Ladislav Rieger

Problém tzv. absolutně nerozhodnutelných vět teorie čísel

Časopis pro pěstování matematiky, Vol. 85 (1960), No. 1, 1--13

Persistent URL: http://dml.cz/dmlcz/108122

ČASOPIS PRO PĚSTOVÁNÍ MATEMATIKY
Vydává Matematický ústav ČSAV, Praha
SVAZEK 85 * PRAHA 18. II. 1960 * ČÍSLO 1

PROBLÉM TZV. ABSOLUTNĚ NEROZHODNUTELNÝCH VĚT TEORIE ČÍSEL

LADISLAV RIEGER, Praha

(Došlo dne 17. prosince 1958)

Jedná se o kritický rozbor problému formální (relativní) a obsahové (absolutní) nerozhodnutelnosti vět teorie čísel. Je poukázáno (na základě autorových výsledků jednak do časopisu Чех. Мат. ж. k tisku přijatých a jednak připravovaných) na potřebu radikálního opuštění dosud zastávaného názoru o tzv. obsahové kategoričnosti teorie čísel. Je naznačena autorova nová algebraicko-logická metoda tzv. dyadických okruhů, která by mohla přispět k řešení problému.[1])

ÚVODNÍ POZNÁMKA

Uvedený principiální problém patří na rozhraní elementární teorie čísel, axiomatické teorie množin a matematické logiky. Přitom obsahově absolutně nerozhodnutelnou nazývejme, zhruba řečeno, takovou větu dané matematické teorie (např. elementární teorie čísel, nebo elementární geometrie), k níž existují dva modely této teorie: jeden, v němž věta platí, a druhý, v němž věta neplatí. Tak např. v tzv. absolutní (elementární) geometrii je eukleidův rovnoběžkový postulát takovou větou (neboť vedle modelu normální eukleidovské roviny, kde postulát platí, máme v této rovině např. Poincarého model Lobačevského roviny, kde rovnoběžkový postulát neplatí).

Sám problém absolutně nerozhodnutelných vět elementární teorie čísel (či konkretněji peanovské aritmetiky) byl, pokud je autorovi známo, výslovně publikován teprve v referátu profesora A. MOSTOWSKÉHO o současném stavu teorie základů matematiky na sjezdu Polských matematiků ve Varšavě v r. 1953 (viz [1], str. 23). V podstatě byla ovšem problematika absolutně nerozhodnutelných vět teorie čísel otevřena vlastně již proslulou klasickou prací [2] K. GÖDELA.

[1]) Článek je zpracováním přednášky, kterou měl autor v matematické obci pražské dne 10. listopadu 1958.

Autor — přes dosavadní neúspěchy (svoje i jiných) v pokusech o řešení tohoto obtížného problému — se domnívá, že nicméně našel ve svých posledních výsledcích (viz [3]) nové cesty, jež by mohly řešení usnadnit; naznačení těchto metod je věnována závěrečná část článku. Popudem tu bylo mj. také nedávné sdělení amerického matematika JOHNA KEMENYHO na Světovém kongresu matematiků v Edinburku v r. 1958 o výsledku, jímž byla (matematicko-logickými metodami teorie tzv. nestandartních modelů peanovské aritmetiky) v jistém smyslu „téměř" prokázána absolutní nedokazatelnost proslulé Goldbachovy hypotézy z pouhých Peanových axiomů. [Toto „téměř" nedovede autor bohužel na základě kusého sdělení ve sjezdové knížce referátů přesně tlumočit; vyrozumívá jen, že se snad Kemenymu podařilo sestrojit jistý systém objektů, řekněme „přirozených quasi čísel" (s relací „následníka") tak, že jsou zaručeny kromě prvých tří Peanových axiomů i některé (důležité) případy čtvrtého axiomu, tzv. axiomu úplné indukce (který je ve skutečnosti schematem, tj. souhrnem nekonečně mnoha indukčních axiomů), ale při tom neplatí Goldbachova hypotéza (ne každé „quasi-číslo" > 2 se dá psát jako součet přesně tří „quasiprvočísel").]

AXIOMATISACE A FORMALISACE ELEMENTÁRNÍ TEORIE ČÍSEL

Připomeňme nejprve čtyři základní stadia matematicko-logické analysy dané matematické teorie, majíce na mysli především elementární teorii čísel:

1. Systematické nahrazení všech známých vět a definic dané skutečné, v hovorové řeči formulované teorie, systémem (konečně mnoha) konečných posloupností jistých základních znaků (tj. zavedení normovaných, jednoduchých i složených symbolických zkratek místo hovorových slov a vět). (*Kodifikace.*)

2. Vytčení primitivních pojmů a axiomů a na tom spočívající charakterisace obsahového vztahu logického důsledku mezi (symbolisovanými) větami dané matematické teorie jistým jejich vztahem formálně-kombinatorickým (tj. vztahem mezi konečnými posloupnostmi základních znaků bez ohledu na jejich význam). (*Formalizace vztahu důsledků.*)

3. Matematická konstrukce *idealizované* („extrapolované") nekonečné (symbolické) „*řeči*" dané teorie ve smyslu zavedení neomezeného množství možných (přípustných) nových matematických proměnných, konstant, „vět", „důkazů", „definic" atd. (jež mohou být předem neomezené délky a sotva představitelného smyslu).

