Předmluva: o logice 20. století

V L. Dostálová et. al., ed., *Kurt Gödel: úplnost a neúplnost*,

OPS Plzeň a ZČU Plzeň, 2015

Vítězslav Švejdar*†

Říjen 2013, s malými opravami znovu vysázeno v květnu 2017

1 Úvod

Vzrůstající přesnost ve vyjadřování v matematice, a to jak při formulování tvrzení, tak při jejich dokazování, byla ve 20. století silným podnětem pro rozvoj logiky. V souvislosti s tím si povšimněme tří důležitých okolností, o kterých můžeme také mluvit jako o zajímavých pozorováních nebo o dobrých nápadech.

Zaprvé, v matematických důkazech lze vypozorovat užití stále týchž logických kroků, nebo jinak řečeno, jsou v nich opakovaně aplikována *logická pravidla,* kterých je jen několik. Například víme-li současně, že pokud A, pak C, a pokud B, pak také C, a víme-li kromě toho, že A nebo B, můžeme právem usoudit, že C. Tomuto logickému kroku (pravidlu) říkáme *rozbor případů.* Domluvíme-li se, že symbol $\forall$ čteme „pro každé“, můžeme s jeho užitím formulovat druhý příklad logického pravidla, známého jako pravidlo *konkretizace* nebo pravidlo *specifikace*: když $\forall x A(x)$, pak $A(y)$. Vyjádřeno slovy, víme-li, že všechna individua (nějakého zkoumaného univerza) mají vlastnost A, můžeme usoudit, že naše individuum y, tj. to, o kterém právě mluvíme nebo se kterým potřebujeme pracovat, má vlastnost A. Pokud všechna přirozená čísla tvaru $60k + 47$ jsou prvočísla, pak i číslo 407, tj. číslo $60 \cdot 6 + 47$, je prvočíslo. To je příklad správného úsudku (logického kroku) učiněného podle pravidla konkretizace. Na jeho správnosti se nic nezmění, zjistíme-li (třeba později), že číslo 407 prvočíslem není.

*Tato *Předmluva* vznikla z podnětu Petra Vopěnky, který autora o její napsání požádal přibližně v roce 2009.

†Charles University in Praha, vitezslavdotsvejdaratcunidotcz, Palachovo nám. 2, 116 38 Praha 1, Czech Republic. http://www.cuni.cz/~svejdar/

Místo logická pravidla se také říká *pravidla (správného) usuzování* nebo *odvozovací pravidla.* V dalším si ukážeme několik konkrétních příkladů matematických důkazů a upozorníme na logické kroky, jež se v nich vyskytují.

Skutečnost, že logických pravidel bylo identifikováno pouze několik, vzbuzuje otázku, zda vůbec existují nějaká další. *Věta o úplnosti* tvrdí, že neexistují. Přesněji řečeno, *(logický) kalkulus* je definován jako soubor (seznam) logických pravidel. Věta o úplnosti tvrdí, že logický kalkulus lze zvolit tak, že aplikací pravidel do něj přijatých lze odvodit všechna (korektní) logická pravidla, a to včetně těch, která dosud nikdo ani neformuloval. Věta o úplnosti je důležitým výsledkem logického výzkumu. Je matematickou větou v tom smyslu, že je dokázána matematickými prostředky. Její význam ale přesahuje matematiku tak dalece, jak matematiku přesahuje logika. Logické usuzování se neomezuje pouze na matematiku, neexistuje nějaká zvláštní logika aplikovatelná pouze v matematice, pouze snad v matematice máme zajímavější a složitější příklady úsudků než v jiných oborech, a také matematika je na logice více závislá.

Důkaz věty o úplnosti je podán v článku Kurta Gödela z r. 1930, jehož překlad je v této knize na str. 54–73. Důkaz (takové nebo onaké varianty, či spíše několika variant) věty o úplnosti je dnes v každé pokročilejší knize o logice. Gödelovým důkazem se v této Předmluvě podrobněji zabývat nebudeme, avšak poznamenejme, že je důležitý z nejméně dvou hledisek. Jednak z hlediska historického, neboť Gödel sice jako první publikoval přehledný důkaz, avšak je možné, že někteří logikové, možná T. Skolem, měli povědomí o platnosti věty o úplnosti ještě před Gödelovým článkem. Gödelův důkaz věty o úplnosti je zajímavý i z čistě technického hlediska, neboť je poměrně málo podobný důkazům, které jsou dnes oblíbené.

Zadruhé, kromě toho, že v matematických důkazech lze vysledovat použití stále týchž logických pravidel, která jsou společná pro všechna odvětví matematiky a též pro usuzování mimo matematiku, matematické důkazy lze také analyzovat z toho hlediska, jaké *matematické předpoklady,* či *mimologické předpoklady,* jsou v nich použity. Žádný matematický důkaz totiž není důkazem „z ničeho“, nýbrž vždy vlastně redukuje tvrzení, které se má dokázat, k jiným tvrzením, která jsou buď pokládána za zřejmá, nebo byla dokázána již dříve. Důkazy tvrzení dokázaných dříve lze ovšem dále logicky analyzovat a opět identifikovat matematické předpoklady, které v nich byly použity. Například prohlédneme-li si důkaz Pythagorovy věty, třeba v některé středoškolské učebnici, pravděpodobně v něm nalezneme použití předpokladu, že dva pravoúhlé trojúhelníky, které mají shodnou přeponu a shodné oba k ní přilehlé úhly, musí mít stejný obsah. A dále v něm asi bude použit předpoklad, že pro počítání s (reálnými) čísly platí distributivní zákon, tj. že pro každou trojici čísel a, b a c platí rovnost $a \cdot (b + c) = a \cdot b + a \cdot c$. Analyzujeme-li důkaz tvrzení, že přirozené číslo je dělitelné třemi, právě když jeho ciferný součet je dělitelný třemi, asi v něm nalezneme použití předpokladu, že pro každé přirozené číslo a existuje jednoznačně

určená dvojice čísel q, r taková, že $a = 3 \cdot q + r$ a přitom $r < 3$. Například pro číslo 37 máme $37 = 3 \cdot 12 + 1$, a je-li $q \neq 12$ *nebo* $r \neq 1$, a přitom $r < 3$, číslo $3 \cdot q + r$ je určitě něco jiného než 37. Tomuto předpokladu můžeme říkat věta o (existenci a jednoznačnosti) dělení třemi se zbytkem. Větu o dělení třemi se zbytkem se opět můžeme pokusit dokázat. Předtím ji ovšem můžeme zobecnit na větu o dělení libovolným nenulovým číslem se zbytkem, protože lze odhadnout, že to její důkaz již nezkomplikuje. Pokud ji pak opravdu dokážeme a svůj důkaz analyzujeme, mezi několika předpoklady v něm použitými pravděpodobně bude onen již náhodou zmíněný distributivní zákon.

Vyhledávání mimologických předpokladů použitých v důkazech, jejich třídění na ty, které jsou zřejmé, a na ty, které je třeba ještě dokázat, a jejich posuzování z hlediska, zda jsou užitečné ještě v dalších důkazech, můžeme označit jako *logickou analýzu*. Mohlo by se zdát, že nalezením důkazu nějakého tvrzení byl splněn určitý účel, totiž tvrzení, které dosud bylo jen hypotézou, překvalifikovat na „pravdu“, a sám důkaz onoho tvrzení už pak důležitý není a není důvod jej logicky analyzovat. Také by se mohlo zdát, že logická analýza je neperspektivní práce, protože zkoumání dalších a dalších důkazů, třeba i jen v jedné oblasti matematiky, pravděpodobně povede k vyhledání nepřehledného množství dalších a dalších mimologických předpokladů. A nadto, neexistuje žádné objektivní kritérium, které by dovolilo určit, zda daný předpoklad může být už považován za zřejmý. Ve skutečnosti se však ukazuje, a to je právě naše druhá důležitá okolnost či zajímavé pozorování, že logická analýza důkazů z určité oblasti matematiky, například aritmetiky přirozených čísel, teorie množin nebo geometrie, často *vede k nalezení přehledného souboru předpokladů*, se kterými pak již lze při hledání dalších důkazů v oné oblasti matematiky pravděpodobně vystačit.

Souboru předpokladů vypozorovaných z důkazů určité oblasti matematiky v naději, že s nimi bude možné vystačit i v dalších důkazech, se říká *axiomatická teorie*, předpokladům tvořícím axiomatickou teorii se pak říká *axiomy* (oné teorie). Například kdybychom chtěli rovinnou geometrii chápat jako axiomatickou teorii, jedním z axiomů by mohlo být tvrzení, že pokud dva různé body a a b leží současně na přímce p_1 i na přímce p_2, pak $p_1 = p_2$. Jinak řečeno, dva různé body jednoznačně určují přímku, která jimi prochází. Jako axiomy (axiomatické) aritmetiky přirozených čísel by mohla být přijata mimo jiné tvrzení, že jak sčítání, tak násobení jsou asociativní a komutativní operace a že pro ně platí distributivní zákon.

Axiomy axiomatické teorie nejen určují základní pravdy o zkoumaných objektech, ale určují také, o čem se v dané teorii může mluvit, tj. definují *jazyk teorie*. Například v rovinné geometrii lze mluvit o bodech a přímkách a o tom, že určité body leží na určitých přímkách neboli že určité přímky procházejí určitými body. V aritmetice přirozených čísel lze mluvit o součtech a součinech přirozených čísel a o tom, že některé číslo je menší než některé jiné. Axiomatická teorie může obecně být definována jako soubor (množina) předpokladů, obvyklejší ale je de-

finovat ji jako jazyk dohromady s množinou předpokladů formulovaných v onom jazyce. Místo axiomatická teorie se někdy také říká axiomatický *systém*.

