$ má v 26-rozměrném Lorentzově prostoru (používaném v teorii strun) vzdálenost od počátku v zobecněné Minkowského metrice rovnou nule.

ještě dvě grupy Ly a J_4, které obsahují některé netriviální podgrupy Monstra (viz obr. 6.4). Těmto 22 sporadickým grupám se říká *Šťastná rodinka* (angl. Happy Family). Skupina zbývajících čtyř sporadických grup nese přiléhavý název *Vyvrhelové* (angl. Pariahs).

6.6. 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. 6.4). 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.[15] Tzv. 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.*

[15] Poznamenejme, že nový Vítězný oblouk v La Défense v Paříži je „projekcí“ čtyřrozměrné krychle do trojrozměrného prostoru.

Poznámka. Pokud vám v hlavě stále vrtá paradox z obr. 6.2 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 odbarvíme všech 16 čtverečků černě a bíle jako políčka na šachovnici. Tento podklad se nebude během řešení měnit. Při každém tahu tedy prázdné políčko vždy 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 řádku, vykonáme sudý počet tahů a problém je tedy potenciálně řešitelný. Nyní si můžete prakticky vyzkoušet, že problém lze skutečně vyřešit.

Literatura

[1] Abel, N. H.: *Mémoire sur les équations algébriques oú on démontre l'impossibilité de la résolution de l'equation générale du cinquième dégré*. 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] Křížek, 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., Křížek, 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.): *Œeuvres 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.

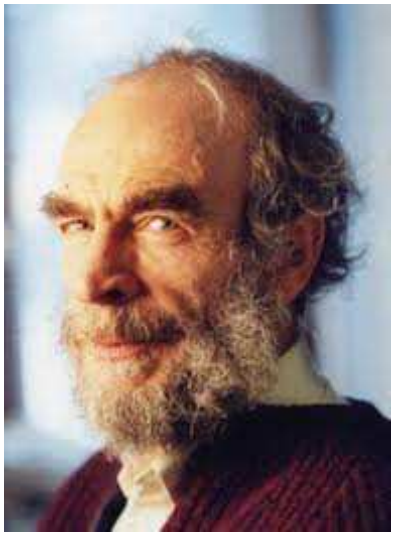
[27] Tůma, J.: *Matematické hlavolamy a základy teorie grup*. Mladá fronta, Praha 1988.

7. Abelova cena v roce 2009 udělena Michailu Gromovovi

Oldřich Kowalski, Michal Křížek

7.1. Úvod

Matematici se poměrně dlouho a těžce vyrovnávali se skutečností, že se za jejich obor neuděluje Nobelova cena. Po velice dlouhých jednáních Norská akademie věd zřídila Abelovu cenu za matematiku, jejíž finanční ohodnocení je srovnatelné s Nobelovou cenou (tj. okolo 10^6 USD). Právo nominovat kandidáta na Abelovu cenu má kdokoliv. Výběrová komise je složena z pěti mezinárodně uznávaných matematiků. Každý člen komise je volen na 2 roky s výjimkou předsedy, který je volen na 4 roky. Podle statutu Abelovy ceny musí být předseda norským matematikem. Další tři členové jsou voleni IMU (International Mathematical Union) a zbývající pátý člen je volen EMS (European Mathematical Society). V roce 2009 komise pracovala ve složení: Kristian Seip (předseda), John Kingman, Sergey Novikov, Neil Trudinger a Efim Zelmanov.



Michail Leonidovič Gromov

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.[1] V dalších letech pak následovaly ceny za topologii a algebru (2004), za aplikovanou a numerickou matematiku (2005), harmonickou analýzu a teorii dynamických systémů (2006), za teorii pravděpodobnosti a statistiku (2007) a za teorii grup (2008). V roce 2009 získal Abelovu cenu rusko-francouzský matematik Michail Leonidovič Gromov za své revoluční výsledky týkající se především diferenciální geometrie, algebry a topologie. Předseda Norské Akademie věd Øyvind Østerud oznámil veřejnosti jméno nového laureáta, jemuž pak cenu osobně předal norský král Harald V. v hlavní aule univerzity v Oslo dne 19. května 2009.

Pamětní řeč pronesla paní Ingrid Daubechies (Princeton Univ.), bývalá členka výběrové komise a zakladatelka teorie waveletů. Poté následovaly čtyři abelovské přednášky, z nichž první měl M. Gromov (viz [16]).

7.2. Kdo je Michail Gromov?

Michal Gromov se narodil 23. prosince 1943 v Boksitogorsku (cca 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. Pak odešel na Newyorskou státní univerzitu v Stony Brook na Long Islandu.

V roce 1981 se natrvalo přestěhoval do Francie. Nejprve nastoupil na Université de Paris a o rok později získal stálé místo profesora na 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. Prof. Gromov je znám především svými výsledky v těch oblastech matematiky, které úzce souvisí s geometrií. Je autorem celé řady monografií, viz např. [3]–[8]. V poslední době se M. Gromov 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 cena (1999) a Bolyaiova cena (2005). Prof. Gromov je zahraničním členem Národní akademie věd v USA, Americké akademie věd a umění 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[2] v New Yorku. V této prestižní instituci pracují i Peter Lax a Srinivasa Varadhan, kteří získali Abelovu cenu v roce 2005, resp. 2007.

[1] O prvních pěti Abelových cenách podrobně pojednává publikace [11].

[2] Courantův ústav byl zřízen v 19. století známým podnikatelem Jayem Gouldem, který se kromě jiného soukromě věnoval studiu matematiky.