4. Vystižení zákonitosti nejprve bezprostředně kombinatoricky definovaného vztahu důsledku (v ideální „nekonečné" symbolické „řeči" teorie) pomocí vhodné matematické teorie, např. opět elementární teorie čísel, nebo (méně bezprostředně) pomocí teorie zobecněných spočetných Booleových

σ-algeber, pomocí axiomatické teorie konečných množin apod. (*Matematická logika dané teorie.*)

Pro teorii čísel nejjednodušší přímé užití tohoto postupu jednoznačně dává dosud nejvíce užívaný systém formalizované aritmetiky (pocházející od D. Hilberta a P. Bernayse, viz [4]), jímž je bezprostředně idealisovaná a formalizovaná peanovská aritmetika s metamatematickým schematem indukce, opřená o primitivní relaci následníka.

Peanovské axiomatické indukční schema představuje však vlastně nekonečně mnoho aritmetických axiomů a ukazuje se, že při zachování následníka jako primitivního pojmu nelze ani za cenu dodání dalších primitivních pojmů vystačit s konečným počtem axiomů. To ovšem znamená, že již samo vytčení axiomů peanovské aritmetiky vyžaduje pojem neomezeného množství přirozených čísel.

Třebaže tato okolnost (při opatrné formulaci) není logicky závadná, je nicméně zdrojem četných metamatematických obtíží. Zejména pokud jde o náš problém absolutně nerozhodnutelných vět aritmetiky, jsou tyto potíže dány nutností verifikovat nekonečně mnoho axiomů v příslušných modelech a jsou dosavadními prostředky sotva překonatelné.

Řekněme proto hned, že je tu i možnost zcela jiné konečné axiomatisace a formalisace aritmetiky; je dána 19ti Gödelovými axiomy (viz [5]) teorie tzv. konečných množin, kde původní axiom C 1 (nekonečna) je nahrazen svým opakem (tzv. axiomem konečna). Zde ovšem primitivním pojmem je relace náležení množiny do třídy; pojem následníka lze definovat. Tato množinová axiomatisace (a formalisace) elementární teorie čísel není sice bezprostřední, má však mnoho výhod. Aniž bychom zde mohli zacházet do podrobností, dodejme ještě, že se tím do teorie čísel nezavádí žádný cizí „nearitmetický" prvek. To vyplývá z jednoho autorova nedávného (dosud neuveřejněného) výsledku, podle něhož Gödelova axiomatická teorie konečných množin je plně ekvivalentní s jistou axiomatickou teorií základních aritmetických operací, sečítání, násobení, dělení se zbytkem a mocnění dvojky jako primitivních pojmů (blíže viz závěr).

Nyní můžeme v rámci axiomatické teorie množin formulovat problém tzv. absolutně nerozhodnutelných vět elementární teorie čísel přesně a nadějněji než prve. Je to (v podstatě) úkol udat větu z axiomatické teorie konečných množin, k níž by (v dané celé axiomatické teorii množin) byl sestrojen jednak model, v němž věta platí, jednak model, v němž věta neplatí.

ABSOLUTNÍ A FORMÁLNÍ NEROZHODNUTELNOST

K další orientaci v našem problému bude ještě vhodné kriticky rozebrat pojem tzv. formálně nerozhodnutelných vět aritmetiky ve smyslu Gödelově. (Viz klasický výsledek Gödelův z r. 1931 [2] a jeho rozmanitá zdokonalení pocházející od B. Rossera, A. Tarského, S. Kleeneho, L. Kalmára a pak dosud nejobecnější systematické zpracování celé teorie v Mostowského monografii [6] s bohatou literaturou.)

Jde o věty formalizované peanovské aritmetiky, které lze udat při každé její rekurentní formalizaci a k nimž (v dané formalizaci) neexistuje ani formální důkaz ani formální vyvrácení.

Nejprve je třeba si uvědomit okolnost, že čistě číselně teoretický smysl gödelovských vět nám uniká pro jejich nepřehlednou délku a komplikovanost. Jde vždy o uměle vytvořenou „teoretickou" větu, jejíž úplné slovní vypsání by zaujalo v každém případě několik tiskových stran.

Na druhé straně ovšem metamatematický (aplikovaný) smysl gödelovských vět vesměs mluví ve prospěch jejich obsahové správnosti.