Vyhledávání předpokladů, formulování axiomatických teorií a uvažování, zda v nových důkazech lze vystačit s dříve nalezenými axiomy, tedy to, co jsme před chvílí označili jako logickou analýzu, je důležitou součástí matematické práce. A to přestože v některých disciplínách, například v kombinatorice, se axiomatické teorie příliš neuplatňují. Důležitost axiomatických teorií a axiomatického myšlení zvyšuje také fakt, že některé axiomatické teorie v jistém (neformálním a neexaktním) smyslu obsahují všechny ostatní. V Gödelově článku z r. 1931, v této knize na str. 75–119, jsou zmíněny dvě takové *univerzální teorie:* teorie typů uvedená v díle Principia Mathematica a teorie množin. *Teorie typů* dnes mezi matematiky populární není, má význam hlavně historický a filosofický. Avšak *teorie množin* je živou a zkoumanou disciplínou. Je dnes světem matematiky v tom smyslu, že o veškeré matematice si lze myslet, že se děje v teorii množin. Všechny známé matematické důkazy, kdyby byly napsány dostatečně podrobně, by bylo možno redukovat k jejím axiomům a s těmito axiomy by se v důkazech dalo vystačit. To pokládáme za skutečně pozoruhodné: všechny matematické poznatky jsou vlastně důsledkem axiomů, kterých je, podle konkrétní varianty teorie množin, například pouze osm nebo čtrnáct.

Vyřešit nějaký matematický problém obvykle znamená zjistit, zda nějaké tvrzení A platí, nebo naopak platí jeho negace. Negace tvrzení A se značí $\neg A$ a čte se „non A“ nebo „ne A“. Předchozí výklad měl naznačit, že v mnohých matematických oblastech si řešení takového problému lze představit jako nalezení důkazu jednoho z tvrzení A nebo $\neg A$ v nějaké axiomatické teorii T, která je v daném kontextu pokládána za adekvátní. Je-li v teorii T dokazatelná negace $\neg A$ tvrzení A, říkáme, že tvrzení A je v teorii T *vyvratitelné*.

Pokud je zaručeno, že každé tvrzení A je v T dokazatelné nebo vyvratitelné, avšak nikoliv současně dokazatelné a vyvratitelné, říkáme, že teorie T je *úplná*. Pojem úplnosti axiomatické teorie má jiný význam než pojem úplnosti logického kalkulu, který vystupuje ve větě o úplnosti a o kterém byla řeč na začátku této Předmluvy. Úplnost je důležitá vlastnost axiomatické teorie. Dokazatelnost v úplné teorii odpovídá intuitivní představě, že každé tvrzení je pravdivé nebo nepravdivé, a je-li nepravdivé, znamená to, že pravdivá je jeho negace. V dalším podáme příklad úplné axiomatické teorie. Lze si snadno představit, že teorie T úplná není, například protože její axiomy byly formulovány nesprávně nebo jsou příliš slabé. Pokud teorie T úplná není, znamená to, že existuje nějaké tvrzení, které je v T současně dokazatelné i vyvratitelné, nebo existuje tvrzení, které není dokazatelné ani vyvratitelné. V prvním případě říkáme, že teorie T je *sporná*. Sporná teorie je nezajímavá, neboť lze ověřit, že kromě oněch dvou tvrzení A a $\neg A$, jež jsou současně dokazatelná a reprezentují spor, lze v T dokázat *každé* tvrzení B. Spor ve sporné teorii tedy nemůže být reprezentován pouze jedním nebo pouze některými tvrzeními.

Je-li teorie T neúplná a přitom není sporná, tj. je *bezesporná*, existuje tvrzení A, které není v T dokazatelné ani vyvratitelné. O takovém tvrzení říkáme, že je na T *nezávislé*. V Gödelově článku se říká *nerozhodnutelné*, tento termín ale dnes užíváme pro něco jiného, totiž pro algoritmickou nerozhodnutelnost. Příklad teorie, která je bezesporná a přitom neúplná, lze získat odstraněním některých axiomů z úplné teorie, nebo ještě jednodušeji tak, že pro teorii definujeme její jazyk, avšak nepřidělíme jí žádné axiomy.

Tím jsme stručně popsali situaci v logice krátce před rokem 1931 a dostali jsme se k zajímavému pozorování, v tomto případě spíše k velmi dobrému nápadu, který chceme zmínit *zatřetí*. Je pravda, že odstraněním axiomu z úplné teorie vznikne teorie neúplná, avšak nemusí být automaticky pravda, že z neúplné bezesporné teorie lze získat úplnou teorii přidáním jednoho nebo několika axiomů. A skutečně, První Gödelova věta o neúplnosti, dokázaná v slavném článku z roku 1931, jehož překlad je v této knize nabídnut, tvrdí, že *každá dostatečně silná axiomatická teorie s jednoduchou množinou axiomů je neúplná.*

Podmínka, že T má jednoduchou množinu axiomů, přesněji znamená to, že existuje algoritmus, který je schopen o daném tvrzení na základě jeho symbolického zápisu rozhodnout, je-li axiomem teorie T. Tato podmínka je splněna mimo jiné vždy tehdy, když množina všech axiomů teorie T je jen konečná. Druhou podmínku, že teorie T je dostatečně silná, nelze jednoduše popsat přesněji. Pouze poznamenejme, že se týká jak axiomů, tak jazyka teorie T, který musí mít určitou vyjadřovací sílu. A dále poznamenejme, že tuto podmínku splňují všechny varianty teorie množin a jejich i velmi slabé podteorie a že ji splňují i různé aritmetiky přirozených čísel, pokud jsou formulovány v jazyce obsahujícím symboly pro sčítání i násobení. Je naproti tomu známo, že v jazyce obsahujícím pouze sčítání a nikoliv násobení lze formulovat axiomatickou teorii, která je úplná. Této teorii se říká Presburgerova aritmetika a je to příklad teorie, na kterou se První Gödelova věta nevztahuje, neboť jazyk neobsahující symbol pro násobení dostatečnou vyjadřovací sílu nemá. Lze shrnout, že Gödelova věta se vztahuje na velmi mnoho teorií, na „všechny rozumné“, její dvě podmínky nejsou zvlášť omezující.

O První Gödelově větě, na rozdíl od věty o úplnosti, nelze spekulovat, že byla známa již před oficiální publikací, to určitě nebyla. A nelze ani tvrdit, že byla okamžitě přijata a pochopena. To souvisí s jejím poněkud paradoxním zněním: každá dostatečně silná teorie je vlastně slabá v tom smyslu, že z ní bez porušení bezespornosti můžeme přidáním axiomů vytvořit silnější teorii. Je-li totiž T teorie, na kterou se První Gödelova věta vztahuje, a je-li A nezávislé tvrzení, které tudíž musí existovat, teorii T můžeme zesílit jak přidáním A, tak jeho negace $\neg A$ jako nového axiomu. Přitom je jasné, že přidáním jednoho axiomu vznikne z T teorie, která je dostatečně silná a má jednoduchou množinu axiomů, takže Gödelova věta se na ni vztahuje také (tady bychom správně měli mluvit o určitém zesílení Gödelovy věty známém jako *Rosserova věta*, tato nepřesnost ale nic ne-

mění na vyznění textu). Takže přidáním nového axiomu nevznikne úplná teorie. Gödelova věta nás tak nutí změnit pohled na neúplnost. Zatímco před rokem 1931 bylo možné neúplnost chápat jako chybějící axiomy a neúplnou teorii jako polotovar, ze kterého se úplná teorie stane, až chybějící axiomy budou nalezeny, z Gödelovy věty vidíme, že mnohé teorie jsou *nezúplnitelné*, a tyto teorie není třeba zvlášť hledat, v matematické praxi se běžně vyskytují. Nezúplnitelné jsou všechny používané varianty teorie množin, všechny další „univerzální“ teorie včetně těch, které teprve vzniknou nebo naopak už vyšly z módy jako například teorie typů, mnohé i celkem slabé fragmenty těchto teorií, a také mnohé teorie, které v žádném případě univerzální nejsou, neboť se vztahují jen k určité oblasti matematiky.

V dalším si podrobněji vysvětlíme některé aspekty Gödelova důkazu jeho přelomové věty. Gödelova věta je podstatným výsledkem moderní logiky a nic na tom nemění to, že dnes jsou známy i její jiné a názornější důkazy a že terminologie se dnes používá trochu jinak. Vysvětlili jsme si, že „formálně nerozhodnutelná“ v titulu Gödelova článku je lépe číst jako *nezávislá*, místo „věta“ by se dnes spíš řeklo tvrzení nebo *sentence*, protože „věta“ se obvykle chápe jako dokazatelné tvrzení, a místo „Principia Mathematica“ by mohlo stát *každá rozumná teorie*.

2 Peanova aritmetika

V minulém oddílu jsme si udělali představu, že v matematické praxi se uplatňují axiomatické teorie, že axiomatická teorie může vzniknout analýzou důkazů v určité oblasti matematiky, například v geometrii nebo v aritmetice přirozených čísel, že pojem axiomatické teorie je velmi důležitý v logice a zkoumání vlastností axiomatických teorií je poměrně obsáhlou součástí logického výzkumu a že Gödelova věta (První Gödelova věta o neúplnosti) tvrdí, že mnohé axiomatické teorie, (skoro) všechny rozumné, jsou neúplné. Připomeňme k tomu, že axiomatická teorie je dána jazykem a množinou axiomů a že úplná teorie je taková, v níž je každé tvrzení dokazatelné nebo vyvratitelné, avšak nikoliv současně dokazatelné a vyvratitelné.

Vzhledem k tomu, že Gödelova věta je poněkud abstraktním poznatkem, a přitom ji chceme přiblížit i čtenáři, který se matematikou hlouběji nezabýval, a nemá tudíž zkušenost s matematickými důkazy, ukážeme v tomto oddílu několik důkazů, a to z aritmetiky přirozených čísel. Většinou nebudou složité, avšak budeme schopni je napsat tak podrobně, abychom si byli jisti všemi předpoklady, které se v nich použijí. Tím zároveň podáme příklad logické analýzy a ukážeme, jak lze dospět k jedné konkrétní axiomatické teorii, Peanově aritmetice. Ta je zajímavá a důležitá tím, že je poměrně silná: bez znalosti První Gödelovy věty by bylo velmi obtížné zdůvodnit, že je neúplná. Volbou příkladů důkazů a volbou Peanovy aritmetiky jako ukázkové axiomatické teorie se nám snad podaří také

dokumentovat tezi, že výsledkem analýzy důkazů z určité oblasti matematiky je často přehledná axiomatická teorie, s jejímiž axiomy jako předpoklady lze vystačit v mnoha dalších důkazech. A že právě to je jedna z okolností, které z logiky dělají atraktivní disciplínu.