7.3. Stručně o diferenciální geometrii

Slovo *geometrie* pochází z řečtiny: $\gamma\varepsilon\omega\mu\varepsilon\tau\rho\acute{\iota}\alpha$; 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, 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 Gauss vyslovil jedno ze základních tvrzení v klasické diferenciální geometrii, které lze zhruba charakterizovat takto:

Gaussova Theorema Egregium.[3] *Pokud budeme zakřivenou plochu izometricky deformovat v prostoru, její (Gaussova) křivost v každém bodě zůstane zachována.*

Uveďme si názorný příklad. Rovina reprezentovaná listem papíru má Gaussovu křivost nula. Jestliže stočíme list do válcové či kuželové plochy, bude její Gaussova křivost opět 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 Göttingen 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 nejprve globální vlastnosti ploch a nadploch v souvislosti s topologií, později pak 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 metrizovatelný 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 sou-*

[3] Latinsky egregius znamená nádherný, vynikající, výtečný, výborný, znamenitý.

řadnic a kde přechody mezi dvěma soustavami lokálních souřadnic jsou vyjádřeny diferencovatelnými funkcemi třídy C^∞.

Obecně nelze d-rozměrnou varietu vložit do $\mathbb{R}^{d+1}$. Nejznámějším příkladem této překvapivé skutečnosti je (viz [19, Corollary 11.16]) Kleinova láhev, což je dvojrozměrná varieta ve čtyřrozměrném prostoru, kterou nelze vložit do trojrozměrného prostoru.[4] Tato plocha navíc není orientovatelná. Platí však následující tvrzení (viz [19, Th. 11.14]):

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

Z předpokladů 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 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 $\mathbb{S}^2$, která je homeomorfní s povrchem čtyřstěnu, okamžitě zjistíme, že $\chi(\mathbb{S}^2) = 2$.

Pro anuloid $\mathbb{T}^2$ snadno nalezneme triangulaci toroidálního mnohostěnu a jemu odpovídající Eulerovu charakteristiku $\chi(\mathbb{T}^2) = 0$. 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 překvapivě nula, jak plyne ihned z Gaussovy-Bonnetovy věty.

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

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

Gaussova-Bonnetova formule pak zní

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

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.

Albert Einstein (1879–1955) zjistil, že všechny hmotné objekty (planety, hvězdy, galaxie aj.) náš prostoročas lokálně zakřivují. 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 jednoznačně určená. Například na ideálním modelu povrchu Země jsou všechny poledníky nejkratšími spojnicemi obou pólů.

Geodetika nemusí být vždy nejkratší spojnicí dvou bodů. To platí pouze lokálně, kdy všechny perturbované křivky mezi dvěma dostatečně blízkými body na geodetice jsou delší. Nejednoznačné geodetiky 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 [15, kap. 27.3] izotropie implikuje homogenitu. Astronomická pozorování rozložení supernov, γ-záblesků a reliktního záření zatím izotropii vesmíru potvrzují.

Einsteinův kosmologický princip nám dává odpověď na otázku, jaký by mohl být tvar našeho vesmíru, pokud lze odpovídající varietu vložit do čtyřrozměrného prostoru. Platí totiž následující tvrzení (viz [13], [19]), 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 3-rozměrná topologická varieta homeomorfní se sférou $\mathbb{S}^3 = \{(x_0, x_1, x_2, x_3) \in \mathbb{R}^4 \,|\, x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1\}$, tj. trojrozměrným povrchem čtyřrozměrné jednotkové koule (viz [17, kap. 5]).[5] Pokud jsou uvedené předpoklady pro model vesmíru splněny, 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, přičemž čas t plyne v radiálním směru (srov. [15, 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 výsledky M. Gromova

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]–[14].

1) *Bishopova-Gromovova nerovnost*

Nechť M je úplná d-rozměrná Riemannova varieta s pozitivně semidefinitní Ricciho křivostí. Pak objem koule v M je menší nebo roven objemu koule[6] 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 $S' = \{g_1, \ldots, g_n\}$ je množina generátorů konečně generované grupy G a $S = \{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\}$ 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. J. 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 přesně 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:

3) *Gromovova-Hausdorffova konvergence*

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

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

[5] Pro 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 [18].

[6] Např. 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. [15, s. 1099].

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

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 Riemannnových 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“. Nechť (X,d) je metrický prostor a nechť $x,y,z \in X$ 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

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

Metrický prostor (X,d) se nazývá *δ-hyperbolický*, jestliže pro všechny body $p,x,y,z \in X$ platí $(x,z)_p \ge \min\{(x,y)_p,(y,z)_p\} - \delta$, 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 $\gamma : I \to X$, která lokálně minimalizuje vzdálenosti. Přesněji řečeno, existuje konstanta $\nu \ge 0$ 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 $d(P,Q) \le \delta$. 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 splňující 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 $g^{-1}h$. 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 $f : X \to Y$ 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 spojité 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 $\operatorname{diam}(M, g(\varepsilon))$ 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 semi-direktního součinu $N \rtimes F$ na N. Kompaktní kvocient grupy N podle podgrupy součinu $N \rtimes F$ (operující volně na N) se nazývá „infranil-varieta“. Infranil-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 infranil-varieta. Opět 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 nestažitelné 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 $\operatorname{sys}\pi_1$, 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

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

kde C_d je univerzální konstanta závisející 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 $\operatorname{FillRad}(C)$. 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 euklidovského 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 $\operatorname{FillRad}(M)$ pro obecnou varietu potřebujeme teorii homologií, a proto se tím zde nebudeme zabývat. Gromov také dokázal následující (druhou) systolickou nerovnost:

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

Dále ještě nalezl odhad shora $\operatorname{FillRad}(M) \leq C_d(\operatorname{vol}(M))^{1/d}$ 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-formou. (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. Thurstonem[7] 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. Gromov použil tento poznatek 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.

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

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.

[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] Kobayshi, S., Nomizu, K.: *Foundation of differential geometry*, vol. II. Interscience, London, New York 1969.

[14] Mac Lane, S., Birkhoff, G.: *Algebra*. Alfa, Bratislava 1973.

[15] Misner, C. W., Thorne, K. S., Wheeler, J. A.: *Gravitation*, (20th edition). Freeman, New York 1997.