Byly to zejména tyto dvě skutečnosti (vedle celé řady dalších momentů a vžitých představ), které vedly k následujícímu dosud běžnému výkladu formální gödelovské nerozhodnutelnosti. (Srov. např. předmluvy k I. a II. dílu monografie [4] nebo shora citovaný referát [1]; mám při tom na mysli výklady matematicky střízlivé.)

I. Nerozhodnutelnost gödelovských vět aritmetiky je třeba chápat jako nerozhodnutelnost výlučně formálního rázu, tj. ona nijak nemusí souviset s nerozhodnutelností ve smyslu číselně teoretického obsahu resp. pravdivosti gödelovských vět, a to tím spíše ne, že podobně jako ve formalizované aritmetice lze gödelovsky nerozhodnutelné věty sestrojit v každé obšírnější formalizované matematické teorii (resp. i v tzv. systémech matematické logiky vyšších typů). Je tedy gödelovská nerozhodnutelnost spíše *výrazem principiální omezenosti rekursivní formální metody matematické logiky než dokladem existence obsahově nerozhodnutelných vět z teorie čísel.*

II. Přirozená čísla jsou základní a evidentní matematické předměty, které však nelze uspokojivě charakterisovat vytčením axiomů a odvozovacích pravidel aritmetiky. Axiomatická metoda není (na rozdíl od elementární geometrie) pro elementární aritmetiku vhodná. Vlastní metodou budování elementární aritmetiky je metoda intuitivně konstruktivní. (*Stanovisko konstruktivně intuitivní kategoričnosti.*)

III. Uvažovat o obsahové (absolutní) nerozhodnutelnosti určité věty elementární teorie čísel nemá exaktního smyslu, pokud nemáme potřebnou „minimální" axiomatizaci této teorie, aby bylo možno precizovat matematicky pojem jejího modelu.

IV. Sama konstrukce formalizované teorie a pojem důkazu jsou vždy podstatně rekurentní; už proto každá exaktní metamatematika je (aplikovaná) intuitivní (konstruktivní) aritmetika, jakožto ostatně nejprostší a zároveň nejbezpečnější matematická disciplina; nemá smyslu v kritické matematické logice užívat jiných, zejména ne tzv. infinitních prostředků (jako např. prostředků, patřících do matematické analýzy), neboť ty samy k svému založení potřebují kritické finitní matematiky.

Nechme stranou dobře možnou kritiku stanoviska IV (srvn. [6]) a připusťme, že vlastními metodami matematické logiky jsou jen metody aritmetické. Pokusme se nicméně kriticky rozebrat body I, II, III. To je nutné už proto, že podle nich s hlediska právě vyloženého se jeví být otázka absolutně nerozhodnutelných vět aritmetiky neaktuální, ne-li vůbec beze smyslu, tj. nemá smyslu hledat strukturně odlišné modely intuitivně kategorické teorie, která není axiomatisována.

Nebude na škodu pro kritiku právě podaného výkladu zjevu gödelovské formální nerozhodnutelnosti si uvědomit, na čem tento zjev spočívá. Gödelova metoda (a příbuzné metody) vycházejí heuristicky vždy z některé ze známých tzv. semantických antinomií (jako je antinomie lháře, antinomie Richardova, antinomie Berryho apod.). Nahrazením vágních obecně semantických pojmů užšími a přesnějšími pojmy aritmetizované metamatematiky, v případě že zkoumanou teorií je sama (formalizovaná) aritmetika, dosahuje se vhodným diagonálním postupem nikoli již antinomie, nýbrž (v aritmetické formě) jistých vět o větách, které v případě bezespornosti formalizované aritmetiky nemohou být ani formálně dokazatelné, ani formálně vyvratitelné (t. j. ani pro ně, ani pro jejich opak neexistuje formální důkaz). Přitom je však jedno podstatné: Ta část intuitivní aritmetiky, která byla fakticky užita v aritmeticky formulované metamatematice formalizované aritmetiky, nejen může, ale přímo (a podle II shora) musí být považována za konečný fragment aritmetiky formalizované. (Tento principiální předpoklad zůstává, i když se po vzoru Kleeneho a Mostowského původní semantická heuristika nahradí matematičtějšími analogiemi s teorií projektivních resp. Borelovských množin.)

Je však jasné, že každá pochybnost o bezvýhradné obsahové kategoričnosti aritmetiky sub II má za následek i jisté pochybnosti o logické (nikoli matematické) legitimnosti dosavadního výkladu Gödelova výsledku. To jest, vzniká otázka, zda nejde o neúspěch formálně axiomatické metody založení aritmetiky vůbec, ale o jistou nevhodnou aplikaci této metody. Jakmile bychom totiž připustili více neisomorfních druhů přirozených čísel, nutno se ptát, který z nich má být užit v metamatematice aritmetiky a zda to má být týž druh čísel, který je právě objektem vyšetřované (formalizované) aritmetiky. Mohlo by se také stát, že na tom by podstatně záviselo pojetí a posouzení formální rozhodnutelnosti té které věty, jakož i posouzení uspokojivosti formulace pojmu (formálního) důkazu formalizované aritmetiky; to by případně Gödelův výsledek podstatně dále relativizovalo. [Tato možnost je ostatně dobře myslitelná, uvážíme-li např. Gentzenův důkaz bezespornosti (viz [8]) aritmetiky, vedený v jistém smyslu „finitními" prostředky, zatím co věta, vyjadřující (aritmeticky) bezespornost formalizované aritmetiky patří ke gödelovským formálně nerozhodnutelným větám.] Uvidíme níže další důvody k tomu, že vskutku jsou takové pochybnosti o stanovisku sub II na místě.

