MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Jakub Hofman

Důkazy

Katedra didaktiky matematiky

Vedoucí bakalářské práce: RNDr. Jakub Staněk, Ph.D.
Studijní program: Fyzika
Studijní obor: Fyzika zaměřená na vzdělávání

Praha 2018

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

Praha 17. května 2018 Podpis autora:

Rád bych vyjádřil poděkování vedoucímu mé práce, RNDr. Jakubu Staňkovi, Ph.D., za odbornou pomoc při vypracování této bakalářské práce. Zvláštní poděkování patří RNDr. Ireně Dvořákové, Ph.D., která mi byla stálou oporou a zejména jejíž zásluhou tato práce vznikla.

Název práce: Důkazy

Autor: Jakub Hofman

Procoviště: Katedra didaktiky matematiky

Vedoucí bakalářské práce: RNDr. Jakub Staněk, Ph.D., Katedra didaktiky matematiky

Abstrakt:

Tato bakalářská práce má žákům středních škol přiblížit pojem matematického důkazu, stručně popsat jednotlivé důkazové metody a poskytnout vzorově dokázané věty z různých oblastí matematiky. Dalším cílem této práce je poskytnout žákům středních škol studijní materiál, který svou strukturou odpovídá matematickým učebnicím a skriptům, které bývají k dispozici na vysokých školách.

V první části je žák obeznámen se základními pojmy logiky. Jsou zde obsaženy pojmy, se kterými se žáci střední školy běžně setkají v hodinách matematiky. Znalost těchto pojmů je klíčová pro pochopení principů jednotlivých důkazových metod.

Hlavní část práce se věnuje vysvětlení jednotlivých důkazových metod a jejich aplikaci při dokazování matematických vět. Tyto věty svou odbornou obtížností odpovídají znalostem žáka střední školy. Věty jsou řazeny podle obtížnosti jejich důkazu, samotné věty na sebe nenavazují ani nevytváří ucelenou matematickou teorii, neboť to není záměrem práce.

Součástí práce je také přehled vět, které by měl žák být schopen samostatně dokázat, jakmile se seznámí se způsobem práce s důkazovými metodami. U většiny vět si žák vystačí se znalostmi ze střední školy, ovšem vyskytují se zde i věty nad rámec klasické školní výuky. Dále jsou v práci uvedeny některé chybné důkazy, které má žák opravit. Řešení všech těchto úloh jsou uvedena v samostatné kapitole textu.

Klíčová slova: Důkaz, přímý důkaz, důkaz sporem, obměněná implikace, matematická indukce

Title: Proofs

Author: Jakub Hofman

Department: Department of Mathematics Education

Supervisor: RNDr. Jakub Staněk, Ph.D., Department of Mathematics Education

Abstract:

This bachelor thesis should clarify the concept of a mathematical proof, briefly describe the individual proof methods and provide examples of proved theorems from various branches of mathematics. Another objective of this thesis is to provide a high school pupil with a study material which with it structure corresponds to mathematical textbooks and lecture notes provided by universities.

In the first part of the thesis the basic terms of logic are introduced to the pupil. These are terms a pupil can usually encounter in math classes at school. The knowledge of these terms is essential for understanding the principles of the individual proof methods.

The main part of the thesis is focused on explaining the individual proof methods and their application in proving mathematical theorems with difficulty appropriate to a pupil of secondary education. The theorems are ordered by the difficulty of their proof; they do not follow from one another nor do they form a coherent mathematical theory as that is not the goal of this thesis.

The thesis also contains a list of theorems which a pupil should be capable of proving after being acquainted with the methods of mathematical proof. Most of these require knowledge provided by a secondary school, but there are also theorems which are beyond the scope of secondary education. The thesis also includes some incorrectly formed proofs that the pupil is to correct. The solutions to all these exercises are given in a separate chapter of the text.

Keywords: Proof, Direct Proof, Proof by Contradiction, Contraposition, Mathematical Induction

Obsah

Úvod

V této práci se věnuji stručnému a jasnému popisu několika metod, kterými se v matematice dokazují věty. Také prezentuji pravidla, kterými by se měl autor matematického důkazu řídit, aby byl jeho důkaz přehledný, správně formulovaný a jasný. Veškeré popsané strategie pak přímo aplikuji na množství jednoduchých i obtížnějších vět. Dále čtenářům poskytuji seznam vět, které mohou zkusit sami dokázat.