Peanova aritmetika je teorií přirozených čísel, přesněji řečeno jednou z více teorií přirozených čísel. Přirozená čísla jsou čísla nula, jedna, dvě, ..., tj. celá nezáporná čísla. K přirozeným číslům určitě chceme počítat i nulu bez ohledu na to, že ve středoškolské praxi se to někdy neděje. Víme již, že než začneme uvažovat o důkazech a axiomech nějaké teorie, musíme určit její jazyk. Tím bude určeno, jaká tvrzení lze v dané teorii utvářet neboli o čem lze v dané teorii mluvit. Nuže, v Peanově aritmetice lze mluvit o sčítání a násobení přirozených čísel, o jejich uspořádání a o dvou významných číslech nula a jedna. Konkrétněji, *jazyk* Peanovy aritmetiky (jazyk zde vykládané verze Peanovy aritmetiky) sestává z pětice symbolů. Jsou to symboly $+$ a $\cdot$ pro sčítání a násobení, symbol $<$ pro uspořádání a symboly 0 a 1 jako jména dvou významných čísel. Poznamenejme, že jménům význačných objektů se v logice říká *konstanty*.

Tvrdili jsme sice, že *axiomy* vypozorujeme z důkazů, mnohé axiomy ale vyjadřují natolik jednoduché skutečnosti, že je vyjmenujeme rovnou a nebudeme čekat, až si jejich zařazení na seznam axiomů vynutí nějaký ukázkový důkaz. Axiomy A1–A5 se týkají obou operací:

A1: $\forall x \forall y \forall z((x + y) + z = x + (y + z))$,

A2: $\forall x \forall y(x + y = y + x)$,

A3: $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$,

A4: $\forall x \forall y(x \cdot y = y \cdot x)$,

A5: $\forall x \forall y \forall z(x \cdot (y + z) = x \cdot y + x \cdot z)$.

Z předchozího oddílu víme, že význam symbolu $\forall$ je „pro každé“. Například axiom A2 můžeme číst „pro každá dvě čísla x a y platí, že $x + y$ je totéž číslo jako $y + x$“. Axiom A2 tak vyjadřuje tzv. komutativní zákon, tj. fakt, že při sčítání dvou čísel nezáleží na pořadí sčítanců. Axiom A4 vyjadřuje fakt, že i operace násobení je komutativní. Axiomy A1 a A3 vyjadřují asociativitu obou operací: máme-li sečíst nebo vynásobit tři čísla, můžeme si vybrat, v jakém pořadí provedeme dvě sčítání resp. dvě násobení. Axiom A5 mluví současně o sčítání a násobení a vyjadřuje distributivní zákon. O něm jsme se již zmínili v Úvodu.

Jednoduchým příkladem tvrzení, které je dokazatelné z dosud uvedených axiomů (je jejich důsledkem) je $\forall x \forall y \forall z \forall v((x \cdot v) \cdot (y \cdot z) = ((v \cdot x) \cdot y) \cdot z)$. Pokud s tím čtenář souhlasí, znamená to, že v duchu provedl jednoduchý důkaz v Peanově aritmetice, v němž pravděpodobně jednou použil axiom A4 a jednou axiom A3.

Axiomy A6 a A7 vyjadřují vlastnosti význačných čísel 0 a 1:

A6: $\forall x(x+0=x \ \& \ x\cdot 0=0)$,

A7: $\forall x(x\cdot 1=x)$.

V axiomu A6 je použit třetí (po $\forall$ a $\neg$ zmíněných v Úvodu) logický symbol $\&$, který čteme „a“ nebo „a současně“ nebo „a přitom“, případně latinsky „et“. Jednoduchými důsledky axiomu A6 jsou tvrzení $\forall x(x+0=x)$ a $\forall x(x\cdot 0=0)$, z nichž první vyjadřuje, že nula je *neutrálním objektem* operace sčítání. Axiom A7 tvrdí, že je číslo jedna je neutrálním objektem operace násobení.

Logických symbolů, které se mohou vyskytnout v našich symbolických zápisech, je celkem sedm. Význam symbolu $\vee$ je „nebo“. Zápis tvaru $A\vee B$ čteme „A nebo B“ nebo „A vel B“. Zápis tvaru $A\to B$ čteme „když A, pak B“. Symbolům $\&$, $\vee$, $\to$ říkáme konjunkce, disjunkce a implikace. Tyto termíny vztahujeme i na celá tvrzení, jejichž „nejvnějšnějším“ symbolem je $\&$, $\vee$, $\to$, a mluvíme tak například o implikaci $A\to B$. Tvrdit $A\to B$ je totéž jako tvrdit, že B vyplývá z A. Symbolům $\neg$, $\&$, $\vee$, $\to$ říkáme *logické spojky*, i když první z nich, negace, nic s ničím nespojuje (patří k pouze jednomu tvrzení). Pátou logickou spojkou je ekvivalence $\equiv$. Zápis $A\equiv B$ pokládáme za zkratku pro $(A\to B)\&(B\to A)$. Tvrdit $A\equiv B$ znamená tvrdit, že A a B znamenají totéž (jsou spolu ekvivalentní, každé z tvrzení A a B vyplývá z toho druhého). Posledním z našich logických symbolů je $\exists$, čteme jej „existuje“. Symbolům $\forall$ a $\exists$ říkáme *kvantifikátory*. Kdyby na to přišlo, vystačili bychom jen s jedním z nich, neboť tvrdit, že existuje x, které má vlastnost A, je totéž jako tvrdit, že není pravda, že pro každé x platí, že x nemá vlastnost A. Symbolicky zapsáno, z $\exists xA(x)$ vyplývá $\neg\forall x\neg A(x)$ a naopak. Také z $\forall xA(x)$ vyplývá $\neg\exists x\neg A(x)$ a naopak.

Než pokročíme k dalším axiomům Peanovy aritmetiky a pak k příkladům důkazů, zamysleme se nad vyjadřovacími možnostmi aritmetického jazyka neboli nad jeho expresívní silou. V aritmetickém jazyce máme symboly $+$, $\cdot$, $<$ a konstanty 0 a 1 pro dvě význačná čísla. Tento zdánlivě chudý jazyk ale stačí, abychom mohli mluvit i o mnoha dalších pojmech a vlastnostech a o dalších číslech. Například výraz $(1+1)+1$ označuje číslo tři a tak jej také můžeme číst. Zápis

$$\forall u\forall v(u\cdot v=(1+1)+1 \ \to \ u=1 \ \vee \ v=1) \tag{1}$$

říká, že v každé dvojici čísel, jejichž součin je tři, musí (alespoň) jeden člen dvojice být roven jedné. Jinak řečeno, tři není součinem dvou čísel, z nichž obě jsou různá od jedné, nebo ještě jinak řečeno, číslo tři je prvočíslo. Zápis

$$\forall u\forall v\exists z(z\neq u \ \& \ z\neq v), \tag{2}$$

který říká, že ke každé dvojici čísel existují čísla různá od obou členů oné dvojice, lze stručněji číst existují alespoň tři různá čísla.

Vidíme, že jazyk Peanovy aritmetiky umožňuje mluvit i o pojmech a skutečnostech, kterým v něm bezprostředně neodpovídají symboly, například o prvočíslech nebo o počtu existujících navzájem různých čísel. Právě tato vlastnost, bohaté vyjadřovací schopnosti jazyka ve smyslu rozšiřitelnosti o další pojmy, kterou se nepokoušíme přesně definovat, je podstatná pro axiomatické teorie, pro něž platí První Gödelova věta o neúplnosti. U tvrzení, která můžeme v aritmetickém jazyce zapsat, se můžeme ptát, zda je také můžeme dokázat. Dosud uvedených sedm axiomů ale nestačí k důkazu tvrzení, že tři je prvočíslo, ani k důkazu tvrzení, že dvě je prvočíslo, ani k důkazu tvrzení, že existují alespoň tři různá čísla. Lze dokázat tvrzení

$$((1+1)+1)\cdot(1+1) = ((((1+1)+1)+1)+1)+1, \tag{3}$$

které říká, že tři krát dvě je šest. K tomu stačí jednou použít axiomy A4 a A5, dvakrát A7 a pak několikrát A1. To ale nestačí k důkazu tvrzení, že šest není prvočíslo. Potřebovali bychom totiž vědět, že šest je součin dvou čísel různých od jedné. To ale nevíme, neboť z axiomů A1–A7 nelze dokázat $1+1 \neq 1$ ani $(1+1)+1 \neq 1$. K symbolu $\neq$ poznamenejme, že jej nepovažujeme za nový symbol: zápis $x \neq y$ znamená $\neg(x = y)$.

Shrňme a poněkud doplňme dosavadní poznatky o symbolických zápisech. Máme *logické symboly* $\neg$, $\rightarrow$, $\&$, $\vee$, $\equiv$, $\forall$, $\exists$. Ty se spolu s rovnítkem mohou používat v symbolických zápisech všech axiomatických teorií. Pak máme *mimologické symboly*, které dohromady tvoří jazyk určité teorie. Mimologické symboly Peanovy aritmetiky jsou $+$, $\cdot$, $<$, 0, 1. Některé symbolické zápisy, například $0 = 1$, nebo $0 < 1$, nebo zápis (1) uvedený výše, vyjadřují tvrzení (o přirozených číslech). Jiné symbolické zápisy vyjadřují vlastnosti čísel. Například

$$x \neq 1 \ \& \ \forall u \forall v (u \cdot v = x \ \rightarrow \ u = 1 \ \vee \ v = 1) \tag{4}$$

vyjadřuje, že (nespecifikované) číslo x je prvočíslo. Zápis $\exists v((1+1)\cdot v = x)$ vyjadřuje, že číslo x je dvojnásobkem určitého čísla, tj. že číslo x je sudé. Některé vlastnosti jsou vlastnostmi nikoliv jednotlivých čísel, ale vlastnostmi dvojic (nebo trojic, ...), například $x < y$. V tom případě mluvíme spíše o *podmínkách* než o vlastnostech. Místo symbolických zápisů často používáme jejich neformální čtení zapsaná bezpatkovým písmem (v elektronické verzi navíc vyznačená barevně). A naopak, za vyjádřením zapsaným bezpatkovým písmem, například číslo x je dělitelné třemi, si představujeme symbolický zápis, v tomto případě $\exists v(((1+1)+1)\cdot v = x)$. Jak symbolické, tak neformální zápisy mají své výhody i nevýhody. Zápisům podmínek, vlastností a tvrzení se v logice říká *formule*. Neobsahuje-li formule *volné proměnné*, tj. nemluví-li o nespecifikovaných číslech (nýbrž vyjadřuje tvrzení), říkáme jí *sentence*.