Nejprve ještě ale poznamenejme, že na druhé straně už sám objev formální gödelovské nerozhodnutelnosti (ve formalizované aritmetice) vyvolal první pochybnosti o obsahové kategoričnosti aritmetiky (sub II). Opuštění tohoto tradičního gnoseologického stanoviska tedy, i když by ev. vedlo k změně (a relativizaci) výkladu Gödelova výsledku, by bylo nicméně výrazem dalšího myšlenkového vývoje, samým Gödelem vyvolaného.

Kritisován může být dále gnoseologický pesimismus, nutně z bodů I a II plynoucí, pokud jde o možnosti metamatematicko-logické na formalizaci vztahu důsledku založené metody (je vyjádřen mj. v III). Opustíme-li však stanovisko sub II, objevují se nové možnosti matematické logiky, i když připustíme omezení jejich prostředků na aritmetiku (což není nutné).

V neposlední řadě je třeba uvážit tuto námitku: Zastánci konstruktivistického pojetí, jak se během let ukázalo, jsou šmahem nuceni neustále modifikovat původní zásady konstruktivně finitní metamatematiky (viz např. zcela případné kritické poznámky překladatele v ruském překladu jinak velmi přesné učebnice Kleeneovy [9]), jakmile jen se dostanou za elementární úvahy. Je tedy otázka, zda i značně nedůsledná tzv. konstruktivní (intuitivní) metoda budování metamatematické aritmetiky může být považována za uspokojivou, resp. vůbec za realizovatelnou, zejména pokud jde o negativně existenční tvrzení tvaru „neexistuje číslo takové, že ...“; srov. také doplněk na konci tohoto článku.

A konečně je třeba uvést, že tzv. nenormální (s normálními neisomorfní) modely aritmetiky byly v podstatě bez metamatematických úvah sestrojeny už v létech 1933—34 (viz [10]) nezávisle na Gödelových výsledcích. T. Skolem totiž ve skutečnosti (i když ne zcela přesným způsobem a užívaje kritizovatelných prostředků intuitivní teorie množin) ukázal, že každá spočetná formalizovaná teorie čísel (v níž je spočetně mnoho znaků pro číselné proměnné, číselné konstanty a číselné operace, ale není jiných základních znaků) má kromě svého obvyklého číselného modelu ještě jiný model, sestávající z jistých tříd posloupností těchto čísel (přičemž třídy konstantních posloupností tvoří zde vlastní část isomorfní s původními čísly). Je zajímavé, že Gödel ve své recensi Skolemovy práce [10] (viz [11]) poznamenává, podle mého mínění ne zcela správně, že výsledky Skolemových úvah lze vesměs odvodit i jeho (Gödelovými) metodami. Je ovšem stále ještě běžné také Skolemův výsledek vykládat s hlediska námi kritisovaného (viz I, II shora) jako jen jiné potvrzení zejména bodu II, tj. jako zásadní neschopnost metodou axiomatizace a formalizace vystihovat zákonitosti přirozených čísel; sám Skolem se klonil k takovému výkladu.

Přejděme nyní ke kritice názorů sub I, II, III na základě novějších výsledků, včetně výsledků autorových.

Především řada po staletí otevřených elementárních číselných problémů podle autorova názoru nutně vybízí k domněnce, že jde o problémy v jistém smyslu neřešitelné. Také další práce v teorii nenormálních modelů peanovské aritmetiky (autorů B. Rossera, Hao Wanga a zejména J. Kemenyho v posledním jeho shora uvedeném výsledku) se zdají stále rozhodněji svědčit o dobré možnosti nalézt věty elementární teorie čísel, které jsou nejen formálně, ale i obsahově nerozhodnutelné, tedy o potřebě změnit stanovisko sub II a III. (Srovnej však ještě zmíněný Mostowského referát [1], v němž se autor takové změně rozhodně brání.) Lze ovšem říci, že přesvědčivost těchto prací (vesměs navazujících na [10]) o nenormálních modelech peanovské formalizované aritmetiky (pokud jde o zdůvodnění potřeby opustit stanovisko intuitivní kategoričnosti aritmetiky) ještě trpí okolností, že se musí užít už v samé formulaci axiomů aritmetiky pojmu přirozeného čísla. Obtíže přitom nejsou menší, užije-li se absolutního (intuitivního) pojmu přirozeného čísla, nebo užije-li se pojmu relativního „přirozeného čísla". Tento pojem je sice stanoven pomocí vytčeného konečného počtu axiomů indukce, ale zato příliš volně, pokud se užívá pojmu následníka jako primitivního pojmu.