Motivací k napsání této práce mi byly názory některých studentů vysokých škol zaměřených na matematiku, kteří byli po nástupu do prvního ročníku zaskočeni tím, jak odlišný je způsob výuky matematiky na vysoké škole od výuky na střední škole. Po společné diskusi s těmito studenty a s žáky středních škol a také z vlastní zkušenosti ze střední školy jsem došel k závěru, že se na mnohých středních školách nevěnuje důkazům dostatečná pozornost. Ačkoliv je běžné, že učitelé některé skutečnosti odvozují, jedná se převážně o přímé odvozování vzorců jednoduchou manipulací výrazů bez nutnosti uvádění argumentů. Zkušenost s takovými důkazy ovšem není postačující pro studium na vysoké škole, proto studenti prvních ročníků mnohdy narážejí na překážky v porozumění učivu, které je zbytečně brzdí. Důkazy jsou obsahem středoškolských učebnic a rámcového vzdělávacího programu pro gymnázia, nejsou ovšem požadované na většině odborných středních škol, proto není možné žáky z důkazů testovat u společné maturitní zkoušky ani na gymnáziích, u jejichž žáků se předpokládá další studium. Důkazy nejsou požadavkem ani k maturitní zkoušce z Matematiky+.

Středoškolské učebnice většinou zmínku o důkazech obsahují, ovšem bývá to v rámci tématu matematické logiky, ve kterém se důkazy objeví pouze na pár stranách. To navozuje dojem, že důkazy jsou pouze jedno malé téma v matematice, nikoliv že jsou nedílnou součástí celé matematiky jako takové. Naopak na druhé straně spektra stojí odborné knihy, které se důkazům věnují velmi dopodrobna, pro běžného čtenáře jsou ovšem příliš nestravitelné, zbytečně obsáhlé a věnují se formálním důkazům v hilbertovském kalkulu. Pro žáky mohou být schůdnější internetové zdroje, které však často bývají nespolehlivé či prezentují velmi omezené typy vět, na které jsou jednotlivé důkazové metody používány. Žák může z tohoto zdroje nabýt dojmu, že jedna důkazová metoda je vhodná pouze pro jeden konkrétní druh vět.

Na základě těchto zjištění jsem se rozhodl napsat tuto práci jako cvičebnici důkazových technik, která obsahuje věty z různých oblastí matematiky různého charakteru, je pro žáka střední školy přiměřená svou úrovní a obsahuje věty i nad rámec středoškolského učiva, a to věty jednoduché vysokoškolské či pouhé matematické kuriozity.

Matematická teorie je prezentována stejně jako na vysoké škole, tedy formou lidově zvanou D-V-D neboli definice-věta-důkaz. Před většinou vět je uvedena definice či lemma, kterých je při důkazu věty využito. Toto má žákům středních škol přiblížit styl, kterým jsou vedeny učební materiály využívané na vysokých školách. Cílem je překlenout propast, která se nachází mezi způsoby výuky matematiky na středních a vysokých školách.

Práce je rozdělena do čtyř kapitol. V první kapitole je stručně uvedeno několik termínů z logiky a obecné matematiky, které jsou nepostradatelné při výkladu důkazových metod. Druhá kapitola již přímo tyto metody žákům představuje a předvádí jejich užívání na několika příkladech. Cvičení z logiky a znění vět, které má žák již zkusit samostatně dokázat, jsou uvedena ve třetí kapitole. Závěrečná čtvrtá kapitola pak obsahuje jejich řešení.