[16] Sapiro, G.: *Abel Prize science lecture: Revolutionary work in geometry and shape analysis*. SIAM News *42* (2009), 1, 3.

[17] O Shea, D.: *Poincarého domněnka*. Edice Galileo, Academia, Praha 2010.

[18] Smale, S.: *Generalized Poincaré's conjecture in dimensions greater than four*. Ann. Math. *74* (1961), 391–406.

[19] 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. Úvod

Abelova cena je považována za „Nobelovu cenu“ za matematiku. Její finanční ohodnocení kolem 1 miliónu amerických dolarů je stejné jako u Nobelovy ceny za fyziku. Abelova cena se uděluje za výjimečně hluboké výsledky, které významně ovlivnily matematické vědy. V roce 2010 ji získal americký matematik prof. John Tate z University of Texas 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 rukou norského krále Haralda V. Při této příležitosti přednesl slavnostní proslov předseda Norské akademie věd Nils Ch. Stenseth a předseda výběrové

John Tate (foto: Charlie Fondville)

komise (Abel Committee) Kristian Seip. Další den pak pronesl prof. Tate laureátskou přednášku na téma:

The arithmetic of elliptic curves.

O eliptických křivkách pojednáme v kapitole 8.4. Připomeneme i některé jejich aplikace v kryptografii.

Tateovy výsledky z teorie eliptických křivek podstatně přispěly k důkazu Velké Fermatovy věty[1] — jednoho z nejslavnějších matematických problémů (viz např. [11], [13], [14], [15]). Tato věta říká, že neexistují přirozená čísla $n > 2$ a a, b, c tak, že

$$a^n + b^n = c^n. \tag{8.1}$$

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 [18], [19]). Další přehledovou přednášku měl Andreas Enge na téma: *The Queen of Mathematics in Communication Security*, v níž poukázal na překvapivé aplikace teorie čísel v kryptografii.[2] Na večerním banketu pak promluvil mj. Michael Atiyah, který získal Abelovu cenu v roce 2004.

8.2. Kdo je John Tate?

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

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

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

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

[1] V originále „Fermat's Last Theorem", což se většinou interpretuje jako „poslední nevyřešený z Fermatových problémů". Poznamenejme ale, že např. problém, zda je Fermatových prvočísel tvaru $2^n + 1$ nekonečně mnoho, dodnes nebyl vyřešen [5].

[2] Článek [8] na podobné téma vyšel nedávno i v PMFA (viz též [20]).

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

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

8.3. Velice stručně o teorii čísel

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

Teorie čísel se zabývá zejména vlastnostmi množiny přirozených čísel

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

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

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

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

Za zakladatele moderní teorie čísel je považován francouzský matematik Pierre de Fermat (viz [15]). Jeho nejčastěji používaný výsledek, který má i velké množství praktických aplikací (viz [5]), lze zformulovat takto:

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

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

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

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

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

Největší známé prvočíslo je v současnosti Mersennovo číslo $2^{57885161} - 1$ ($\approx 10^{17425170}$). Pro srovnání uveďme, že počet atomů v pozorovatelné části vesmíru je přibližně jen 10^{80}, což je o více než 17 miliónů řádů menší číslo než $M_{57885161}$.

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

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

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

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

8.4. Eliptické křivky

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

$$y^2 = x^3 + Ax^2 + Bx + C, \tag{8.2}$$

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.

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

V jedné části důkazu Velké Fermatovy věty (srov. (8.1) a [9]) se pracuje se speciálními grupami bodů na eliptických křivkách tvaru $y^2 = x(x - a^p)(x + b^p)$ (kde vhodnou lineární substitucí lze „vynulovat“ koeficient u x^2). Abychom se blíže seznámili s těmito grupami, zabývejme se pro jednoduchost jen jedinou křivkou $\mathcal{C}$ danou vztahem

$$y^2 = x^3 - x + \tfrac{1}{4}\,, \tag{8.3}$$

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

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

$$\ominus U = (x, -y), \tag{8.4}$$

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).

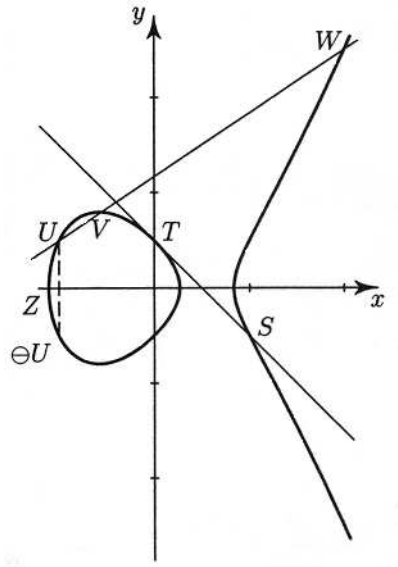
Nyní popíšeme, jak budeme definovat binární grupovou operaci $\oplus$. Nechť $U, V \in \mathcal{C}$ jsou dva různé body ležící na přímce $y = kx + q$. Potom z (8.3) dostáváme kubickou rovnici

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

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

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



Obr. 8.1. Grupa na eliptické křivce.

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

$$U \oplus V = \ominus W. \tag{8.6}$$

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

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

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 $N \in \mathcal{C}$, že pro libovolné $U \in \mathcal{C}$ platí

$$U \oplus N = U. \tag{8.7}$$

Co to konkrétně geometricky znamená? Podle (8.6) body U, $\ominus U$ a N leží na jedné přímce, která je rovnoběžná s osou y. 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 C neleží.

Abychom dokázali, že body křivky (8.3), k nimž je doplněn neutrální prvek N, tvoří grupu s operací $\oplus$ definovanou v (8.6), zbývá ještě dokázat asociativitu grupové operace. Takový důkaz ale není snadný a přesahuje rámec tohoto výkladu.