Avšak právě tuto závadu se snad podařilo autorovi jeho teorií dyadických druhů obejít (viz [3]) a vyloučit jak z formulace aritmetiky tak i z konstrukce jejich modelů metamatematické úvahy.[2]) (Ve skutečnosti se navíc podařilo sestrojit bez metamatematických úvah celou nespočetnou škálu nenormálních modelů aritmetiky, jakož i model aritmetiky, v němž je nespočetně mnoho „přirozených" čísel.)

Rýsuje se tedy vskutku stále zřetelněji možnost, že se dostáváme v základech teorie čísel do situace podobné základům geometrie před více než 130 lety. Můžeme to — shrnujíce uvedené — na rozdíl od stanoviska sub I a II shora vyslovit asi tímto soudem (který ovšem není prost osobního přesvědčení autorova):

Tzv. nenormální (vzájemně neisomorfní) modely teorie čísel nelze považovat dnes již za pochybné metamatematické kuriosity, ale je třeba vzít na vědomí jejich existenci jako řádných matematických objektů. Může tedy existovat více aritmetik a to je příčinou, proč od peanovských (anebo jiných) axiomů nelze žádat jednoznačnou definici pojmu přirozeného čísla, stejně jako od geometrie nelze žádat jednoznačnou definici pojmů bod a přímka. Pojem a představa neozemené posloupnosti přirozených čísel je totiž jen zdánlivě („názorně") jednoznačná. Ve skutečnosti mohou platit další axiomy pro ten který podstatně odlišný druh přirozených čísel; jaké axiomy budou užívány, to ukáže další vývoj teorie čísel a jejich aplikací (srovnej dále). Že by se žádný axiomatický systém (a formalizace) pro exaktní základy aritmetiky nehodil,

[2]) To ovšem neznamená, že by metamatematické pojmy nadále nehrály důležitou roli heuristicko-metodickou!

to nelze pak již jako dříve na základě tradičního výkladu Gödelova s Skolemova výsledku tvrdit (srv. shora). Ovšem nelze také tvrdit, že jeden axiomatický systém aritmetiky vystačí provždy a všude.

Je však třeba kriticky zdůraznit toto: Pokud se neprokáže absolutní nerozhodnutelnost aspoň jedné konkrétní číselně teoretické věty (vzhledem k základním axiomům), a ta právě ještě ze samé prokázané obsahové nekategoričnosti aritmetiky nevyplývá, potud analogie s růzností geometrií zůstane omezena na cosi, co odpovídá zhruba různosti dimensí, totiž na různost typů resp. mohutností různých druhů přirozených čísel.

Je tedy gnoseologický smysl problému absolutně nerozhodnutelných vět teorie čísel ten, že teprve jeho kladné řešení by znamenalo průkaz analogie s geometrií i v druhém, mnohem hlubším smyslu, a to ve smyslu mnohosti axiomaticky podstatně různých aritmetik, podobné mnohosti axiomaticky různých geometrií.

Budiž na tomto místě autorovi dovoleno vyslovit konkrétní domněnku, že by absolutně nerozhodnutelným postulátem přidaným k axiomatické aritmetice snad mohlo být např. positivní řešení tzv. anonymova prvočíselného problému (viz [12] díl I, Chap. XV, p. 376). Je to otázka, zda všechna čísla tvaru

$$2+1\,,\quad 2^2+1\,,\quad 2^{2^2}+1\,,\quad 2^{2^{2^2}}+1\ldots$$

(až snad na konečně mnoho výjimek, jež ale dosud nebyly zjištěny) jsou prvočísla. (Všechny metody teorie čísel, elementární, algebraické, analytické totiž zde selhávají pro enormní vzrůst iterované mocniny dvojky.)

DYADICKÉ OKRUHY A PROBLÉM ABSOLUTNĚ NEROZHODNUTELNÝCH VĚT TEORIE ČÍSEL

V souvislosti s předchozím zbývá konkretněji odpovědět i na bod III shora formulovaného a dnes běžného skeptického názoru na účinnost metod matematické logiky v aritmetice vůbec a v problému absolutně nerozhodnutelných vět zvláště. To souvisí s naznačením nových metod, jakými podle autorova názoru matematická logika přece jen může k řešení problému absolutně nerozhodnutelných vět aritmetiky přispět a které se již osvědčily v zmíněné snadnější otázce škály nenormálních modelů různých ordinálních typů pro axiomatickou aritmetiku (ve smyslu axiomatické teorie konečných množin).