Seznam použitých symbolů

symbol	čteme	použití
$=$	rovná se	$x = 3$
$\neq$	není rovno	$2 \neq 7$
$\leq$	je menší nebo rovno než	$x \leq \|x\|$
$<$	je menší než	$5 < 10$
$\geq$	je větší nebo rovno než	$4 \geq 3 + (-1)^k$
$>$	je větší než	$7 \geq 3$
$\in$	náleží	$B \in p$
$\mathbb{R}$	reálná čísla	$x \in \mathbb{R}$
$\mathbb{Z}$	celá čísla	$n \in \mathbb{Z}$
$\mathbb{N}$	přirozená čísla	$n \in \mathbb{N}$
$\mathbb{N}_0$	přirozená čísla s nulou	$n \in \mathbb{N}_0$
( )	otevřená a uzavřená závorka	$2(3 + 5) = 16$
(,)	otevřený interval	$x \in (-1, 1)$
[ ]	otevřená a uzavřená hranatá závorka	$[(1 + 2) \cdot 3 + 1] \cdot 4$
[,]	uzavřený interval	$x \in [-1, 1]$
∞	nekonečno	$\mathbb{R} = (-\infty, \infty)$
$\forall$	pro všechna	$\forall x \in \mathbb{R}$
$\exists$	existuje	$\exists n \in \mathbb{N}$
$\neg$	negace	$\neg V$
$\wedge$	a zároveň	$V_1 \wedge V_2$
$\vee$	nebo	$V_1 \vee V_2$
$\Rightarrow$	implikuje	$V_1 \Rightarrow V_2$
$\Leftrightarrow$	je ekvivalentní s	$V_1 \Leftrightarrow V_2$
$\binom{n}{k}$	n nad k	$\binom{3}{2} = 3$
$\sin x$	sinus x	$\sin x =$ protilehlá/přepona
$\cos x$	kosinus x	$\cos x =$ přilehlá/přepona
$\sqrt{x}$	druhá odmocnina z x	$\sqrt{16} = 4$
$\|x\|$	absolutní hodnota z x	$\|-5\| = 5$
$f(x)$	funkce s proměnnou x	$f(x) = x^2 + 2x + 1$

1 Základní poznatky

Tato kapitola je věnována stručnému uvedení některých základních poznatků, které by měl čtenář ovládat, než se pustí do studia samotných důkazových technik.

1.1 Základy matematiky

Následující pojmy jsou důležité základy matematiky jako vědy, představují stavební kameny matematické teorie.

- **Definice** přesně zavádí pojmy na základě nějaké vlastnosti. Například definice prvočísel zní „prvočíslo je takové přirozené číslo, které je dělitelné pouze 1 a samo sebou“. Definice obsahuje název definovaného objektu (prvočíslo) a vlastnost, která tento objekt jednoznačně určí (přirozené číslo dělitelné pouze 1 a samo sebou). Definice je obecně platná, protože v podstatě jen pojmenovává nějakou skupinu objektů, které sdílí jednu vlastnost. [BC09, str. 90.]

- **Věta** je tvrzení, které hovoří o těch vlastnostech nějakých definovaných objektů, které nejsou součástí definice, avšak dané objekty je také mají. Příkladem je věta „součet velikostí úhlů trojúhelníka je roven 180°“, protože definovaným objektům (úhlům trojúhelníka) přisuzuje nějakou vlastnost (součet velikostí je 180°). Matematická věta musí být dokázaná. Principem důkazu se budeme v této práci zabývat. V některých případech může věta také jednoznačně určovat skupinu objektů a mohla by být použita jako definice. [BC09, str. 90.]

- **Axiom** je tvrzení, které je přijímáno bez pochyby a bez důkazu. Soubor takových tvzení vytváří podloží, ze kterého se buduje matematická teorie. Příkladem mohou být Peanovy axiomy [Ecc97, str. 113.]

pro přirozená čísla nebo Eukleidovy axiomy (postuláty) eukleidovské geometrie. [BC09, str. 90.]

- **Základní pojmy** jsou objekty, jejichž vlastnosti jsou popsané v axiomech. Spolu s axiomy (a dalšími náležitostmi) patří do axiomatického systému budované teorie. [GT96, str. 98.]
- **Důkaz** je postup, kterým z axiomů a již odvozených vět vyvozujeme nové věty. Právě v důkazu se ukrývá největší část matematiky a představuje hlavní náplň práce matematiků teoretiků. [BC09, str. 90.]

