Pokroky matematiky, fyziky a astronomie

Pavel Pudlák

Doslov k překladu Gentzenova článku „Současný stav ve výzkumu základů matematiky“

Pokroky matematiky, fyziky a astronomie, Vol. 37 (1992), No. 5, 270--272

Persistent URL: http://dml.cz/dmlcz/138899

Terms of use:

© Jednota českých matematiků a fyziků, 1992

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

Doslov k překladu Gentzenova článku

„Současný stav ve výzkumu základů matematiky“

Pavel Pudlák, Praha

Byl jsem požádán redakcí, abych stručně shrnul události, ke kterým došlo v této oblasti od doby napsání tohoto Gentzenova článku. Je to věc, která by si zasloužila podstatně podrobnější článek a delší přípravu, než mám k dispozici pro tento krátký doslov. Proto se omezím jen na vyjmenování nejdůležitějších událostí s vědomím toho, že poskytnu nové informace pouze matematikům, kteří se nezabývají matematickou logikou.

Podobně jako v jiných vědních oborech došlo v druhé polovině století v oblasti logiky a studia základů matematiky ke značné divergenci do speciálních oborů. V současné době se tato oblast dělí do tří základních oborů:

- matematická logika;
- filozofická logika;
- aplikace logiky v informatice.

Matematickou logiku lze považovat za jednu z matematických disciplín; filozofická logika se zabývá zkoumáním struktur lidského myšlení a zejména jazyků; aplikace logiky tvoří značnou část teoretického výzkumu v informatice. Nebudu vyjmenovávat podobory těchto základních směrů, zmíním se jen o těch podoborech matematické logiky, které souvisí se zkoumáním základů matematiky.

(i) V teorii množin se výzkum soustředil na axiomatickou teorii Zermela a Fraenkla (zkratka ZF) doplněnou o axióm výběru (zkratka ZFC). Tuto teorii akceptuje naprostá většina matematiků jako teorii popisující „skutečné“ množiny. Jiné systémy se nedostaly mimo rámec logické komunity (a obávám se, že mají naděje stejně malé, jako jsou naděje prosadit vedle angličtiny další světový jazyk). Vzhledem k paradoxním důsledkům nebyl axióm výběru přijat hned. Teprve když v roce 1940 Gödel dokázal, že pokud je ZF bezesporná teorie, potom je i ZFC bezesporná, se ukázalo, že je to vlastně neškodný axióm. Ve stejné práci Gödel učinil podstatný krok vpřed v řešení dalšího, z hlediska základů matematiky velice důležitého problému — tzv. hypotézy kontinua (CH). CH je tvrzení, že každá nekonečná množina reálných čísel je buď spočetná, nebo má stejnou mohutnost jako množina všech reálných čísel; jinak řečeno, mohutnost reálných čísel je první nespočetná mohutnost. Gödel dokázal, že bezespornost ZF implikuje bezespornost ZFC i s CH.[1]) To znamená, že CH

[1]) Přesněji řečeno, Gödel použil jiný systém, Gödelovou-Bernaysovou teorii množin, který je však ekvivalentní s ZFC.

RNDr. Pavel Pudlák, CSc. (1952), je samostatným vědeckým pracovníkem MÚ ČSAV, Žitná 25, 115 67 Praha 1.

nelze vyvrátit na základě ZFC, ale Gödel nevyloučil, že CH lze dokázat z ZFC. Nejdůležitějšího výsledku po důkazu Gödelových vět dosáhl Paul Cohen v roce 1966. Dokázal, kromě jiného, totéž co Gödel, ale pro negaci CH. Tudíž ani CH ani negace CH není dokazatelná ZFC, jinak řečeno CH je nezávislá na axiómech ZFC. Cohenova metoda („forcing“) má široké aplikace a umožnila dokázat mnoho dalších nezávislostí. Podívejme se však na Cohenův výsledek z hlediska základů. To, že existuje tvrzení nezávislé na ZFC plynulo už z první Gödelovy věty. Gödelova konstrukce dává ovšem tvrzení velice umělé a proto bylo možno doufat, že v matematické praxi se s tímto jevem nesetkáme. To se nepotvrdilo, protože CH se týká jednoho z centrálních objektů — kontinua reálných čísel. Druhá důležitá skutečnost je, že se dosud nepodařilo rozšířit ZFC o axióm založený na nějakém obecném principu tak, aby rozšířená teorie rozhodla platnost CH. Zdá se, že se budeme muset smířit s tím, že pojem množiny je nejednoznačný už na tak nízké úrovni, jako jsou podmnožiny reálných čísel.