Nazveme (viz (3)) *dyadickým okruhem* diskretně uspořádaný okruh s axiomaticky zavedeným mocněním dvojky na libovolný nezáporný prvek okruhu ve smyslu axiomů

$$2^1 = 2\,,\quad 2^x\,.\,2^y = 2^{x+y}\,,\quad 0 \leqq x < 2^x$$

a ještě dvou dalších, z nichž jeden žádá možnost dělení se zbytkem každého prvku okruhu libovolnou mocninou dvojky a druhý žádá existenci maximální mocniny dvojky, dělící daný nenulový prvek beze zbytku. (Zřejmě obyčejný okruh celých čísel je dyadickým okruhem; lze však udat i zcela jiné dyadické okruhy, viz [3].)

Definujme nyní jistou binární relaci „náležení" (mezi nezápornými prvky dyadického okruhu) takto:

$$(*) \qquad y \in^* x \Leftrightarrow \left[\frac{x}{2^y}\right] - 2\left[\frac{x}{2^{y+1}}\right] = 1\,.$$

Ukazuje se, že již v libovolném dyadickém okruhu splňuje tato relace náležení mnohé (ale obecně ne všechny) z axiomů teorie konečných množin.[3]) (V okruhu přirozených čísel máme $y \in^* x$ tehdy a jen tehdy, když číslo x psané v dvojkové soustavě má na y-tém místě jednotku; zde jsou splněny všechny axiomy teorie konečných množin.)

Přidejme ještě několik dalších axiomů tak, aby byly splněny pro relaci $\in^*$ všechny axiomy teorie konečných množin (nejprve pro množiny); tak máme tzv. *mt-(tj. množinově teoretický) dyadický okruh.* Abychom axiomy teorie konečných množin zaručili i pro (vlastní) třídy, musíme však doplnit tento okruh jistými „ideálními" elementy; dostaneme tak v nejjednodušším případě okruh tzv. celých Henselových p-adických čísel pro $p = 2$ (dyadická čísla, viz např. [13]). V obecnějším případě pak dostáváme jisté zobecnění těchto Henselových dyadických okruhů, tzv. *dyadický obal.* (Jak bylo již řečeno, autor zkonstruoval celou nespočetnou škálu takových okruhů a jejich obalů.) Ukazuje se ale, že i obráceně, máme-li libovolný „rozumný" model axiomatické teorie konečných množin, pak lze relaci náležení množiny do třídy modelu isomorfně jediným způsobem vystihnout ve vhodném obalu jistého dyadického *mt*-okruhu, ve smyslu shora vypsané definice (*) relace $\in^*$.

Je tedy v podstatě teorie konstrukce modelů axiomatické aritmetiky, ztotožňujeme-li ji s axiomatickou teorií konečných množin (čili nakonec s teorií dyadických *mt*-okruhů a jejich obalů), teorií rozšíření speciálních dyadických okruhů.

A nyní se ukazuje toto (a v tom je právě jádro nové algebraicko-logické metody, jež může usnadnit nalezení absolutně nerozhodnutelných vět aritmetiky):

Každé aritmetické větě se dá přiřadit vzájemně jednoznačně jistá rovnice o jedné neznámé, sestavená nad příslušným mt-dyadickým okruhem resp. jeho obalem (pomocí běžných aritmetických operací, ale včetně mocnění dvojky), *a to takto: Daná věta v modelu platí* (tj. je dokazatelná v axiomatické teorii množin, vzaté za základ) *tehdy a jen tehdy, když řečená rovnice má v uvažovaném dyadickém okruhu nezáporné řešení.*

---

[3]) Je míněn systém Gödel-Bernaysův jakožto dnes nejběžnější.

Můžeme tedy říci, že otázka absolutní nerozhodnutelnosti toho kterého problému teorie čísel je v tomto smyslu převedena v otázku řešitelnosti jisté rovnice o jedné neznámé nad obalem jistého dyadického okruhu. Jaké (a zda vůbec nějaké) ulehčení problému absolutně nerozhodnutelných vět teorie čísel tato jeho redukce dá, to se ovšem může ukázat teprve v průběhu dalšího zkoumání. K tomu bude asi zapotřebí spolupráce číselných teoretiků s pracovníky v matematické logice a algebře.

Pro větší zřetelnost shrňme takto:

1. Ukazuje se potřeba opustit přesvědčení o tzv. obsahové kategoričnosti aritmetiky přirozených čísel a zároveň potřeba rehabilitovat axiomatickou metodu zakládání aritmetiky. Je však třeba vycházet z daného konečného (dobře přehlédnutelného) počtu axiomů, což bude vyžadovat jiných primitivních pojmů, než je pojem následníka. Takovou axiomatickou základnou by mohla být Gödel-Bernaysova axiomatická teorie konečných množin vzhledem k autorovu výsledku o její ekvivalenci s axiomatickou teorií jistých dyadických okruhů (založených jen na primitivních pojmech sečítání, násobení a mocnění dvojky).