Poznamenejme ještě (srov. [9]), že rovnici (8.6) lze ekvivalentně zapsat takto

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

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

Lze ukázat, že rovnice

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

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

Na druhé straně rovnice

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

má nekonečně mnoho racionálních řešení (např. $(3, \pm 5)$). Jedna z klíčových otázek řešení rovnic typu (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, který vyvinul sofistikovanou metodu, jež pomáhá překonávat záhady eliptických křivek a rozhodovat, zda odpovídající diofantské rovnice mají konečný či nekonečný počet racionálních řešení. Na každé eliptické křivce existuje jen konečně mnoho celočíselných bodů, ale grupa racionálních bodů je typicky nekonečná,[4] i když je vždy konečně generována (Mordellova věta).

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

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

dokázal (viz [6]), že rovnice

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

pro $xyz \neq 0$ nemá řešení v množině Gaussových komplexních celých čísel $\mathbb{Z}[\mathrm{i}]$.

8.5. Závěr

John Tate se v roce 1950 ve své doktorské dizertaci [16] zabýval Fourierovou analýzou v číselných tělesech. Tím vytyčil zcela ojedinělou cestu k moderní teorii automorfních forem. Vyškolil přes 20 Ph.D. studentů v teorii čísel. Mnozí z nich se později velice proslavili, např. Joe Buhler, Joseph Silverman, Benedict Gross či Kenneth Ribet. Posledně jmenovaný ukázal, že Velká Fermatova věta plyne z Taniyamaovy-Šimurovy

[4] Existují však výjimky – viz např. (8.8).

Obr. 8.2. V jihofrancouzském Beaumont-de-Lomagne rodišti Pierra de Fermata v říjnu 1996: *Velká Fermatova věta byla tedy skutečně dokázána?* ptají se vesničané A. Wilese.

domněnky,[5] a tím pomohl A. Wilesovi s R. Taylorem k nalezení důkazu Velké Fermatovy věty. Domněnka byla v plné obecnosti dokázána až v roce 2001 v článku [3], kde je R. Taylor spoluautorem.

Další Tateův student, Carl Pomerance, ve své 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 [10], spolupodílel se na efektivní metodě pro testování prvočíselnosti (spoluautoři Adleman a Rumely) a na důkazu, že Carmichaelových čísel je nekonečně mnoho [5]. Prof. Tate tak měl podstatný vliv na rozvoj moderní teorie čísel i prostřednictvím svých studentů.

Sám Tate má velké množství publikací v prestižních matematických časopisech, např. v Annals of Mathematics [2], [7], [12] a [17]. Přitom práci [12] napsal s Jean-Pierrem Serrem, který získal Abelovu cenu za matematiku jako vůbec první. J. Tate se svým bývalým školitelem Emilem Artinem napsali hojně citovanou monografii [1], v níž je představen nový pohled na teorii číselných těles. V pořadí již osmá Abelova cena je tedy jistě ve správných rukou. Bez Tatea a jeho studentů by A. Wiles Velkou Fermatovu větu jen těžko dokázal (srov. obr. 8.2).

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

L i t e r a t u r a

[1] Artin, E., Tate, J.: *Class field theory*. AMS Chelsea Publ. 1967, 2009.

[2] Brauer, R., Tate, J.: *On the characters of finite groups*. Ann. of Math. *62* (1955), 1–7.

[3] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: *On the modularity of elliptic curves over Q: wild 3-adic exercises*. J. Amer. Math. Soc. *14* (2001), 843–939.

[4] Klazar, M.: *Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti*. PMFA *49* (2004), 177–188.

[5] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Edice Galileo, sv. 39, Academia, Praha 2009, 2011.

[6] 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.

[7] Lubin, J., Tate, J.: *Formal complex multiplication in local fields*. Ann. of Math. *81* (1965), 380–387.

[8] Mlýnek, J.: *Informační bezpečnost*. PMFA *51* (2006), 89–98.

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

[10] Pomerance, C.: *Vyprávění o dvou sítech*. PMFA *43* (1998), 9–29.

[11] Ribenboim, P.: *Fermat's Last Theorem for amateurs*. Springer, New York 1999.

[12] Serre, J.-P., Tate, J.: *Good reduction of abelian varieties*. Ann. of Math. *88* (1968), 492–517.

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

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

[15] Šolcová, A., Křížek, M., Mink, G. (eds.): *Matematik Pierre de Fermat*. Cahiers du CEFRES No. 28 Praha, 2002.

[16] 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.

[17] Tate, J.: *The higher dimensional cohomology groups of class field theory*. Ann. of Math. *56* (1952), 294–297.

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

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

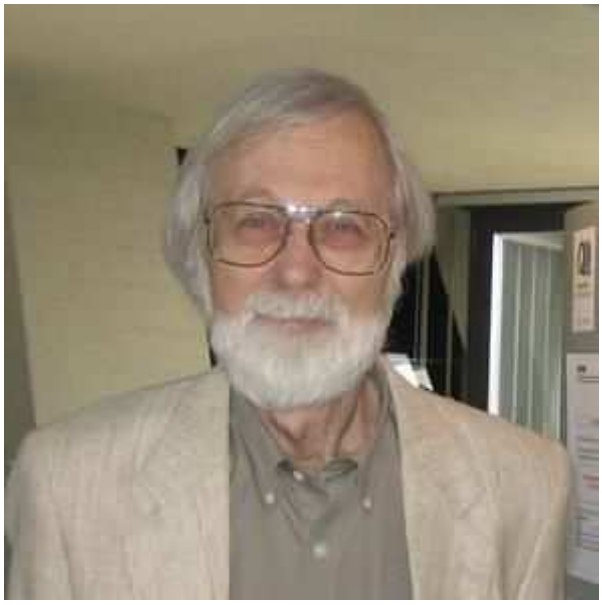
[20] `http://www.dtc.umn.edu/~odlyzko`

9. Abelovu cenu za rok 2011 získal John Milnor

Michal Křížek, Martin Markl

9.1. Úvod

Dne 23. března 2011 ve 12 hodin středoevropského času předseda Norské akademie věd, Øyvind Østerud, ohlásil, že Abelovu cenu za rok 2011 získává John Willard Milnor z University of Stony Brook 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 cenu za matematiku. Navíc je spojena s částkou 6 000 000 norských korun.