Čtenář si pravděpodobně dovede představit, že pojem formule má přesnou definici, takže správně zapsané formule lze od nic neříkajících (nesprávných)

zápisů odlišit *algoritmem*. To znamená, že formule lze počítačově zpracovávat. V Úvodu, v úvahách o odvozovacích pravidlech, bylo naznačeno, že formalizovat a počítačově zpracovávat lze celé důkazy. Formalizovanými důkazy zapsanými v určitém kalkulu se nezabýváme, avšak na použití některých odvozovacích pravidel příležitostně upozorníme. Možnost symbolického zapisování celých důkazů znamená, že všechny své neformální důkazy bychom vlastně také měli zapisovat bezpatkovým písmem. To ale dělat nebudeme. Poznamenejme, že i bez formálně zapisovaných důkazů lze po jisté zkušenosti snadno poznat, zda celý neformální důkaz je správný a úplný. Právě to chceme čtenáři v tomto oddílu přiblížit.

Dalších šest axiomů Peanovy aritmetiky mluví o vlastnostech uspořádání a o tom, jak uspořádání souvisí se sčítáním a násobením.

A8: $\forall x \forall y \forall z (x < y \ \& \ y < z \ \rightarrow \ x < z)$,

A9: $\forall x \neg (x < x)$,

A10: $\forall x \forall y (x < y \ \vee \ x = y \ \vee \ y < x)$,

A11: $\forall x \forall y \forall z (x < y \ \rightarrow \ x + z < y + z)$,

A12: $\forall x \forall y \forall z (x < y \ \& \ z \neq 0 \ \rightarrow \ x \cdot z < y \cdot z)$,

A13: $\forall x \forall y (x < y \ \rightarrow \ \exists z (x + z = y))$.

Axiom A8 vyjadřuje tzv. *tranzitivitu* uspořádání, axiom A9 vyjadřuje *antireflexivitu:* žádné číslo není menší než ono samo. K axiomu A12 je nutné poznamenat, že o konjunkci & a disjunkci $\vee$ předpokládáme, že mají „vyšší prioritu“ než implikace $\rightarrow$ a ekvivalence $\equiv$. Díky této úmluvě si můžeme dovolit psát $A \,\&\, B \rightarrow C$ místo $(A \ \& \ B) \rightarrow C$. Axiom A12 tedy tvrdí, že nerovnost zůstane zachována, vynásobíme-li výrazy na obou stranách týmž nenulovým číslem. Již jsme poznamenali, že zápis $z \neq 0$ je vlastně zkratka pro $\neg(z = 0)$. Axiom A10 vyjadřuje tzv. *trichotomii* (nebo *linearitu*) relace uspořádání: v každé dvojici různých čísel je některé z čísel menší než to druhé (čili obě čísla jsou srovnatelná).

Domluvme se, že $x \leq y$ je zkratka pro $x < y \ \vee \ x = y$. Bezprostředním důsledkem axiomu A10 je pak tvrzení $\forall x \forall y (x \leq y \ \vee \ y \leq x)$. Skutečně, když pro x a y platí $x < y$, pak podmínka $x \leq y$, tj. podmínka $x < y \ \vee \ x = y$ platí, protože v ní platí její levý člen. Když $x = y$, pak v podmínce $x < y \ \vee \ x = y$ platí pravý člen a opět máme $x \leq y$. Když pro x a y platí $y < x$, pak z analogických důvodů $y \leq x$, a když $x = y$, pak $x \leq y$ i $y \leq x$.

Další příklady dokazatelných tvrzení budeme číslovat a říkat jim lemmata nebo věty. Než se pustíme do formulace a důkazu Lemmatu 1, které se vztahuje k axiomu A10, zmiňme se ještě o významu disjunkce, která se v axiomu A10 (dvakrát) vyskytuje. Tvrdíme-li $A \vee B$, tvrdíme tím, že „A a ne B, nebo B a ne A, nebo současně A i B“. Disjunkci tedy chápeme v tzv. nevylučovacím smyslu, $A \vee B$ znamená, že platí *alespoň jedno* z tvrzení (alespoň jedna z podmínek) A a B. Podíváme-li se z tohoto hlediska na axiom A10, na první pohled není

vyloučené, že by některé (nebo všechny) z podmínek $x < y$, $x = y$ a $y < x$ mohly platit současně. Následující lemma ale tvrdí, že to vyloučené je.

Lemma 1 *Podmínky $x < y$, $x = y$ a $y < x$ se navzájem vylučují, tj. pro žádná dvě čísla nemohou kterékoliv dvě z těchto podmínek platit současně.*

Důkaz Tvrdit, že $x < y$ se vylučuje s $x = y$, je totéž jako tvrdit, že $x = y$ se vylučuje s $y < x$. V obou případech se tvrdí, že máme-li dvě stejná čísla, nemůže jedno z nich být menší než druhé. To je pravda: máme-li dvě stejná čísla, tj. máme-li *jediné* číslo, toto číslo nemůže být menší než ono samo, protože to vylučuje axiom A9.

Zbývá zdůvodnit, že současná platnost první a třetí podmínky je vyloučená, tj. že v žádné dvojici čísel nemůže být jedno menší než druhé a současně druhé menší než první. Představme si tedy, že v nějaké dvojici čísel je jedno menší než druhé a současně druhé menší než první. Označme tato čísla u a v. Máme tedy $u < v$ a $v < u$. Aplikujme axiom A8 na $x = u$, $y = v$ a $z = u$: z $u < v$ a $v < u$ máme $u < u$. To je opět situace vyloučená axiomem A9. ⊣

K důkazu Lemmatu 1 poznamenejme, že jiné axiomy než A8 a A9 jsme v něm nepotřebovali. Následující lemma lze označit jako lemma o krácení a rušení.

Lemma 2 *Rovnost i nerovnost zůstane zachována, zrušíme-li (odečteme-li) na obou stranách totéž číslo nebo vykrátíme-li na obou stranách týmž nenulovým číslem:*
(a) $\forall x \forall y \forall z (x + z = y + z \rightarrow x = y)$,
(b) $\forall x \forall y \forall z (x + z < y + z \rightarrow x < y)$,
(c) $\forall x \forall y \forall z (x \cdot z = y \cdot z \ \& \ z \neq 0 \rightarrow x = y)$,
(d) $\forall x \forall y \forall z (x \cdot z < y \cdot z \rightarrow z \neq 0 \ \& \ x < y)$,
(e) $\forall x \forall y (x \cdot y = 0 \rightarrow x = 0 \vee y = 0)$.

Důkaz Uvažujme čísla x, y a z taková, že $x + z = y + z$ a předpokládejme, že přitom neplatí $x = y$. Podle axiomu A10 pak platí $x < y$ nebo $y < x$. Rozeberme první možnost, druhá je analogická. Když $x < y$, pak axiom A11 dává $x + y < y + z$. To ale není možné vzhledem k Lemmatu 1: platí-li $x + z = y + z$, nemůže současně platit $x + y < y + z$.

Důkaz tvrzení (b) je podobný. Platí-li $x + z < y + z$ a neplatilo-li by $x < y$, dle axiomu A10 by muselo platit $x = y$ nebo $y < x$. V prvním případě $x + z = y + z$, v druhém axiom A11 dává $y + z < x + z$. Obě možnosti jsou ale vzhledem k předpokladu $x + z < y + z$ a Lemmatu 1 vyloučené.

Důkazy tvrzení (c) a (d) jsou podobné, místo axiomu A11 se použije axiom A12. Je ale důležité upozornit na rozdíl ve formulaci obou tvrzení. V (d) se tvrdí o něco více, než že z $x \cdot z < y \cdot z$ a $z \neq 0$ plyne $x < y$. Když $x \cdot z < y \cdot z$, pak z

musí být nenulové, neboť kdyby $z = 0$, pak obě čísla $x \cdot z$ a $y \cdot z$ by se rovnala nule dle axiomu A6, tedy by nemohlo platit $x \cdot z < y \cdot z$.

V (e) předpokládejme, že $x \cdot y = 0$ a přitom $x \neq 0$ a $y \neq 0$. Pak $0 < x$ nebo $x < 0$. V prvním případě axiom A12 dává $0 \cdot y < x \cdot y$, tedy $0 < x \cdot y$. To je vzhledem k $x \cdot y = 0$ a Lemmatu 1 (nebo axiomu A9) vyloučené. Úvaha v druhém případě, kdy $y \neq 0$, je analogická. ⊣

Lemma 3 *Když $x < y$, pak existuje jednoznačně určené z takové, že $x + z = y$.*

Důkaz Předpokládejme, že dvě čísla z_1 a z_2, o kterých zatím netvrdíme, zda si jsou nebo nejsou rovna, splňují podmínky $x + z_1 = y$ a $x + z_2 = y$. Z toho máme $x + z_1 = x + z_2$ a Lemma 2(a) dává $z_1 = z_2$. Čísla z_1 a z_2 si tedy rovna jsou. ⊣

Upozorněme ještě jednou na určité logické kroky, které se vyskytují v našich důkazech. Děláme to již naposled, a to jednak proto, že logickými kroky se již nebudeme chtít zabývat, ale také proto, že po tomto upozornění budou logické kroky už víceméně vyčerpány.

Důkaz daného tvrzení B z předpokladů $A_1, \ldots, A_n$ může mít ten tvar, že zdůvodníme, že kdyby B neplatilo, tj. pokud by platilo $\neg B$, mělo by to nějaký absurdní důsledek. Takovému uvažování se říká *důkaz sporem*, neboť za absurdní důsledek neboli spor se pokládá současná platnost nějakého tvrzení a jeho negace. Důkaz sporem tedy vypadá tak, že máme-li dokázat B z předpokladů $A_1, \ldots, A_n$, dokážeme místo toho nějaká jiná tvrzení D a $\neg D$ z předpokladů $A_1, \ldots, A_n, \neg B$. Přitom D může pro potřeby důkazu být zvoleno libovolně, například D nebo $\neg D$ může být jedním z předpokladů $A_1, \ldots, A_n, \neg B$. Důkaz sporem jsme použili již několikrát, například na začátku důkazu Lemmatu 2 jsme odvodili spor ze současné platnosti předpokladů $x + z = y + z$ a $x \neq y$, a usoudili jsme pak, že tudíž z $x + z = y + z$ plyne $x = y$.