2. Na tomto základě se rýsuje akutní a exaktní pojetí problému obsahově (absolutně) nerozhodnutelných vět teorie čísel, jakož i redukce tohoto problému na jistý problém z teorie rovnic v dyadických okruzích.

DOPLNĚK

Aby nebylo nedorozumění, zdůrazněme a vysvětleme nakonec, že jsme pod pojmem aritmetika (teorie čísel) měli na mysli ryze matematickou teorii o hotových souhrnech tzv. přirozených čísel, jakožto o matematických objektech aritmetiky ve skutečnosti (ve více nebo méně konkrétní formě) existujících.

Vedle tohoto (po zpřesnění nutně axiomatického) pojetí aritmetiky je totiž možno nacházet, sestrojovat a rozebírat v přírodě probíhající a lidmi (resp. stroji) napodobované a neukončené procesy postupného tvoření přirozených čísel, které v nejjednodušším (základním) případě spočívají v neomezené reprodukci a v postupném přidávání stejného předmětu z téže „strany" (v časovém nebo v prostorovém smyslu), jako je např. neomezené přidávání svislé čárky ve stejné vzdálenosti vpravo, což se naznačuje zpravidla jako |, ||, |||, ||||, ... a bývá považováno za tzv. „intuitivní definici" přirozených čísel; ve složitějších případech pak běží o procesy na procesy takového základního druhu zákonitě redukovatelné, jako např. |, |||, |||||, |||||||, ... (čili 1, 3, 5, 7, ...) nebo ||, |, |||, ||, ||||, |||, |||||, ||||, ... (čili 2, 1, 3, 2, 4, 3, 5, 4, ...) a podobně, stále složitěji.

Ony tři tečky, naznačující zásadní neukončenost procesu takového či složitějšího druhu, které se rekurencemi, resp. operací minima převádějí na základní proces „vytváření přirozených čísel“, to je podstata tzv. konstruktivního čili intuitivního,[4] čili absolutního pojetí přirozených čísel resp. na něm budované *teorie obecně rekurentních „funkcí“*,[5] resp. tzv. *teorie algoritmů* (v podstatě jde o totéž). A právě z tohoto pojetí se rodí přesvědčení o kategoričnosti aritmetiky.

Jakkoli důležitá je tato matematická nauka (konstruktivní teorie čísel, teorie algoritmů apod.) už proto, že systematicky a exaktně zprostředkuje mezi axiomatickou aritmetikou (i jinými matematickými teoriemi) a mezi strojově početní praxí a aplikacemi, není to však podle autorova přesvědčení teoretická aritmetika ve vlastním slova smyslu a tím méně universální základ veškeré matematiky a logiky, jak se dosud domnívají někteří zastánci někdejšího Hilbertova programu. Teorii čísel a teorii algoritmů lze sice do jisté míry budovat nezávisle na axiomatické aritmetice způsobem tzv. ryze konstruktivně finitním (intuitivním), při čemž pojetí tohoto způsobu kolísá od autora k autoru. Avšak čím dále chceme proniknout za elementární číselně teoretické poznatky, tím větší jsou technické komplikace a logické obtíže, spočívající konec konců v intuitivním neaxiomatickém pojetí (pokud se ovšem vůbec snažíme je co možno vymezit a pak se ho důsledně a kriticky držet). S jedné strany se tak zdá být intuitivní pojetí aritmetiky (založené na představě neukončeného procesu vytváření přirozených čísel[6])) obdobné tzv. intuitivnímu pojetí klasické analysy opřenému o základní představu procesu spojitého neomezeného blížení.[7] Intuitivní pojetí klasické analysy není ovšem rovněž nikterak zbytečnou věcí a především přirozeně vládne v matematické fysice. Bylo by však podle autorova názoru krokem zpět, kdyby měla být na něm zakládána teoretická analysa. Něco podobného lze říci i o intuitivní aritmetice resp. o teorii algoritmů.

S druhé strany připomíná (svojí úlohou zprostředkující mezi matematickou teorií a aplikacemi matematiky) teorie algoritmů také tzv. praktickou geometrii, míníme-li tím nauku o způsobech přesného přímého proměřování, geometrického konstruování a zpodobňování v „praktickém“ trojrozměrném prostoru.

Tolik doplňkem k otázkám resp. nedorozuměním, jež by mohly na základě četby článku vzniknout a jež také, jak ukázaly některé diskuse, vznikly.

---

[4] Nikoli však nutně intuicionistického, to je něco poněkud jiného.

[5] V konstruktivním pojetí vlastně nejde o funkce v běžném množinovém smyslu slova, nýbrž o konstruktivní jednoznačné binární predikátové konstanty.

[6] Toto pojetí aritmetiky není nijak nové; v klasické formulaci pochází od L. Kroneckera.

[7] Toto pojetí analysy (na rozdíl od staršího pojetí „nekonečně malých veličin“) pochází od C. F. Gausse.