John Willard Milnor

John Milnor převzal Abelovu cenu z rukou norského krále Haralda V. na slavnostním shromáždění v Oslo dne 24. května 2011. Další den na Univerzitě v Oslo pronesl prof. Milnor laureátskou přednášku[1] 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 odvětil: *Řešitelem problémů. Nikdy jsem se nepokoušel vytvořit nějakou velkou teorii, ale snažil jsem se řešit různé drobné problémy a klást si záludné otázky. Nikdy však nevíte, co z toho může vzejít.*

Abelova cena se uděluje za výjimečně hluboké výsledky, které významně ovlivnily matematické vědy. Podle vyjádření výběrové komise (Abel Committee) John Milnor získal cenu za objevné 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 is a wonderfully gifted expositor of sophisticated mathematics. He has often trackled difficult, cutting-edge subjects, where no account in book form existed. Adding novel insights, he produced a stream of timely yet lasting works of masterly lucidity. Like an inspired musical composer who is also a charismatic performer, John Milnor is both a discoverer and an expositor.

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 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].

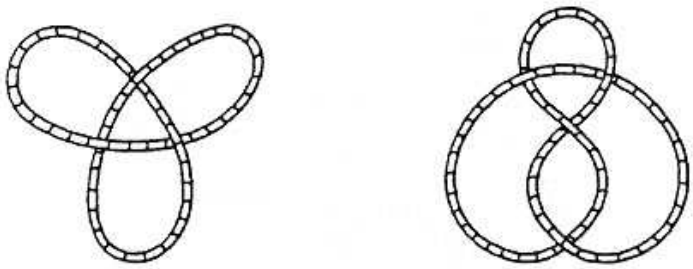
Fáryho-Milnorova věta. *Nechť K je uzavřená křivka v trojrozměrném eukleidovském prostoru dostatečně hladká tak, aby v každém jejím bodě existovala křivost κ. Splňuje-li celková křivost nerovnost*

$$\oint_K \kappa(s)\,ds \leq 4\pi, \tag{9.1}$$

pak K není zauzlená.[2]

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

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



Obr. 9.1. Schematické znázornění dvou zauzlených křivek.

Větu ve stejné době nezávisle vyslovil i Istvan Fáry, jenž její důkaz publikoval v Bulletin de la Societé 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, 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 grupami[3] a jejich zobecněními. Po absolvování doktorského studia pokračoval na univerzitě v Princetonu a později na Institute for Advanced Study, též v Princetonu, N. J. V roce 1989 přestoupil na univerzitu v Stony Brook v severní části Long Islandu, kde se spolupodílel na řízení Institute for Mathematical Sciences.

Milnorův nejznámější výsledek pochází z roku 1956, kdy objevil zvláštní sedmirozměrnou varietu – tzv. exotickou topologickou sféru, která má nestandardní diferenciální strukturu a není tedy difeomorfní se standardní sférou $\mathbb{S}^7$. 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. Tadatoshi 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 Mandelbrotovy množiny a také lokální souvislostí Juliových 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“.

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

Profesor Milnor získal během svého života celou řadu ocenění za vynikající vědecké výsledky. Připomeňme ty nejdůležitější. Před více než padesáti lety Milnor dostal Fieldsovu medaili (1962) a vzápětí se stal editorem Annals of Mathematics, kde působil několik let. V roce 1967 obdržel U.S. National Medal of Science a v roce 1989 Wolfovu cenu. Je jediným matematikem, který vyhrál tři Steelovy ceny Americké matematické společnosti za Seminal Contribution to Research (1982), Mathematical Exposition (2004) a Lifetime Achievement (2011). V roce 1994 byl zvolen zahraničním členem Ruské akademie věd a v roce 2004 se stal řádným členem The European Academy of Sciences, Arts and Letters. 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 sedmirozměrné sféře, viz [9]. Tento výsledek má navíc výhodu určité názornosti, proto mu v následujícím přehledu věnujeme nejvíce prostoru.

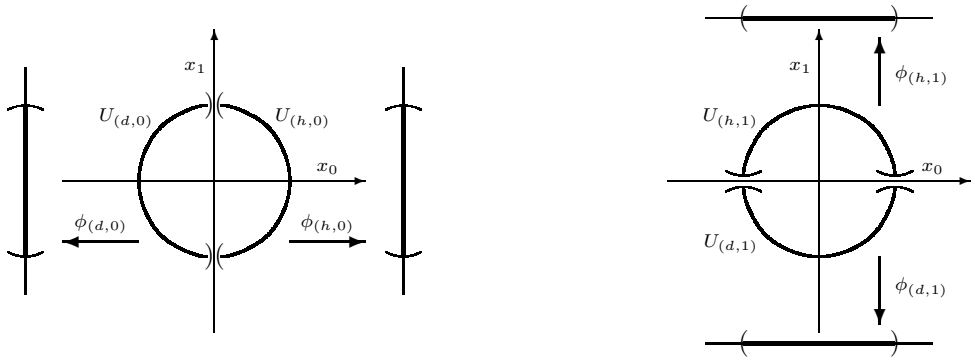
Ve zbytku kapitoly bude n označovat přirozené číslo. Standardní *jednotková n-rozměrná sféra* $\mathbb{S}^n$ je podmnožina bodů $(x_0, \dots, x_n)$ z $(n+1)$-rozměrného Eukleidova prostoru $\mathbb{R}^{n+1}$ vyhovujících rovnici $x_0^2 + \cdots + x_n^2 = 1$. Jednorozměrná sféra je tedy jednotková kružnice 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 domněnka[4] 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 spojité 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 spojité, ale má ve všech bodech derivace všech řádů. O to více překvapil Milnorův příklad sedmirozměrné 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, zopakujme si nejprve základní pojmy diferenciální topologie. Připomeňme, že *atlas* $\mathscr{A}$ 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 $\mathscr{A}$. Povšimněme si, že topologický prostor X s atlasem $\mathscr{A}$ je podle definice lokálně homeomorfní prostoru $\mathbb{R}^n$. Tvoří tedy *n-rozměrnou topologickou varietu*.[5]

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

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



Obr. 9.2. Atlas $\mathscr{A}_0$ pokrývá kružici $\mathbb{S}^1$ čtyřmi otevřenými polokružnicemi. Mapující zobrazení jsou homeomorfizmy na otevřené podintervaly $\mathbb{R}^1$.