Jednodušší případ je ten, kdy máme jen jeden předpoklad A, máme dokázat B, a místo toho z $\neg B$ dokážeme $\neg A$. To je vlastně také důkaz sporem, neboť z předpokladů A a $\neg B$ plyne spor A a $\neg A$. Tomuto jednodušššímu případu důkazu sporem se říká postup *kontrapozicí*, neboť implikaci $\neg B \to \neg A$ se říká kontrapozice (česky *obměna*) implikace $A \to B$. Důkaz Lemmatu 3 by mohl také vypadat takto:

> Předpokládejme, že pro dvě čísla z_1 a z_2 platí $x + z_1 = x + z_2$ *a přitom* $z_1 \neq z_2$. Pak Lemma 2(a) dává $z_1 = z_2$, což je ve sporu se $z_1 \neq z_2$.

Pak by to byl důkaz sporem. Náš důkaz Lemmatu 3 ale usuzování sporem čili obměnou nepoužil, vystačili jsme s přímým důkazem.

V důkazu Lemmatu 3 je ale použit ještě jeden důležitý logický krok skrytý za slovy „předpokládejme, že čísla . . . “. Kdybychom tvrzení Lemmatu 3 zapsali symbolicky, vypadalo by takto:

$$\forall x \forall y \forall z_1 \forall z_2 (x + z_1 = x + z_2 \ \to \ z_1 = z_2).$$

Důkaz takovéhoto tvrzení s univerzálními kvantifikátory na začátku, tj. tvrzení tvaru $\forall x_1 \,..\, \forall x_k B(x_1,..,x_k)$, obvykle v matematické literatuře začíná slovy „nechť objekty $x_1,..,x_k$ jsou dány, pak ...“ a směřuje k závěru „takže pro $x_1,..,x_k$ platí $B(x_1,..,x_k)$“. Tomuto logickému kroku říkáme *generalizace*: nejprve pro blíže neurčené objekty $x_1,..,x_k$ zdůvodníme, že splňují podmínku $B(x_1,..,x_k)$, a pak usoudíme, že protože $x_1,..,x_k$ byly blíže neurčené, *všechny* k-tice $x_1,..,x_k$ splňují $B(x_1,..,x_k)$. Obecně generalizace vypadá tak, že dokážeme-li $B(x_1,..,x_k)$ z předpokladu A, tj. dokážeme-li implikaci $A \to B(x_1,..,x_k)$, a v předpokladu A se nic nepraví o $x_1,..,x_k$, máme právo usoudit implikaci $A \to \forall x_1 \,..\, \forall x_k B(x_1,..,x_k)$. Přitom „nic se nepraví“ má týž význam, jako když jsme před chvílí řekli „blíže neurčená“. Důkaz generalizací si lze představit jako hru, v níž na začátku je na tahu protihráč, jehož první a jediný tah spočívá ve volbě objektů $x_1,..,x_k$. Protihráč se ovšem snaží zvolit nějaké zapeklité objekty $x_1,..,x_k$. Pak následuje *náš* tah, ve kterém se máme snažit zdůvodnit, že pro protihráčem zvolené $x_1,..,x_k$ platí implikace $A \to B(x_1,..,x_k)$. Účelem této představy hry, v níž každý ze dvou hráčů má jen jeden tah a první táhne protihráč, je vysvětlit a opět zdůraznit význam obratu „blíže neurčené objekty“.

V našich úvahách jsme generalizaci použili již vícekrát. Například už tehdy, když jsme tvrdili, že jednoduchým důsledkem axiomu A6 je tvrzení $\forall x(x \cdot 0 = 0)$. To jsme vlastně provedli takovouto úvahu:

> Nechť x je (protihráčem) dáno. Pro toto, námi nezvolené čili blíže neurčené, avšak nám teď už viditelné x, axiom A6 dává $x + 0 = x$ a $x \cdot 0 = 0$. Tedy $x \cdot 0 = 0$.

K tomu poznamenejme, že (naše) aplikace axiomu A6 na (protiháčem zvolené) x je použitím pravidla specifikace, o kterém jsme se zmínili hned v druhém odstavci Úvodu. A ke generalizaci ještě poznamenejme, že má i symetrickou formu pro existenční kvantifikátor: zdůvodníme-li platnost implikace $B(x_1,..,x_k) \to A$ a v A se nic nepraví o $x_1,..,x_k$, je korektní usoudit i $\exists x_1 \,..\, \exists x_k B(x_1,..,x_k) \to A$.

Vraťme se k úvahám o volbě vhodných, správných a užitečných axiomů Peanovy aritmetiky. Po vyjmenování prvních sedmi axiomů A1–A7 jsme zmínili tři tvrzení, dvě označená čísly (1) a (2) a třetí „šest je prvočíslo“, která z axiomů A1–A7 dokázat nelze. Pokud si jejich dokazatelnost přejeme, a to si přejeme, bylo nutné přidat další axiomy. Nyní jsme v situaci, kdy máme axiomy A1–A13, dokazatelnost těch tří tvrzení si stále přejeme, ona ale ani teď dokazatelná nejsou. Zdůvodnění, že opravdu nejsou, by vyžadovalo určité další znalosti logiky. Avšak dá se mu snad věřit vzhledem k tomu, že v našich axiomech se toho zatím dost málo tvrdí o číslu 1 a o poloze čísel 0 a 1 vůči uspořádání. Přidejme tedy ještě tyto axiomy:

A14: $\quad 0 \neq 1 \;\&\; \forall x(0 < x \;\to\; 1 \leq x)$,

A15: $\quad \forall x(0 \leq x)$.

Jednoduchým důsledkem první části axiomu A14 je sentence $\forall x(x+1 \neq x)$: stačí Lemma 2(a) aplikovat na rovnost $x+1 = x+0$. Ke druhé části axiomu A14 a k axiomu A15 pro jistotu připomeňme, že $y \leq x$ je zkratka pro $y < x \ \vee \ y = x$. Teď už tedy víme, tj. z axiomů A1–A15 plyne, že nula je nejmenší ze všech čísel. Tedy i $0 \leq 1$. K tomu díky první části axiomu A14 můžeme dodat $0 < 1$. A druhá část axiomu A14 k tomu ještě dodává, že mezi čísly nula a jedna není nic, tj. že jedna je nejmenším nenulovým číslem.

Z $0 < 1$ a axiomu A11 máme $0+1 < 1+1$, tj. $1 < 1+1$. Axiom A8 dává $0 < 1+1$ a z Lemmatu 1 máme $0 \neq 1+1$. Tím je dokázáno tvrzení nula, jedna a dvě jsou navzájem různá čísla. Jeho důsledkem je tvrzení existují tři navzájem různá čísla, které lze symbolicky zapsat jako

$$\exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \ \& \ x_1 \neq x_3 \ \& \ x_2 \neq x_3)$$

nebo ekvivalentně zápisem (2) uvedeným výše. V těchto úvahách lze ovšech pokračovat a dokázat, že tři je větší než (a tudíž různé od) nula, jedna i dva, pak že číslo čtyři je větší než nula, jedna, dva i tři, a tak dále. Takže existují i čtyři navzájem různá čísla, a také existuje pět navzájem různých čísel, a tak dále.

Víme-li již, že $(1+1)+1 \neq 1$ a $1+1 \neq 1$, můžeme dokončit i dříve započatou úvahu o čísle šest: ne, šest není prvočíslo.

Uvažujme nyní nějaké (protihráčem zadané) číslo x různé od 0 i od 1. Předpoklad $x \neq 0$ a axiomy A15 a A14 dávají $1 \leq x$. K tomu předpoklad $x \neq 1$ dává $1 < x$. Aplikace axiomu A13 na čísla 1 a x dává číslo z takové, že $1+z = x$. Z Lemmatu 3 víme, že existuje jen jedno takové z. To teď ale důležité není, o „tom svém“ z bychom mohli uvažovat, i kdyby jich bylo více. Pro naše z platí $z \neq 0$, protože $1+0 = 1$, ale $x \neq 1$. Axiom A14 dává $1 \leq z$. Z toho, použitím axiomu A11, máme $1+1 \leq 1+z$, tedy $1+1 \leq x$. Tím jsme dokázali, že každé číslo x (každé, neboť x bylo zadáno protihráčem), které je různé od nuly i jedné, je alespoň $1+1$, symbolicky

$$\forall x(x \neq 0 \ \& \ x \neq 1 \ \rightarrow \ 1+1 \leq x).$$

Jinými slovy, k vědomosti, že $1+1$ je jiné číslo než 1 i než 0, se nám podařilo dodat, že dvě je nejmenší z čísel různých od nuly a jedné. Podobně, pokračováním analogických úvah, bychom také mohli dokázat, že tři je nejmenší z čísel různých od nuly, jedné a dvou, čtyři je nejmenší z čísel . . . , a tak dále. Zároveň jsme dokázali a použili tvrzení, že je-li x nenulové, existuje k němu jednoznačně určené z takové, že $x = z+1$.

Podívejme se nyní na tvrzení (1) výše. Uvažujme nějaká čísla u a v taková, že $u \cdot v = (1+1)+1$. Z dosavadních úvah a axiomu A6 je jasné, že $u \neq 0$ a $v \neq 0$. Chceme dospět k závěru, že $u = 1$ nebo $v = 1$. Postupujme sporem a předpokládejme $u \neq 1$ a $v \neq 1$. Protože víme, že $1+1$ je nejmenší z čísel různých od nuly a jedné, máme $1+1 \leq u$ a $1+1 \leq v$. Víme (je to důsledkem axiomu A12),

že vynásobíme-li obě strany neostré nerovnosti týmž číslem, nerovnost zůstane zachována. Vynásobme první nerovnost číslem $1+1$, druhou číslem u. To dá $(1+1)\cdot(1+1) \leq (1+1)\cdot u$ a $(1+1)\cdot u \leq u\cdot v$. Z toho plyne $((1+1)+1)+1 \leq u\cdot v$. Použijeme-li předpoklad $u\cdot v = (1+1)+1$, dospějeme k závěru, že čtyři je menší nebo rovno třem. To je ovšem ve sporu s naším poznatkem z předchozího odstavce, že čtyři je větší než (nula, jedna, dvě i) tři. Je tedy jasné, že tři je prvočíslo.