V této práci se budeme zabývat strukturou důkazů. Nebudeme budovat žádnou matematickou teorii, pouze se zaměříme na některá vybraná tvrzení, jejichž objekty zájmu si zadefinujeme, ale pojmy využité v těchto definicích budeme chápat buď intuitivně, nebo na základě předchozích znalostí z hodin matematiky na základní či střední škole.

1.2 Logika

Dokazování v matematice probíhá jako posloupnost tzv. *výroků*. Samotné matematické věty jsou také výroky a zvolená dokazovací metoda závisí na tom, jaké podoby výrok nabývá. V této části si stručně uvedeme některé důležité pojmy matematické logiky.

- **Výrok** je oznamovací věta, o které má smysl rozhodovat, zdali je pravdivá, nebo ne. [Blo00, str. 4.] Výroky budeme označovat písmenem V s případným spodním indexem.

  Příklady vět, které jsou výroky:
  V_1: „Pes je savec.“
  V_2: „Hlavním městem České republiky je Plzeň.“
  V_3: „Názvy všech států světa začínají na písmeno R.“
  V_4: „V roce 3018 začne lidstvo osidlovat Merkur.“
  V_5: „Některé druhy hadů jsou jedovaté.“

  Příklady vět, které nejsou výroky:
  „Pes by měl být savec.“
  „Hlavní město České republiky, Plzeň.“
  „Začínají názvy všech států světa na písmeno R?“
  „Kéž by v roce 3018 začalo lidstvo osidlovat Merkur.“
  „Vyjmenuj některé jedovaté druhy hadů.“

- **Pravdivostní hodnota** určuje, jestli je výrok pravdivý, nebo nepravdivý. Budeme psát $P(V) = 1$, pokud je výrok pravdivý (např. výroky V_1 a V_5), a $P(V) = 0$, pokud je nepravdivý (výroky V_2 a V_3). Výrok V_4 je také buď pravdivý, nebo nepravdivý, ale jeho pravdivostní hodnotu momentálně nemůžeme znát. [Blo00, str. 5.]

- **Negace** je výroková operace, která nějakému výroku V přiřadí výrok, který má opačnou pravdivostní hodnotu. Negaci značíme ¬, negace výroku V by tedy byla ¬V. [Blo00, str. 8.]

  Příklady negovaných výroků V_1 až V_5:
  $\neg V_1$: „Pes není savec."
  $\neg V_2$: „Hlavním městem České republiky není Plzeň."
  $\neg V_3$: „Názvy některých států světa nezačínají na písmeno R."
  $\neg V_4$: „V roce 3018 nezačne lidstvo osidlovat Merkur."
  $\neg V_5$: „Žádný druh hadů není jedovatý."

  Složené výroky negujeme následujícím způsobem:
  $P(V_1 \wedge V_2) \Leftrightarrow P(\neg V_1 \vee \neg V_2)$
  $P(V_1 \vee V_2) \Leftrightarrow P(\neg V_1 \wedge \neg V_2)$
  $P(V_1 \Rightarrow V_2) \Leftrightarrow P(V_1 \wedge \neg V_2)$

- **Kvantifikátor** určuje, o jakém množství věci mluvíme. Dvěma základními kvantifikátory jsou univerzální kvantifikátor ∀ a existenční kvantifikátor ∃ (také zvané velký a malý kvantifikátor). První se čte „pro všechna" nebo podobně a byl použit v příkladovém výroku V_3. Druhý kvantifikátor často čteme „existuje", dá se však nahradit jiným slovem, jako je tomu ve výroku V_5. Obsahuje-li výrok jeden z těchto kvantifikátorů, obsahuje jeho negace druhý z těchto kvantifikátorů, jako je tomu u výroků V_3 a V_5 a jejich negací. [Blo00, str. 43–44.]

Dalšími důležitými slovy jsou *nejvýše*, *právě* a *alespoň*. Tato slova blíže určují počet objektů zájmu při použití existenčního kvantifikátoru. V následujících větách jsou tato slova použita na příkladech.
„Kvadratická rovnice má nejvýše dva reálné kořeny."
„Prvočíslo je takové číslo, které má právě dva různé dělitele."
„Každý mnohoúhelník má alespoň 3 vrcholy."