Příkladem je standardní atlas $\mathscr{A}_0$ 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 $0 \le i \le n$ je

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

Označme π_i ortogonální projekci prostoru $\mathbb{R}^{n+1}$ do nadroviny $\big\{(x_0,\dots,x_n) \in \mathbb{R}^{n+1};\ x_i = 0\big\}$, tedy zobrazení vynechávající $i$tou souřadnici:

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

Mapující zobrazení $\phi_{(h,i)}$, resp. $\phi_{(d,i)}$ atlasu $\mathscr{A}_0$ 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 $\mathscr{A}$ na topologické varietě X. Pro každou dvojici indexů $\alpha, \beta \in A$ s neprázdným průnikem $U_\alpha \cap U_\beta$ definujme *přechodové zobrazení* $\phi_{\alpha\beta} : \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$ předpisem $\phi_{\alpha\beta}(x) := \phi_\beta\big(\phi_\alpha^{-1}(x)\big)$ pro $x \in \phi_\alpha(U_\alpha \cap U_\beta)$, viz diagram:

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

Přechodová zobrazení jsou zobrazeními mezi otevřenými podmnožinami $\mathbb{R}^n$. Atlas $\mathscr{A}$ 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 altlas $\mathscr{A}_0$ sféry $\mathbb{S}^n$ je hladký. Příslušnou hladkou strukturu nazýváme *standardní hladkou strukturou* sféry $\mathbb{S}^n$.

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

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

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 homeomorfizmus s hladkou inverzí se nazývá *difeomorfizmus*. 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 kvocient[6]

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

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 kvaternionů[7]. 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.*

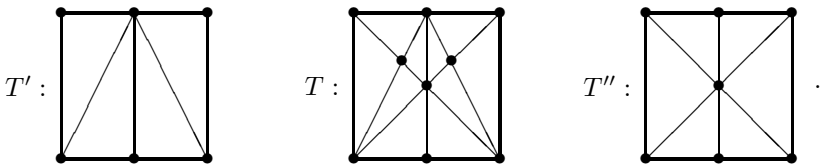
Volně řečeno, Milnorovu sféru M_3^7 sice můžeme homeomorfně zobrazit na standardní sféru $\mathbb{S}^7$, musíme ji však přitom „pomačkat“. Proto překvapí, že existuje homeomorfizmus prostoru M_3^7 na $\mathbb{S}^7$, který je difeomorfizmem všude kromě jediného bodu. Z tohoto důvodu se Milnorovým sférám někdy říká „rohaté sféry“. V roce 1963 J. Milnor společně M. A. Kervairem v [5] dokázal, že existuje 28 různých[8] 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

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

[7] Kvaterniony 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.

[8] Dvě hladké struktury považujeme za různé, jestliže se na sebe nedají převést homeomorfizmem.



Obr. 9.3. Tři triangulace čtverce.

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 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	17	18
řád grupy	1	1	1	**?**	1	1	28	2	8	6	992	1	3	2	16 256	2	16	16

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 doměnka*, 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 $\{e_0, \ldots, e_n\} \subset \mathbb{R}^{n+1}$. Můžeme jej také definovat jako množinu

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

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 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.

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 prostoru[9] s hranicí třírozměrného simplexu má dvě konečné triangulace bez společného zjemnění. Tím sestrojil *protipříklad* k Hauptvermutungu. Povšimněme si, že tento výsledek má podobnou příchuť 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 $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{C}^n$. 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 anuluje determinant *Hessiánu* funkce g, což je matice druhých derivací

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

Následující výklad zaměříme na funkce se singulárním bodem v počátku $\mathbf{0} := (0, \ldots, 0)$ a s nulovou funkční hodnotou v tomto bodě. Případ 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 $f(0, \ldots, 0) = 0$. 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 dimenze 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 $\mathbf{0}$ nedegerovanou 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 $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$ definujme perturbaci f_a funkce f předpisem

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

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 $\mu(f)$.

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

Milnorovo číslo má i topologickou charakterizaci. Symbolem $\mathbb{S}_\epsilon^{2n-1}$ 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

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

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

3) *Milnorova fibrace*

Připomeňme, že lokálně triviální hladká *fibrace* $p : E \to B$ je zobrazení hladkých variet, které je lokálně projekcí $B \times F \to B$, kde F je hladká varieta nazývaná *fíbrem* 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 $f : \mathbb{C}^n \to \mathbb{C}$ je nenulový komplexní polynom splňující $f(0, \ldots, 0) = 0$. Označme $\mathfrak{Z}_f$ nulovou množinu polynomu f,

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

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

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

Milnor dokázal, že pro dostatečně malá ϵ je restrikce

$$\mathrm{Arg}_f : \mathbb{S}_\epsilon^{2n-1} \setminus \mathfrak{Z}_f \to \mathbb{S}^1$$

lokálně triviální hladká fibrace, jejíž fíbr je varieta dimenze $2n-2$. V případě, že $\mathbf{0}$ je izolovaný singulární bod, má tento fíbr homotopický typ[10] sjednocení $\mathbb{S}^{n-1} \vee \cdots \vee \mathbb{S}^{n-1}$ se ztotožněnými bázovými body určitého počtu standardních $(n-1)$-rozměrných sfér.