Abych popsal další důležitý směr v teorii množin, musím se chvíli zabývat axiomatikou ZFC. Tato teorie vychází z myšlenky, že antinomie jsou způsobeny tím, že se připouští definice „velkých“ množin. Proto ZFC postuluje, že existuje nějaká (malá) množina a že universum množin je uzavřeno na určité operace. Tyto operace ale nemohou vytvořit nekonečnou množinu z konečných, proto je nutno mít v ZFC tzv. axióm nekonečna, který říká, že existuje nekonečná množina. Potom lze dokázat existenci množin mnohem větších mohutností. Označme ω_α $(\alpha + 1)$-ní nekonečné kardinální číslo. Potom můžeme dokázat existenci ω_0, ω_1, ..., $\omega_{\omega_{\omega_0}}$ etc. Nelze ale dokázat existenci kardinálního čísla α takového, že $\omega_\alpha = \alpha$. Takové číslo se nazývá (slabě) *nedosažitelné*. Axióm o existenci nedosažitelného kardinálního čísla můžeme chápat jako jakýsi silnější axióm nekonečna. Z hlediska filozofie, na které je ZFC založeno, je přirozené zesílit tuto teorii o axióm tohoto typu. Čísla, jejichž existence se takto postuluje, se nazývají *velká kardinální čísla*. Bylo prozkoumáno mnoho značně větších kardinálních čísel, než je první nedosažitelné. Zkušenost ukázala toto:

1. ani v ZFC zesíleném o velice velká kardinální čísla nebyl nalezen spor;
2. přes očekávání mnohých se nepodařilo rozhodnout platnost CH na základě žádného axiómu o velkých kardinálních číslech.

(ii) Když Cohen dokázal nezávislost CH, naskytla se přirozená otázka: může se neúplnost teorií projevit takovýmto explicitním způsobem na nižší úrovni, konkrétně v přirozených číslech? Z důkazu Gödelovy věty plyne, že se pro danou teorii dá napsat pravdivé, ale v této teorii nedokazatelné tvrzení (dokonce — při použití Matijasevičovy věty — můžeme sestrojit neřešitelnou diofantickou rovnici takovou, že v dané teorii není dokazatelné, že tato rovnice je neřešitelná). Nicméně takové tvrzení je umělé a vzdálené zajímavým matematickým problémům. Proto vzbudil velký ohlas výsledek Parise a Harringtona dosažený v roce 1977. Dokázali, že jistá modifikace známé Ramseyovy věty není dokazatelná v aritmetice prvního řádu. Potom byla nalezena další kombinatorická tvrzení nedokazatelná v aritmetice prvního řádu a některá nedokazatelná v silnějších systémech (dokonce v ZFC). Ač zde použité metody poskytují pěkné výsledky, nelze je použít na důkaz nedokazatelnosti známých otevřených problémů v teorii čísel, kombinatorice a teorii složitosti. Proto výzkum v této oblasti pokračuje a soustřeďuje se na slabší axiomatické systémy, kde je větší pravděpodobnost, že určité tvrzení není dokazatelné.

(iii) Další důležitý mezník souvisí spíše s problémem než řešením. Jde o slavný problém zda P = NP formulovaný A. S. Cookem v roce 1971. Je to hlavní a dosud nevyřešený problém dnes už samostatné disciplíny — teorie složitosti. Teorie složitosti patří spíše do teoretické informatiky, ale původní zdroje pro P = NP? jsou v teorii rekurzívních funkcí a studiu složitosti výrokového počtu. Je to problém fundamentálního charakteru: vztah existence a konstruovatelnosti na jedné straně, vztah konečna (reprezentovaného polynomiálním počtem kroků) a nekonečna (reprezentovaného exponenciálním počtem kroků) na straně druhé. V poslední době se nachází víc a víc souvislostí mezi logickými teoriemi a teorií složitosti.

(iv) Nakonec se ještě zmíním o dvou směrech v matematické logice, o kterých Gentzen mluví ve svém článku — o intuicionismu a důkazech bezespornosti, i když v těchto otázkách nedošlo k tak zásadním objevům jako jsou výše uvedené. Intuicionismus jako směr v základech matematiky má ještě pořád své příznivce, ale jejich počet klesá. Největšího uplatnění dosáhla intuicionistická logika (je to logický systém, který určitým způsobem zobecňuje klasickou logiku). Metodu, kterou Gentzen použil ke svému důkazu bezespornosti dále rozvíjela zejména mnichovská logická škola. Tato metoda je nazývána ordinální analýzou teorií. Cílem je pro danou teorii popsat nejmenší ordinální číslo takové, že pro ně nelze dokázat princip dobrého uspořádání. (Tento pojem bohužel není srozumitelný bez podrobnější definice, pro kterou zde nemám dost místa.) Tímto způsobem se podařilo analýzovat podstatně silnější teorie než je aritmetika prvního řádu, kterou zkoumal Gentzen, ale to, o čem snil Gentzen, totiž dokázat bezespornost aritmetiky druhého řádu (to je to, čemu se v logické hantýrce říká „analýza“), se z dnešního hlediska jeví jako velice vzdálený cíl.

Literatura

[1] P. J. COHEN: *Set Theory and the Continuum Hypothesis.* Benjamin, 1966.

[2] S. A. COOK: *The complexity of theorem-proving procedures.* Proc. 3-rd Ann. ACM Symp. on Theory of Computing, 1971, str. 151–158.

[3] K. GÖDEL: *The consistency of the continuum hypothesis.* Ann. Math. Studies, Vol. 3, 1940.

[4] J. PARIS, L. HARRINGTON: *A mathematical incompleteness in Peano Arithmetic.* In *Handbook of Mathematical Logic*, BARWISE ed., 1977, str. 1133–1142.

[5] A. A. FRAENKEL, Y. BAR-HILLEL, A. LEVY: *Foundations of Set Theory.* North-Holland, 1973.