Na výrocích provádíme výrokové operace, kterým říkáme spojky. Tyto spojky spojují dva výroky v jeden složený. My se budeme zabývat pouze čtyřmi základními spojkami. Pravdivostní hodnota složeného výroku závisí na pravdivostních hodnotách původních dvou výroků. Všechny možnosti pravdivostních hodnot můžeme vypsat do pravdivostní tabulky, jako je tabulka 1.1, ve které jsou pravdivostní hodnoty výroků složených z náhodných výroků V_1 a V_2 pomocí čtyř základních výrokových spojek.

- **Konjunkce** se běžně čte jako „a zároveň“. Aby pravdivostní hodnota výroku složeného pomocí konjunkce byla pravdivá, musí být pravdivé oba skládané výroky zároveň. Značíme ji $\wedge$, konjunkce výroků V_1 a V_2 by byla $V_1 \wedge V_2$. [Blo00, str. 6.]
- **Disjunkce** je spojka, kterou čteme „nebo“. Takový složený výrok je pravdivý, je-li alespoň jeden ze vstupních výroků pravdivý. Značíme ji $V_1 \vee V_2$. [Blo00, str. 7.]
- **Implikace** váže dva výroky do věty „pokud V_1, pak V_2“. Výrok V_1 nazýváme postačující podmínkou výroku V_2 a výrok V_2 nazýváme nutnou podmínkou výroku V_1. [GT96, str. 21] Implikaci značíme $V_1 \Rightarrow V_2$. [Blo00, str. 9.]
- **Ekvivalence** je obousměrná implikace, kterou vyjadřujeme větou „V_1 právě tehdy, když V_2“. Pravdivá je tehdy, mají-li oba výroky V_1 a V_2 stejnou pravdivostní hodnotu. Ekvivalence je značena $V_1 \Leftrightarrow V_2$. Pro nás bude důležité, že se ekvivalence dá nahradit konkjunkcí implikací jako $(V_1 \Rightarrow V_2) \wedge (V_2 \Rightarrow V_1)$. [Blo00, str. 10.]

$P(V_1)$	$P(V_2)$	$P(V_1 \wedge V_2)$	$P(V_1 \vee V_2)$	$P(V_1 \Rightarrow V_2)$	$P(V_1 \Leftrightarrow V_2)$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Tabulka 1.1: Pravdivostní hodnoty čtyř základních spojek

2 Důkazové metody

2.1 Obecná pravidla pro psaní důkazů

Jazyková pravidla

Pravidla pro psaní důkazů bychom měli dodržovat nezávisle na tom, kterou metodu při dokazování používáme. Některá tato pravidla jsou velmi obecná a dají se aplikovat i mimo obor matematiky, jelikož apelují na srozumitelnost argumentace a schopnost rozumně se vyjádřit.

Z hlediska sémantického by důkaz měl být vhodně strukturován a dodržovat syntaktická pravidla. Aby se dal důkaz snadno číst, musí být psán celými větami, nikoliv pouze zkratkovitě nebo v bodech. Logické spojky a kvantifikátory píšeme slovně, nikoliv symbolem, pro snazší čitelnost důkazu. Symbol by také neměl následovat ihned po interpunkčním znaménku. Dlouhé důkazy píšeme po krocích nebo dělíme samostatné části do odstavců.

V důkazu je nutné definovat každý matematický symbol, který používáme. Některé symboly definujeme v každém důkazu zvlášť (např. proměnné). Pokud píšeme delší práci, ve které je obsaženo důkazů více, je možné některé symboly nadefinovat na začátku textu (např. znaménka běžných operací). Při psaní důkazu je nutné uvážit, jaká je předpokládaná úroveň znalostí čtenáře, a patřičně se rozhodnout, které kroky v důkazu lze považovat za očividné a které je nutné vysvětlit.

Více o těchto a dalších pravidlech se lze dočíst v [Blo00, str. 93–102].

Logická pravidla

Již jsme zmiňovali, že důkaz je posloupností výroků. Tyto výroky spolu vytváří ucelený argument, proč věta, kterou dokazujeme, musí na základě již dokázaných tvrzení a axiomů platit. Výroky jsou na sebe navázány logickými pravidly. Tato pravidla vyplývají z logických spojek a dají se dokázat (viz kapitolu **Cvičné úlohy**).