Na závěr dovolte osobní poznámku druhého autora. Se jménem John Milnor jsem se seznámil jako student díky známé učebnici [14], kterou Milnor napsal společně s Jimem Stasheffem. Její četba byla požitek, stejně jako četba všeho, na čem se Milnor podílel. S Jimem jsem později napsal několik článků a monografii [7]. Johna Milnora jsem osobně poznal na konferenci v Princetonu v roce 1996.

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.

[10] Zhruba řečeno, topologické prostory mají stejný homotopický typ, pokud se liší spojitou deformací.

[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.* Coo-ment. 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] Křížek, 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. Úvod

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 dlouhotrvajícím vlivům na aditivní teorii čísel a ergodickou

Endre Szemerédi

teorii. Je to již desátá jubilejní Abelova cena od svého vzniku v roce 2003. Dalším matematikem maďarského původu, který tuto nejprestižnější cenu za matematiku získal v roce 2005, je Peter Lax. Matematika v Maďarsku má totiž dlouholetou tradici. Vzpomeňme několika dalších význačných maďarských matematiků světového významu, např. János Bolyai, Lipót Fejér, Marcel Grossmann, Alfréd Haar, András Hajnal, Cornelius Lanzcos, László Lovász, John von Neumann, Rózsa Péter, George Pólya, Alfréd Rényi, Marcel Riesz, Pál Turán a jeho manželka Vera T. Sós, Endre Süli, Karl Zsigmondy, a též Pál Erdős, který má v databázi Mathematical Reviews registrováno přes 1 500 vědeckých prací. Jen málo zemí velikosti Maďarska se může podobným seznamem pochlubit. Maďaři navíc mají 13 nositelů Nobelových cen.

Prof. Endre Szemerédi převzal Abelovu cenu z rukou norského krále Haralda V. dne 22. května v hlavní aule univerzity v Oslu. Při této příležitosti přednesli slavnostní proslov norská ministryně pro školství a vědu Kristin Halvorsen, předseda Norské akademie věd Nils C. Stenseth a předseda výběrové komise (Abelkomiteen) 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 Institute for Advanced Study 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 Szemerédiovy 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.*

Prof. 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 matematik 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 (viz obr. 10.1). V současnosti pracuje v Matematickém ústavu Alfréda Rényiho Maďarské akademie věd v Budapešti. Je též zaměstnán v Department of Computer Science, Rutgers, The State University of New Jersey v USA. Navíc je členem věhlasného Institute for Advanced Study v Princetonu, který se rovněž nalézá ve státě New Jersey. Endre Szemerédi je ženatý a má pět dětí.

10.2. Aditivní teorie čísel

V tomto článku se soustředíme na nejznámější Szemerédiovy výsledky z aditivní teorie čísel, z teorie grafů a teoretické informatiky. Aditivní teorie čísel se věnuje studiu

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

Obr. 10.1. Prof. Endre Szemerédi (vlevo) přebírá čestný doktorát v aule Univerzity Karlovy od prof. Jaroslava Nešetřila (vpravo).

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 Jingrun Chen 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 Chenova věta tvrdí, že pro každé sudé číslo s existuje nekonečně mnoho prvočísel p tak, že $p+s$ je buď prvočíslo, 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 $0, 1, 2, \ldots$, 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 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 Ramachandran Balasubramanian a kol. [3] dokázal, 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 $g(k) = 2^k - 2 + \lfloor (3/2)^k \rfloor$.

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 uvedeme jen jeden ilustrační příklad.

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

Pokusme se dokázat opak, tj. předpokládejme, že posloupnost $1, 2, \ldots, 9$ 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. Rozlišujme 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 všechna červená čísla, což je spor.

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

Dále vidíme, že posloupnost $\underline{1}\overline{2}\underline{3}\overline{4}\overline{5}\underline{6}\overline{7}\underline{8}$ 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 $1, 2, \ldots, 9$, 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.

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

10.3. 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] (která ze Szemerédiovy 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 $\mathbb{N} = \{1,2,3,\dots\}$ definujme *horní asymptotickou hustotu* $\mathbb{B}$ následovně

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

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, že 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 následující větu (viz [16]).

Szemerédiova 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. *Nechť 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. 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 nelze použít Szemerédiovu větu, neboť horní asymptotická hustota množiny $\mathbb{P}$ všech prvočísel je nula.

10.4. Erdősova-Szemerédiova 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 položme

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

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 a zároveň 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 $1/3$.

10.5. Szemerédiovo lemma o regularitě

Nejprve definujme 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 původní hustoty $\rho(A, B)$.

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

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

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.

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

(srov. (10.1)), takže 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 Szemerédiova lemmatu o regularitě se ukázalo, že jej 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 Szemerédiova 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 Rödlovi a jeho studentům a nezávisle také T. Gowersovi.

10.6. Szemerédiovy 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 třídicí síť* pojmenovaná podle počátečních písmen autorů článku [1].

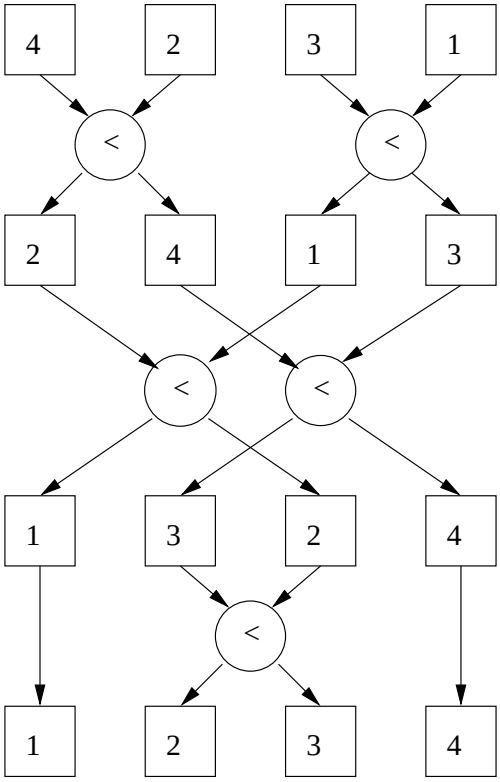
V informatice se často používají algoritmy na třídění. Jde o úlohu, kde je zadaná posloupnost prvků $(a_1, \ldots, a_n)$ nějaké uspořádané množiny a cílem je tuto posloupnost přerovnat tak, aby v ní byly prvky ve vzestupném pořadí. Bez újmy na obecnosti můžeme předpokládat, že zadaná posloupnost je permutací konečné posloupnosti $1, 2, \ldots, n$.