Podobně lze dokázat, že dvě je prvočíslo nebo že pět je prvočíslo. To je čtenáři přenecháno jako cvičení. Další zajímavé cvičení je dokázat, že prvočíselnost čísel dvě a tři lze dokázat bez užití axiomu A15. Tento axiom vlastně zakazuje záporná čísla. Lze ale ověřit, že i bez něj se nic nezmění na tom, že číslo tři ani číslo dvě není součinem dvou čísel různých od jedné.

Prohlédněme si nyní následující tvrzení (5), které pro nás bude příležitostí zamyslet se nad dalšími zajímavými důkazy a nad tím, zda s axiomy A1–A15 už hodláme vystačit:

$$\forall x \forall y (x \neq 0 \;\rightarrow\; y \cdot y \neq (1+1)\cdot x \cdot x). \tag{5}$$

Tvrzení (5) je zapsáno tak, aby se vystačilo se symboly, které máme v aritmetickém jazyce. O něco přehledněji by je ovšem šlo zapsat jako

$$\forall x \forall y (x \neq 0 \;\rightarrow\; y^2 \neq 2 \cdot x^2).$$

Tvrdí se, že pro žádné dvě druhé mocniny nenulových (ano, i y je nenulové, viz Lemma 1(e)) přirozených čísel se nemůže stát, aby jedna byla dvojnásobkem druhé. Přehlednějším zápisem tvrzení (5) jsme zároveň uzavřeli úmluvu, že místo $1+1$ budeme psát 2 a že místo $x\cdot x$ budeme psát x^2. Kdyby to bylo potřeba, místo $(1+1)+1$ bychom psali 3, a podobně. S použitím zlomků by tvrzení (5) šlo také zapsat jako $\neg\exists x \exists y (x \neq 0 \;\&\; (\frac{y}{x})^2 = 2)$, číslo dvě není druhou mocninou žádného zlomku, jehož čitatel i jmenovatel jsou přirozená čísla. Protože číslům, která se dají vyjádřit jako zlomek s celočíselným čitatelem a nenulovým celočíselným jmenovatelem, se říká *racionální*, a ostatním číslům se říká *iracionální*, tvrzení (5) lze vlastně číst druhá mocnina racionálního čísla se nikdy nerovná číslu dvě, nebo stručněji odmocnina ze dvou je iracionální číslo.

V důkazu tvrzení (5) budeme uvažovat o sudých a lichých číslech. Definujme tedy oba pojmy a dokažme o nich pomocná tvrzení, která pak budeme potřebovat v důkazu tvrzení (5), které oficiálně vyslovíme jako Větu 5. Naše definice zní takto: číslo x je *sudé*, jestliže existuje číslo v takové, že $x = 2\cdot v$, a číslo x je *liché*, jestliže existuje číslo v takové, že $x = 2\cdot v + 1$, přičemž stále používáme úmluvu, že 2 píšeme místo $1+1$. Z axiomu A6 víme, že $2\cdot 0 = 0$ a $2\cdot 0 + 1 = 1$, tedy nula je sudé a jedna je liché číslo. Z rovnosti (3) víme, že šest je sudé.

Lemma 4 *(a) Druhá mocnina libovolného sudého čísla je sudé číslo.*
(b) Druhá mocnina libovolného lichého čísla je liché číslo.

Důkaz Je-li x tvaru $2 \cdot v$, pak pro x^2 platí $x^2 = (2 \cdot v) \cdot (2 \cdot v) = 2 \cdot (v \cdot (2 \cdot v))$, tedy x^2 je dvojnásobkem určitého čísla, tedy x^2 je sudé. Je-li x tvaru $2 \cdot v + 1$, pak $x^2 = (2 \cdot v + 1) \cdot (2 \cdot v + 1) = 2 \cdot 2 \cdot v^2 + 2 \cdot v + 2 \cdot v + 1$, tedy $x^2 = 2 \cdot (2 \cdot v^2 + 2 \cdot v) + 1$, tedy x^2 je liché. ⊣

Protože důkaz Věty 5 chceme udržet jasný a stručný, proveďme určité předběžné úvahy. V důkazu se postupuje sporem neboli uvažuje se, co by se stalo, kdybychom měli čísla x a y taková, že $y^2 = 2 \cdot x^2$ a přitom $x \neq 0$. První krok důkazu je, že kdybychom taková x a y měli, tj. měli bychom zlomek $\frac{y}{x}$, jehož druhá mocnina je dvě, měli bychom také *nevykratitelný* zlomek, jehož druhá mocnina je dvě. Kdyby například pro $x = 5\,000$ a $y = 7\,072$ platilo $y^2 = 2 \cdot x^2$, pak by $y^2 = 2 \cdot x^2$ muselo platit i pro $x = 625$ a $y = 884$, neboť zlomky $\frac{7\,072}{5\,000}$ a $\frac{884}{625}$ se rovnají, druhý lze z prvního získat vykrácením osmi a přitom druhý již žádné krácení nepřipouští. Mohli bychom to také vyjádřit beze zlomků čili s přesvědčivějším použitím aritmetického jazyka a s odkazem k axiomům: z rovnosti $7\,072^2 = 2 \cdot 5\,000^2$ dostaneme rovnost $884^2 = 2 \cdot 625^2$, použijeme-li několikrát axiom A3 a pak Lemma 2(c) dvakrát na totéž $z = 8$, kdežto z rovnosti $884^2 = 2 \cdot 625^2$ dostaneme (což ale nepotřebujeme) rovnost $7\,072^2 = 2 \cdot 5\,000^2$ dvojnásobným užitím axiomu A12 a také několikerým užitím axiomu A3. Jestliže zlomek $\frac{884}{625}$ již dále krátit nelze, číslo 625 je nejmenším nenulovým číslem x, pro které existuje y takové, že $y^2 = 2 \cdot x^2$. To vše za předpokladu, že $7\,072^2 = 2 \cdot 5\,000^2$ (jehož platnost z pochopitelných důvodů raději nezkoumáme).

Věta 5 *Pro žádná dvě čísla y a $x \neq 0$ neplatí $y^2 = 2 \cdot x^2$.*

Důkaz Postupujme sporem a předpokládejme, že máme čísla x a y taková, že $x \neq 0$, a přitom $y^2 = 2 \cdot x^2$. V tom případě můžeme navíc předpokládat, že x je nejmenší nenulové číslo, k němuž existuje y takové, že $y^2 = 2 \cdot x^2$. Číslo y^2 je evidentně sudé. To podle Lemmatu 4(b) znamená, že i y je sudé. Existuje tedy číslo v takové, že $y = 2 \cdot v$. Máme tedy $(2 \cdot v)^2 = 2 \cdot x^2$, tedy $2 \cdot 2 \cdot v^2 = 2 \cdot x^2$. Lemma 2(c) dává $2 \cdot v^2 = x^2$. Z toho je jasné, že $v \neq 0$ a $v < x$. Tím jsme dospěli ke sporu s předpokladem, že x je nejmenší nenulové číslo, ke kterému existuje y tak, aby platilo $y^2 = 2 \cdot x^2$: číslo v je ještě menší než x a přitom pro ně a x platí $x^2 = 2 \cdot v^2$. ⊣

Zhruba v tomto tvaru by se důkaz Věty 5 mohl vyskytnout v některé učebnici matematiky. Zde jej ale chceme analyzovat z logického hlediska a posoudit, zda v jednotlivých krocích vystačíme s axiomy, které zatím máme. Například lze snadno ověřit, že kroky „když $2 \cdot v^2 = x^2$ a $x \neq 0$, pak $v \neq 0$“ a „když $2 \cdot v^2 = x^2$ a $v \neq 0$, pak $v < x$“ jsou korektní, lze je napsat podrobněji, poukázat na použití axiomů a potvrdit, že s axiomy A1–A15 v nich lze vystačit. Problematický je ale krok „když y^2 je sudé, pak to dle Lemmatu 4(b) znamená, že i y je sudé.“ Tento krok bychom podrobněji mohli zapsat takto: „předpokládejme, že y^2 je sudé, ale

y sudé není; pak y je liché; dle Lemmatu 4(b) i y^2 je liché, a to je spor.“ V takto podrobněji zapsaném kroku vidíme dvě „logické díry“. Za úsudkem, že není-li y sudé, je liché, se skrývá nedokázaný (a nedokazatelný) předpoklad, že každé y je sudé nebo liché. Za úsudkem, že je-li y^2 liché, je to spor s předpokladem, že y^2 je sudé, se skrývá nedokázaný a pravděpodobně rovněž nedokazatelný předpoklad, že žádné x není současně sudé i liché. Naše pojednání o sudých a lichých číslech bylo (záměrně) příliš stručné, zmínka o obou těchto předpokladech by k němu měla patřit.

Další logickou závadou našeho důkazu je už ten krok, ve kterém jsme usoudili, že existuje-li nenulové x, ke kterému existuje y takové, že $y^2 = 2 \cdot x^2$, pak existuje nejmenší x s touto vlastností:

$$\exists x(x \neq 0 \ \&\ \exists y(y^2 = 2 \cdot x^2)) \ \to\ \exists x(x \neq 0 \ \&\ \exists y(y^2 = 2 \cdot x^2) \ \& \ \& \ \forall v(v < x \ \to\ \neg(v \neq 0 \ \&\ \exists y(y^2 = 2 \cdot v^2)))). \tag{6}$$

Toto tvrzení z axiomů A1–A15 dokazatelné není, avšak protože si jeho dokazatelnost přejeme, musíme k axiomům přidat je samotné nebo něco, z čeho by plynulo. Přidat je samotné je naprosto rozumné řešení, avšak než bychom to udělali a tvrzení (6) přidělili číslo 16 v našem číslování axiomů, mysleme trochu dále. Tvrzení (6) říká, že existuje-li x s vlastností $A(x)$, pak existuje i x s vlastností $A(x)$ & $\forall v(v < x \ \to\ \neg A(v))$ neboli existuje-li x s vlastností $A(x)$, pak mezi takovými x některé je nejmenší, a toto říká pro případ, kdy $A(x)$ je vlastnost $x \neq 0$ & $\exists y(y^2 = 2 \cdot x^2)$. Takové tvrzení by ale mělo platit pro *každou* vlastnost $A(x)$. Přirozených čísel menších než nějaké x je totiž jen konečně mnoho. My v našem aritmetickém jazyce sice nemůžeme mluvit o konečných a nekonečných množinách, to ale neznamená, že máme ignorovat princip, že mezi konečně mnoha čísly některé je nejmenší (ledaže jejich počet by byl nula). Definujme tedy, že každá sentence tvaru

$$\text{LNP:} \qquad \forall y_1 \,..\, \forall y_k(\exists x A(x, \underline{y}) \ \to\ \exists x(A(x, \underline{y}) \ \&\ \forall v(v < x \ \to\ \neg A(v, \underline{y})))),$$

kde $\underline{y}$ je zkratka pro $y_1, \ldots, y_k$, je axiomem. Tím je s konečnou platností, tj. definitivně pro tento text, stanoveno, co je Peanova aritmetika: je to teorie s jazykem $\{+, \cdot, <, 0, 1\}$, s patnácti jednotlivými axiomy A1–A15 a s nekonečně mnoha axiomy tvaru LNP.