Literatura

[1] Die Hauptreferate des 8. Polnischen Mathematikerkongress von 6. bis. 12. September 1953 in Warschau; *Andrzej Mostowski* (u. Mitarbeiter). Der Gegenwärtige Stand der Grundlagenforschung in der Matematik. Deutscher Verlag der Wissenschaften Berlin, 1954.

[2] *Kurt Gödel:* Über formal unentscheidbere Sätze ..., Monatsh. f. Math. u. Phys. *38* (1931), 173—198.

[3] *Ladislav Rieger:* A contribution to Gödel's axiomatic set theory, II. Čech. mat. žurnal *9* (*84*), 1959, 1—49.

[4] *David Hilbert-Paul Bernays*: Grundlagen der Mathematik I, II, Springer, Wien 1934, 1939.

[5] *Kurt Gödel*: The consistency of the axiom of choice and of the generalized continuum hypothesis, Ann. of Math. Studies, Princeton 1940.

[6] *A. Mostowski*: Sentences Undecidable in Formalized Arithmetic, Studies in Logic, North-Holland Publishing Co, Amsterdam 1952.

[7] *Ladislav Rieger*: O některých základních otázkách matematické logiky, Časopis pro pěstování matematiky, *81* (1956), 342—351.

[8] *Gerhard Gentzen*: Die Widerspruchsfreiheit der reinen Zahlentheorie, Math. An. *112* (1936), 493—565.

[9] *Cm. K. Клини*, Уведенис в метаматику, Москва, Изд. ин. лит. 1957. (Překlad z angl. A. S. Jesenina — Vol' pina.)

[10] *Thoralf Skolem*: Über die Nichtcharacterisierbarkeit der Zahlenreihe ..., Fund. Math. *23* (1934), 150—161.

[11] *Kurt Gödel*: Recense práce [10], Zbl. f. Math. *7* (1934), 193—194.

[12] *Leonard Dickson*: History of the Theory of Numbers, Vol. I, Carnegie Inst., Washington 1919.

[13] *Bartel L.* v. d. *Waerden*: Moderne Algebra I, Aufl. Springer Berlin, 1939.

Резюме

ПРОБЛЕМА Т. Н. АБСОЛЮТНО НЕРАЗРЕШИМЫХ ВЫСКАЗЫВАНИЙ ТЕОРИИ ЧИСЕЛ

ЛАДИСЛАВ РИГЕР (Ladislav Rieger), Прага

Условимся называть теорией конечных множеств аксиоматическую теорию множеств Геделя-Бернайса, в которой аксиома бесконечности C1 заменяется ее отрицанием (т. н. аксиомой конечности).

Тогда под проблемой т. н. абсолютно неразрешимых высказываний теории чисел мы будем понимать следующую задачу:

Сконструировать в теории множеств Геделя-Бернайса две модели теории конечных множеств и найти высказывание о конечных множествах так, что в одной модели оно доказано, а в другой опровергнуто.

Эта формулировка вопроса оправдана одним (еще неопубликованным) результатом автора, согласно которому теория конечных множеств вполне равносильна аксиоматической теории т. н. расширенных диадических колец (см. [3]), которая, в свою очередь, создана автором как самостоятельная аксиоматизация теории целых p-адических чисел Гензеля (Hensel) для $p = 2$. (Заметим, что при этом ,,натуральные числа“ являются ,,множествами“ в то время как все остальные абстрактные целые 2-адические числа являются ,,соответственными классами“.)

Обсуждается значение этой трудной проблемы для нового понимания оснований теории чисел по аналогии с основаниями геометрии.

Сообщено также известное сведение проблемы к одному типу задач из теории показательных уравнений над расширенными диадическими кольцами.

Summary

THE PROBLEM OF THE SO-CALLED ABSOLUTELY UNDECIDABLE SENTENCES OF NUMBER THEORY

LADISLAV RIEGER, Praha

Let the term "theory of finite sets" mean the axiomatic set theory of Gödel-Bernays, where however the axiom C1 (of infinity) has been replaced by its negation (i. e., by the so-called axiom of finiteness). The problem in question is then as follows:

To find two models for the theory of finite sets (as constructed in the axiomatic set theory of Gödel-Bernays), and also a sentence concerning finite sets, in such a manner that the sentence is proved in one and disproved in the other model.

Such a formulation of the problem seems to be justified by a new result (to be published) of the author, according to which the theory of finite sets is equivalent to the theory of the so-called extended dyadic rings (see [3]); this latter theory consists of a new self-contained axiomatization of the notion of Hensel's p-adic integral numbers for $p = 2$. (Here abstract integers correspond to sets, and other abstract p-adic integral numbers correspond to proper classes.)

The present paper contains a discussion of various aspects of this very difficult problem; and especially that of the analogy between the axiomatic foundations of geometry and of arithmetic.

Mention is made of a reduction of the problem to a certain problem concerning the solubility of exponential equations over extended dyadic rings.