Třídicí algoritmus (síť) je posloupnost k kroků, kde každý krok je pevně daná množina vzájemně disjunktních dvojic indexů z množiny $\{1, 2, \ldots, n\}$. Tento algoritmus se na vstupní permutaci $a_1 a_2 \ldots a_n$ čísel $1, 2, \ldots, n$ 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. 10.2 je jednoduchý ilustrační příklad třídicí sítě $n = 4$ (není to AKS síť, protože tu lze vytvářet jen pro větší n).

Je snadné dokázat, že každá třídicí síť musí mít hloubku alespoň $\log_2 n$. Třídicí síť si totiž můžeme představit jako způsob, jak 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. 10.2, 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 $c \log n/2$.

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



Obr. 10.2. Příklad třídicí 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.

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

10.7. Závěr

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 grafů[4] či Szemerédiova-Trotterova věta o počtu incidencí přímek a bodů. Databáze Mathematical Reviews eviduje přes 170 jeho prací. Na některých z nich spolupracoval i s českými matematiky (Václavem Chvátalem, Vojtěchem Rödlem či Pavlem

[4]Každý 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.

Pudlákem, viz [2], [9]). Matematická společnost Jánose Bolyaie vydala v nakladatelství Springer sborník *An Irregular Mind* věnovaný sedmdesátým narozeninám E. Szemerédiho, kde se podrobně rozebírá jeho přínos pro matematiku. Nedávno byl také s ním 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.

[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., Deshouillers, 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. Sin. *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.* arXiv: 1201.6656 (přijato do Math. Comp.).

[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/`

Summary

The First Ten Abel Prizes for 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 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.

Niels Henrik Abel (1802–1829)

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 ten Abel Prizes. Each chapter contains a short biographical sketch of a particular laureate and his contribution to various fields of mathematics:

1. Jean-Pierre Serre (2003) – topology, algebraic geometry, and number theory
2. Michael Atiyah and Isador Singer (2004) – topology, geometry, and analysis
3. Peter Lax (2005) – numerical and applied mathematics
4. Lennart Carleson (2006) – harmonic analysis and dynamical systems
5. Srinivasa Varadhan (2007) – theory of probability and statistics
6. John G. Thompson and Jacques Tits (2008) – algebra and theory of groups
7. Michail L. Gromov (2009) – differential geometry
8. John Tate (2010) – algebraic number theory
9. John Milnor (2011) – differential topology, geometry, and algebra
10. Endre Szemerédi (2012) – discrete mathematics and theoretical computer science

ISBN 978-80-7015-014-6
EAN 9788070150146

$e = 2+\sqrt{5} - 2\sqrt{2+\sqrt{5}}$, $e = 2+\sqrt{5} + 2\sqrt{2+\sqrt{5}}$

de quelles la dernière valeur

$$e = 2+\sqrt{5} + 2\sqrt{2+\sqrt{5}} = \left(\frac{\sqrt{5}+1}{2} + \sqrt{\frac{\sqrt{5}+1}{2}}\right)^2$$

appartient à la question, car l'équation

$1 = e^3 \varphi^2\left(\frac{2\omega}{10}\right) \cdot \varphi^2\left(\frac{3\omega}{10}\right)$ nous montre que e doit être plus grand que l'unité.

Connaissant e on trouve la valeur des quantités $\varphi\left(\frac{\omega}{5}\right)$ et $\varphi\left(\frac{2\omega}{5}\right)$ comme il suit :

Nous avons

$$1 = e^3 \cdot \mathcal{P}^2 = e^3 \cdot \frac{f^2\left(\frac{\omega}{5}\right) \cdot f^2\left(\frac{2\omega}{5}\right)}{F^2\left(\frac{\omega}{5}\right) \cdot F^2\left(\frac{2\omega}{5}\right)}$$

en faisant $\varphi\left(\frac{\omega}{5}\right) = \alpha$ et $\varphi\left(\frac{2\omega}{5}\right) = \beta$ on aura

$f^2\left(\frac{\omega}{5}\right) = 1-\alpha^2$; $f^2\left(\frac{2\omega}{5}\right) = 1-\beta^2$

$F^2\left(\frac{\omega}{5}\right) = 1+e^2\alpha^2$, $F^2\left(\frac{2\omega}{5}\right) = 1+e^2\beta^2$

donc :

$$(1+e^2\alpha^2)(1+e^2\beta^2) = e^3 (1-\alpha^2)(1-\beta^2)$$

$$1 + e^2(\alpha^2+\beta^2) + e^4\alpha^2\beta^2 = e^3 - e^3(\alpha^2+\beta^2) + e^3\alpha^2\beta^2$$

$$e^3 - 1 = e^3(e-1)\cdot\alpha^2\beta^2 = e^2(e+1)\cdot(\alpha^2+\beta^2)$$

or nous avons trouvé plus haut $\alpha^2\beta^2 = \frac{\sqrt{5}}{e^3}$

donc

$$e^3 - 1 - e(e-1)\sqrt{5} = e^2(e+1)\{\alpha^2+\beta^2\}$$

On connaît donc $\alpha^2\beta^2$ et $\alpha^2+\beta^2$ et par suite α^2 et β^2 par la résolution d'une équation du second degré. On a donc aussi la valeur de y_1 qui satisfait à l'équation