Nejběžnějším pravidlem používaným ve všech dokazovacích metodách je pravidlo **modus ponens**. To tvrdí, že platí-li implikace $V_1 \Rightarrow V_2$ a zároveň platí V_1, pak musí platit V_2. Toto pravidlo nám dovoluje z pravdivých výroků vyvozovat nové poznatky.

Pravidlo, které budeme využívat u důkazu sporem, se nazývá **modus tollens**. Platí-li implikace $V_1 \Rightarrow V_2$ a neplatí-li V_2, pak nemůže platit ani výrok V_1.

Za zmínku také stojí pravidlo nazývané **modus tollendo ponens**, které udává, že pokud platí disjunkce $V_1 \vee V_2$ a zárověň neplatí jeden z výroků V_1 a V_2, pak musí platit druhý z těchto výroků. Jednoduchým příkladem je přirozené n, které, není-li sudé, musí být liché a naopak.

Uvážíme-li, že platná implikace $V_1 \Rightarrow V_2$ je ekvivalentní s $\neg V_1 \vee V_2$, můžeme použitím pravidla modus tollendo ponens ukázat, že platí také implikace $\neg V_2 \Rightarrow \neg V_1$. Této implikaci říkáme **obměněná implikace** a je jednou z důkazových metod, kterou budeme probírat.

O těchto a dalších logických pravidlech se můžete dále a podrobněji informovat v [Blo00, str. 33].

Struktura důkazu

V následujících sekcích rozebereme čtyři základní důkazové metody. Před každou dokazovanou větou si zadefinujeme pojem, o kterém se věta zmiňuje, případně poskytneme užitečné lemma neboli pravdivé tvrzení, které již někdo dokázal a my se o něj můžeme opřít při důkazu dané věty. V každé definici budeme pro přehlednost název definovaného pojmu podtrhávat. Po definicích a lemmatech uvedeme věty, které budeme dokazovat. Následovat bude samotný důkaz, který je ukončen čtverečkem na pravém okraji stránky.

2.2 Důkaz přímý

Princip přímého důkazu

Nejjednodušší dokazovací metodou je důkaz přímý. Při přímém důkazu vycházíme z toho, co už známe – z předpokladů dokazované věty, z již dokázaných vět, z axiomů a z definic – a pomocí logického pravidla modus ponens přecházíme k dokazovaným poznatkům. Pokud je věta výrok V, hledáme výroky V_1 až V_n, jejichž pravdivost známe, takové, abychom z nich mohli odvodit dokazovaný výrok V. Musí tedy dle [GT96, str. 125] platit

$$(V_1 \wedge V_2 \wedge \ldots \wedge V_n) \Rightarrow V.$$

Je-li dokazovaná věta podmíněným výrokem $V_0 \Rightarrow V$, opět hledáme výroky V_1 až V_n, jejichž pravdivost známe, takové, které spolu s výrokem V_0 implikují výrok V. Musí tedy dle [GT96, str. 125] platit

$$(V_0 \wedge V_1 \wedge \ldots \wedge V_n) \Rightarrow V.$$

Každý z výroků V_1 až V_n může být implikován některými nebo všemi z výroků jemu předcházejících.

Věty dokázané přímo

Definice 1. *<u>Sudé číslo</u> je takové číslo n, které lze vyjádřit jako $n = 2k$, kde k je celé číslo.* [OK04, str. 23].

Věta 1. *Osm je sudé číslo.*

Důkaz. Osm lze vyjádřit jako $8 = 2 \cdot 4$ a, jelikož 4 je přirozené číslo, číslo osm splňuje definici 1 a je tedy sudé. □

Pokud bychom chtěli tento důkaz zapsat jako konjunkci výroků, které implikují větu 1, mohli bychom to udělat následujícím způsobem:

V: „Osm je sudé číslo.“
V_1: „$8 = 2 \cdot 4$.“
V_2: „4 je přirozené číslo.“
V_3: „8 splňuje definici 1.“

$(V_1 \wedge V_2) \Rightarrow V_3 \Rightarrow V.$

Takovýto zápis je ovšem zbytečný a špatně srozumitelný, proto jej nebudeme uplatňovat.