LNP je zkratka pro *least number principle*, česky *princip nejmenšího prvku*. Peanova aritmetika je možná poněkud nezvyklá tím, že má nekonečně mnoho axiomů. Důležité ale je, že všechny sentence tvaru LNP (říká se všechny *instance schématu* LNP) mají stejný tvar, takže o tom, zda nějaká sentence je nebo není axiomem, lze rozhodovat algoritmem. Proměnným označeným $y_1, \ldots, y_k$ se říká *parametry* a schéma LNP vlastně vyjadřuje o něco obecnější princip, než jsme před okamžikem naznačili: existuje-li x s určitou vlastností nebo s určitým vztahem k daným (pevným) parametrům, pak existuje i nejmenší x s onou vlastností

nebo s oním vztahem k týmž parametrům. Ještě je důležité poznamenat a zdůraznit, že řeč je o vlastnostech a vztazích vyjádřitelných v aritmetickém jazyce. Než některou instanci schématu LNP v nějakém důkazu použijeme, musíme se přesvědčit, že opravdu máme vlastnost nebo vztah (podmínku), kterou s pomocí (jen) našich pěti symbolů dokážeme napsat. Ukažme si na několika příkladech, jak se princip nejmenšího prvku používá. Tím zároveň mimo jiné odstraníme zbývající nedostatky v důkazu Věty 5.

Lemma 6 *(a) Každé x je sudé nebo liché.*
(b) $\forall x \forall y (x < y \rightarrow x + 1 \leq y)$.
(c) Žádné x není současně sudé i liché.

Důkaz Zvolme za $A(x)$ vlastnost $\neg\exists v(x = 2 \cdot v \vee x = 2 \cdot v + 1)$. Předpokládejme (tj. snažme se přivést ke sporu předpoklad), že existuje x takové, že $A(x)$, čili takové, že x není sudé ani liché. Instance schématu LNP příslušná k vlastnosti $A(x)$ dává číslo x takové, že x není sudé ani liché, avšak každé $v < x$ je sudé nebo liché. Je jasné, že $x \neq 0$, protože o nule víme, že je sudá. Použijme úvahu, kterou jsme již dříve učinili, a vezměme číslo z takové, že $z + 1 = x$. Je jasné, že $z < x$, takže z, stejně jako všechna čísla menší než x, je sudé nebo liché. Rozeberme oba případy. Když $z = 2 \cdot v$, pak $z + 1 = 2 \cdot v + 1$ čili x je liché. To je spor. Když $z = 2 \cdot v + 1$, pak $z + 1 = 2 \cdot v + 2 = 2 \cdot (v + 1)$, takže x je sudé, což je také spor.

V (b) postupujme obdobně. Kdyby existovala nějaká čísla x porušující podmínku $\forall y(x < y \rightarrow x+1 \leq y)$ tvrdící, že mezi x a $x+1$ není žádné jiné číslo, schéma LNP zaručuje existenci nejmenšího takového x. To si vezměme. K x tedy máme y takové, že $x < y$ a $y < x + 1$. Přitom z axiomu A14 víme, že $x \neq 0$, tedy i $y \neq 0$. Se stejným zdůvodněním jako v důkazu tvrzení (a), existují x' a y' taková, že $x' + 1 = x$ a $y' + 1 = y$. Takže $x' + 1 < y' + 1$ a $y' + 1 < x' + 2$, tedy $x' < y'$ a $y' < x' + 1$. To je spor, neboť y' je mezi x' a $x' + 1$, číslo x' je menší než x, a přitom x bylo nejmenší číslo porušující podmínku, že mezi x a x' není nic.

V (c) uvažme nějaké číslo x, které je současně sudé i liché. Existují tedy u a v taková, že $x = 2 \cdot u$ a $x = 2 \cdot v + 1$. Nemůže platit $u = v$, neboť $2 \cdot u = 2 \cdot u + 1$ jsme vyloučili hned po uvedení axiomu A14. Probereme případy $u < v$ a $v < u$. Když $u < v$, pak $2 \cdot u < 2 \cdot v$, a tím spíše $2 \cdot u < 2 \cdot v + 1$. Když $v < u$, pak dle již dokázaného tvrzení (b) máme $v + 1 \leq u$, tedy $2 \cdot v + 2 \leq 2 \cdot u$, tedy $2 \cdot v + 1 < 2 \cdot u$. To je opět ve sporu s $2 \cdot u = 2 \cdot v + 1$. ⊣

V důkazu tvrzení (c) jsme schéma LNP sice přímo nepoužili, avšak použili jsme tvrzení (b), v jehož důkazu schéma LNP potřebné bylo.

Místo schématu LNP se často používá a v literatuře uvádí *schéma indukce*. To je schéma, které dovoluje z každé podmínky $A(x, \underline{y})$ pro x a parametry $y_1, \ldots, y_k$ (podmínky formulovatelné v aritmetickém jazyce!) utvořit axiom, který tvrdí, že pokud $A(0, \underline{y})$, tj. nula má vztah A k parametrům $y_1, \ldots, y_k$, a pokud přitom

$\forall x(A(x,\underline{y}) \to A(x+1,\underline{y}))$, tj. pro žádné x se nemůže stát, aby x mělo a $x+1$ nemělo vztah A k týmž parametrům $y_1,\ldots,y_k$, pak $\forall x A(x,\underline{y})$. Schéma indukce je se schématem LNP ekvivalentní a s našimi dosavadními znalostmi by ani nebylo tak těžké to dokázat.

V často citované literatuře, například v knize Tarski, Mostowski, Robinson, *Undecidable theories*, 1953, je uvedena verze Peanovy aritmetiky, která má (kromě schématu indukce) pouze sedm jednotlivých axiomů. Naše verze Peanovy aritmetiky je téměř beze změny převzata z knihy R. Kaye, *Models of Peano Arithmetic*, 1991. Všechny verze jsou samozřejmě ekvivalentní v tom smyslu, že jsou v nich dokazatelná táž tvrzení. Tradiční verze s pouhými sedmi axiomy je elegantní, avšak nedrželi jsme se jí, neboť jsme se rychleji chtěli dostat k zajímavějším důkazům a nezdržovat se důkazy jednoduchých tvrzení, která se v naší (Kayeově) verzi jeví jako axiomy A1–A15.

Aby poměr mezi počtem axiomů a počtem dokázaných zajímavých tvrzení byl příznivější a také abychom lépe dokumentovali svou tezi, že všechny známé důkazy z určité oblasti matematiky lze často formalizovat (reprodukovat) v teorii s nevelkým počtem axiomů, uvádíme ještě následující Větu 7. Tato věta se týká dělitelnosti a prvočíselnosti a je pokračováním úvah, jež jsme vedli v okolí podmínky (4), která je naší definicí prvočíselnosti. Domluvme se, že dělitelnost značíme symbolem $|$. Podmínka $x \mid y$ znamená $\exists v(v\cdot x = y)$ a čteme ji „x je dělitel čísla y“ nebo „y je dělitelné číslem x“. Při této definici dělitelnosti to (správně) dopadá tak, že číslo 1 je dělitelem každého čísla a číslo 0 je dělitelné každým číslem. S použitím symbolu pro dělitelnost můžeme vlastnost (4) vyjadřující, že x je prvočíslo, ekvivalentně zapsat takto:

$$x \neq 1 \;\&\; \forall y(y \mid x \;\to\; y = 1 \;\vee\; y = x), \tag{7}$$

přičemž druhý člen konjunkce vyjadřuje, že x nemá žádné dělitele různé od jedné a sebe sama, tj. že x nemá žádné *netriviální dělitele*. V bodu (c) Věty 7 ověříme, že vlastnosti (4) a (7) jsou ekvivalentní.

Uvedením Věty 7 sledujeme ještě další účely. Jednak chceme čtenáři poskytnout více příležitostí k samostatnému zamyšlení. Naše důkazy tvrzení (a)–(g) proto nebudou úplně podrobné, některé budou spíš jen návodem k napsání plného důkazu. Větou 7 také chceme utvrdit dojem, že v Peanově aritmetice můžeme dokázat „všechno, co nás napadne“. To je důležité proto, že kdo by si myslel, že existují nějaká „zjevně pravdivá“ tvrzení nedokazatelná v Peanově aritmetice, nemohl by Gödelovu větu ocenit.

Pokud pro každé x existují prvočísla větší než x, jak se tvrdí v bodu (g) Věty 7, znamená to, že prvočísel je nekonečně mnoho. To je význam Věty 7 a její body (a)–(f) jsou jen pomocná tvrzení pro důkaz bodu (g). Celý důkaz Věty 7 je vlastně Eukleidův klasický důkaz, který je ale upraven tak, aby se vystačilo s aritmetickým jazykem a nepoužily se pojmy, které bychom v něm těžko vyjádřili, totiž faktoriál a prvočíselný rozklad daného čísla.

Věta 7 *(a) $\forall x(x \mid x)$. Když $x \mid y$ a $y \mid z$, pak $x \mid z$.*
(b) Číslo 1 je dělitelem každého čísla. Každé číslo je dělitelem nuly. Číslo 0 je jediné číslo, které je dělitelné nulou, a není to prvočíslo. Každý dělitel čísla z je dělitelem čísla $z \cdot x$.
(c) Dvě definice prvočíselnosti vyjádřené podmínkou (4) a podmínkou (7) jsou spolu ekvivalentní.
(d) Pro každé x existuje $z \neq 0$, které je dělitelné všemi nenulovými čísly v takovými, že $v \leq x$.
(e) Když $1 < v$ a $v \mid z$, pak v není dělitel čísla $z + 1$.
(f) Každé číslo $w \neq 1$ je dělitelné nějakým prvočíslem.
(g) Pro každé číslo x existují prvočísla větší než x.