Definice 2. *<u>Násobek přirozeného čísla m</u> je takové číslo n, které je číslem m dělitelné beze zbytku, tedy platí $n = k \cdot m$, kde k je přirozené číslo.* [BC09, str. 98.]

Věta 2. *Každý násobek čísla* 6 *je dělitelný* 3.

Důkaz. Nechť n je libovolný násobek 6. Pak dle definice 2 lze psát $n = k \cdot 6$, kde k je libovolné přirozené číslo. Vyjádření n upravíme na $n = 2 \cdot 3 \cdot k$ a označíme $l = 2 \cdot k$. Nyní tedy platí $n = 3 \cdot l$, kde l je nějaké přirozené číslo. Dle definice 2 je n násobkem čísla 3 a tedy n je dělitelné 3. □

Věta 2 obsahuje univerzální kvantifikátor, proto jsme si v důkazy museli zavést proměnnou n, která se ve větě vůbec nevyskytuje. Tato proměnná ovšem nezastupuje všechny násobky čísla 6 najednou, ale jeden libovolně zvolený násobek 6. Jelikož jsme větu dokázali pro libovolný násobek 6, musí platit pro každý násobek 6. Pokud vám tato úvaha dělá problémy, představte si balíček karet rubem vzhůru. Pokud dokážete, že libovolná karta z toho balíčku je srdcová, tak nemusíte obracet každou kartu, abyste se o tom ujistili. Tento postup musíme zvolit, protože na rozdíl od karet v balíčku je násobků šesti nekonečně mnoho, proto bychom ani všechny zkontrolovat nemohli.

Definice 3. *Geometrická posloupnost* $\{a_i\}_{i=1}^{\infty}$ je posloupnost, která je dána svým prvním členem a_1 a rekurentním vzorcem $a_n = a_{n-1} \cdot q$, kde $a_1 \in \mathbb{R}$, $q \in \mathbb{R}$ a $n \in \mathbb{N} \setminus \{1\}$. [Pol72, str. 240.].

Lemma 1. *Pro n-tý člen geometrické posloupnosti platí* $a_n = a_1 \cdot q^{n-1}$. [Pol72, str. 241].

Věta 3. *Součet* S_n *prvních* n *členů geometrické posloupnosti je dán vzorcem*

$$S_n = a_1 \cdot \frac{1 - q^n}{1 - q},$$

kde $q \neq 1$. *Pro* $q = 1$ *je součet prvních* n *členů geometrické posloupnosti roven* $S_n = a_1 \cdot n$. [Pol72, str. 241.].

Důkaz. Součet prvních n členů geometrické posloupnosti je jednoduše

$$\begin{aligned} S_n &= a_1 + a_2 + \cdots + a_n \\ &= a_1 + a_1 \cdot q + \cdots + a_1 \cdot q^{n-1} && \text{(Lemma 1)} \\ &= a_1 \cdot (1 + q + \cdots + q^{n-1}). \end{aligned}$$

Za předpokladu, že $q = 1$, je součet v závorce roven n a dokázali jsme druhou část věty 3. Pokud $q \neq 1$, můžeme pravou stranu rovnosti vynásobit výrazem $\frac{1-q}{1-q}$. Dostáváme rovnost

$$\begin{aligned} S_n &= a_1 \cdot \frac{(1-q)(1+q+\cdots+q^{n-1})}{1-q} \\ &= a_1 \cdot \frac{1+q+\cdots+q^{n-1}-q-q^2-\cdots-q^n}{1-q} \\ &= a_1 \cdot \frac{1-q^n}{1-q}. \end{aligned}$$

$\square$

Ve větě 3 jsme využili lemma 1. Lemma je pomocné tvrzení, které slouží k důkazu věty. Lemmata jsou většinou považována za méně významná tvrzení, lemmaty jsou však nazývány i některé důležité důsledky. Jedná se o větu, je tedy dokazatelná. Toto lemma se dá dokázat indukcí, a proto se k němu v kapitole o indukci ještě vrátíme. V této větě jsme dokazovali rovnost dvou výrazů. Vyšli jsme ze součtu členů a došli k jednoduššímu vzorci. Při takovém důkazu musíme dávat pozor na to, aby všechny úpravy, které provádíme, byly ekvivalentní neboli fungovaly oběma směry. Takovýmto způsobem je odvozována většina vzorců, které se učí na středních školách.