Důkaz Když x lze vynásobit číslem v_1 tak, aby vyšlo y, a y lze vynásobit číslem v_2 tak, aby vyšlo z, lze x vynásobit jistým číslem, totiž číslem $v_1 \cdot v_2$, tak, aby vyšlo z. Tím je zdůvodněno druhé tvrzení bodu (a) a stojí za to upozornit, že byl použit axiom A3. První tvrzení v (a) bezprostředně plyne z axiomu A7.

Důkazy tvrzení v bodu (b) jsou lehké a jsou ponechána jako cvičení. V (c) uvažujme $x \neq 1$, které má vlastnost (4) a uvažujme nějakého jeho dělitele y. Máme v takové, že $y \cdot v = x$. Podmínka (4) k tomu říká $y = 1$ nebo $v = 1$. Když $y = 1$, pak y je triviální dělitel. Když $v = 1$, pak $y = x$ a y je triviální dělitel také. Nechť naopak $x \neq 1$ a x má vlastnost (7), a nechť $u \cdot v = x$. Protože nula vlastnost (7) nemá, platí $x \neq 0$. Protože u je dělitel čísla x, z podmínky (7) máme $u = 1$ nebo $u = x$. V prvním případě jsme hotovi. V druhém z $x \cdot v = x$ a $x \neq 0$ máme $v = 1$.

V (d) uvažujme nejmenší číslo x, pro něž neexistuje nenulové z dělitelné všemi nenulovými v takovými, že $v \leq x$. Mírně abstraktní ale správná úvaha ukazuje, že $x \neq 0$. Pro $x = 0$ totiž neexistují nenulová v splňující podmínku $v \leq x$, tedy volba $z = 1$ dává nenulové číslo dělitelné všemi nenulovými čísly splňujícími podmínku $v \leq x$. Když tedy $x \neq 0$, máme x' takové, že $x' + 1 = x$. Protože $x' < x$, k x' existuje z dělitelné všemi nenulovými $v \leq x'$. Pak ale, dle posledního tvrzení v bodu (b), číslo $z \cdot (x' + 1)$ tj. číslo $z \cdot x$ je dělitelné všemi nenulovými $v \leq x'$, a je dělitelné i číslem x. To podle Lemmatu 6(b) znamená, že $z \cdot x$ je dělitelné všemi nenulovými $v \leq x$, a je to spor s předpokladem, že k x neexistuje číslo dělitelné všemi nenulovými $v \leq x$.

Důkaz tvrzení (e) je skoro stejný jako důkaz tvrzení (c) Lemmatu 6, takže jej vynecháváme. V (f) uvažujme nejmenší číslo w, které není dělitelné žádným prvočíslem. Protože $w \mid w$, číslo w není prvočíslo. Číslo w tedy má nějakého netriviálního dělitele. Máme tedy v takové, že $v \mid w$, $v \neq 1$, $v \neq w$. Musí platit $1 < v$ a $v < x$. Protože x je nejmenší číslo větší než 1, které není dělitelné žádným prvočíslem, v nějakým prvočíslem dělitelné je. Týmž prvočíslem je ovšem dělitelné i x, což je spor.

Nechť je v (g) nějaké x dáno. Můžeme předpokládat, že $x \neq 0$, protože pro $x = 0$ evidentně existují prvočísla větší než x. Užijme (d) a uvažujme nenulové z, které je dělitelné všemi nenulovými $v \leq x$. Vezměme $w = z + 1$. Dle (e) číslo w není dělitelné žádným v takovým, že $1 < v$ a $v \leq x$. Není tedy dělitelné ani žádným prvočíslem v takovým, že $v \leq x$. Dle (f) ale nějakým prvočíslem dělitelné je. Toto prvočíslo musí být větší než x. ⊣

Na závěr tohoto oddílu chceme ještě upozornit na jednu nebo dvě okolnosti, které souvisejí s vyjadřovacími schopnostmi aritmetického jazyka. Brzy po uvedení axiomů A14 a A15 jsme dokázali, že dvě je nejmenší z čísel větších než jedna. Předtím, přímo z axiomu A14, bylo jasné, že jedna je nejmenší z čísel větších než nula. Brzy po tom jsme pro čísla 2 a 3 dokázali, že

$$\text{tři (tj. } 2+1\text{) je nejmenší z čísel větších než dva} \tag{8}$$

$$\text{čtyři (tj. } 3+1\text{) je nejmenší z čísel větších než tři} \tag{9}$$

a pravděpodobně jsme čtenáře přesvědčili, že další analogická tvrzení lze dokázat pro čísla čtyři, pět, šest, … Důležité ale je si při tom uvědomit, že tvrzení (8) a (9) a další analogická tvrzení pro čísla čtyři, pět, šest, atd. mají každé svůj vlastní důkaz, takže máme představu o *nekonečně mnoha celkem jednoduchých avšak delších a delších důkazech*. Nekonečně mnoho důkazů tvrzení $A(0)$, $A(1)$, $A(2)$, … ale ještě zdaleka není totéž co jeden důkaz obecného tvrzení

$$\text{pro každé } x\text{, číslo } x+1 \text{ je nejmenší z čísel větších než } x. \tag{10}$$

Na první pohled by se mohlo zdát, že máme-li důkazy *všech* tvrzení $A(0)$, $A(1)$, $A(2)$, …, je tím dokázáno i $\forall x A(x)$. To ale pravda není. Kdo tvrdí dokazatelnost tvrzení $\forall x A(x)$, musí podat jeden (konečný) důkaz tohoto tvrzení. Naše hra se hraje tak, že protihráč zadá x a my se pak ve svém (jednom) důkazu musíme vyjádřit k tomuto x. Nehraje se tak, že protihráč zadá x a my teprve pak píšeme svůj důkaz, různý pro jednotlivá x. Na jedné úrovni totiž mluvíme o číslech, na jiné (logické) mluvíme o formulích a důkazech. Kdybychom na logické úrovni tvrdili například něco takového jako „pro každý důkaz tvrzení B existuje i důkaz tvrzení $f(B)$“, bylo by pochopitelné, že důkaz tvrzení $f(B)$ bychom konstruovali až poté, kdy protihráč zadal svůj důkaz tvrzení B. Ovšem v naší axiomatické teorii, tj. na té úrovni (formální), kde mluvíme o číslech, musíme podat jeden důkaz tvrzení $\forall x A(x)$, který má konečnou délku.

Nalézání důkazů se v něčem podobá psaní počítačových programů. Správný počítačový program, který počítá nějakou úlohu čili zpracovává nějaká data, musí být připraven na všechny možné vstupy či všechna možná data. Bylo by směšné, kdyby jeho autor požadoval, aby nejprve byla zadána data, která má program zpracovat, a on teprve pak napíše svůj program.

Snad jsme tedy čtenáře přesvědčili, že situace, kdy pro nějakou vlastnost $A(x)$ všechna tvrzení $A(0)$, $A(1)$, $A(2)$, … důkaz mají, ale obecné tvrzení $\forall x A(x)$ dokazatelné není, je možná a je nutno s ní počítat. Pak ale přirozená otázka zní, zda tedy máme nějaký konkrétní příklad takové vlastnosti $A(x)$. Vlastnost „číslo $x+1$ je nejmenší z čísel větších než x“ tím příkladem není, neboť pro tuto vlastnost $A(x)$ je $\forall x A(x)$ tvrzením (b) Lemmatu 6 (které jsme úspěšně dokázali).

Příklad vlastnosti $A(x)$ takové, že všechna tvrzení $A(0)$, $A(1)$, $A(2)$, … dokázat lze, ale $\forall x A(x)$ dokázat nelze, není pro tak silnou teorii, jako je Peanova aritmetika, snadné podat. Avšak existenci takové vlastnosti zaručuje Gödelova věta. To znamená, že s existencí takových vlastností je nejen nutné počítat: jejich existence je pro každou rozumnou axiomatickou teorii jistá a První Gödelovu větu lze chápat tak, že tvrdí právě toto.

A ještě si všimněme toho, že na několika místech jsme dodržovali opatrnost ve vyjadřování, aby bylo jisté, že máme vlastnosti, podmínky a tvrzení, která lze vyjádřit v aritmetickém jazyce a zapsat je symbolicky. Například jsme se vyhnuli tvrzení, že

$$\text{každé číslo } x \text{ je vyjádřitelné jako součin několika prvočísel.} \tag{11}$$

Počet prvočísel v prvočíselném rozkladu nějakého čísla x totiž může být jedna nebo dvě nebo tři nebo …, takže tvrzení (11) je vlastně něco jako „každé x je prvočíslo nebo je součinem dvou prvočísel nebo je součinem tří prvočísel nebo …“, zápis s nekonečně mnoha disjunkcemi. Tvrzení (11) jsme nezapsali bezpatkovým písmem, protože nemůžeme bez dalšího výkladu a úmluv po čtenáři požadovat, aby si za ním představil formální zápis. Ještě pádnějším příkladem je „každé číslo je některým z čísel nula, jedna, dvě, tři, …“. To za tvrzení vůbec neuznáváme, neboť je v aritmetickém jazyce nelze formalizovat bez ohledu na další výklad a úmluvy. To znamená, že otázce, zda je pravdivé, nepřikládáme žádný smysl. Nekonečné počítačové programy přeci také neuznáváme, a nepřikládáme tudíž žádný smysl otázce, jestli správně fungují.

Tím chceme říci, že Gödelova věta je poznatkem sice abstraktním, ale ne tak nepřirozeným. S občas se vyskytujícím názorem, že ukazuje meze formálního (matematického) myšlení nebo odkrývá nějakou nedokonalost (formální) logiky, nelze souhlasit. Formální logika je v naprostém pořádku, dobře vystihuje to, jak se v matematice píší důkazy, a také dobře vystihuje to, jak myslíme, ať už je to v matematice, nebo mimo ni.

Reference

[Göd30] K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatsh. Math. Phys.*, 37:349–360, 1930.

[Göd31] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38:173–198, 1931.

[Kay91] R. Kaye. *Models of Peano Arithmetic*. Oxford University Press, 1991.

[Šve98] V. Švejdar. Logika v aritmetice. V P. Jirků a V. Švejdar, editoři, *Miscellanea Logica I*, str. 36–48. Karolinum, Praha, 1998. ISBN 80-7184-578-7.

[TMR53] A. Tarski, A. Mostowski a R. M. Robinson. *Undecidable Theories*. North-Holland, Amsterdam, 1953.