Definice 4. *Kombinační číslo* $\binom{n}{k}$ *je číslo, které je dáno vzorcem*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!},$$

kde $n, k \in \mathbb{N}_0$ *a* $k \leq n$. *Symbol* ! *představuje faktoriál. Faktoriál čísla* n *je součin všech přirozených čísel menších nebo rovných* n, *tedy*

$$n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1.$$

Definujeme též $0! = 1$. [Pol72, str. 255.]

Věta 4. *Pro všechna* $n, k \in \mathbb{N}_0$, $n > k$, *platí*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

[Pol72, str. 255.]

Důkaz. Dokazujeme rovnost dvou výrazů, proto vyjdeme z jedné strany rovnosti a ekvivalentními úpravami dojdeme ke druhé straně rovnosti.

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k+1)!\,(n-k-1)!} \\
&= \frac{n!}{\frac{k+1}{k+1}\,k!\,(n-k)!} + \frac{n!}{(k+1)!\frac{n-k}{n-k}(n-k-1)!} \qquad k+1 \neq 0 \wedge \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad n-k \neq 0 \\
&= \frac{(k+1)n!}{(k+1)!\,(n-k)!} + \frac{(n-k)n!}{(k+1)!(n-k)!} \\
&= \frac{n!\,(k+1+n-k)}{(k+1)!\,(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!\,(n-k)!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

□

Postup důkazu věty 4 se shoduje s postupem důkazu věty 3. Všimněte si, že jsme v důkazu v jednom okamžiku přidali dělení výrazy $k + 1$ a $n - k$. Pokud by tyto výrazy byly rovny nule, nebyly by tyto úpravy ekvivalentní, avšak z požadavků věty na k a na n vidíme, že tyto výrazy rovny nule být nemohou. Proto jsme si mohli tuto úpravu v důkazu dovolit použít s tím, že jsme tam skutečnost, že se tyto výrazy nule nerovnají, napsali, abychom na to kohokoliv, kdo po nás bude důkaz číst, upozornili.

Definice 5. *Ciferný součet přirozeného čísla je součet číslic tohoto čísla v desítkové soustavě.* [OK04, str. 18.]

Věta 5. *Přirozené číslo n je dělitelné třemi právě tehdy, je-li třemi dělitelný jeho ciferný součet.* [BC09, str. 106.]

Důkaz. Jedná se o ekvivalenci, musíme tedy dokázat implikaci oběma směry.

1) Je-li přirozené číslo n dělitelné třemi, je dělitelný třemi i jeho ciferný součet.
Každé k-ciferné přirozené číslo n můžeme rozepsat ve tvaru

$$n = n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \cdots + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

kde n_0 až n_k jsou jeho cifry označované zprava. Toto vyjádření upravíme na

$$n = n_k\cdot(10^k-1+1)+n_{k-1}\cdot(10^{k-1}-1+1)+\cdots+n_1\cdot(10^1-1+1)+n_0\cdot(10^0-1+1).$$

Závorky částečně roznásobíme a přeskupíme jednotlivé členy. Dostaneme tvar

$$n = n_k + \cdots + n_0 + n_k \cdot (10^k - 1) + \cdots + n_1 \cdot (10^1 - 1).$$

Výrazy v závorkách můžeme upravit do podoby, ze které bude zřejmá jejich dělitelnost třemi. Úpravou získáme

$$n = n_k + \cdots + n_0 + n_k \cdot (9 \cdot 10^{k-1} + \cdots + 9) + \cdots + n_1 \cdot (9).$$

V tomto tvaru již můžeme nahlédnout, že výrazy v závorkách jsou součty násobků devíti, tedy výrazy v závorkách jsou dělitelné třemi. Také po přenásobení ciframi čísla n a následném sečtení těchto součinů dostáváme číslo dělitelné třemi. Vyjdeme-li z předpokladu, že n je dělitelné třemi, pak pravá strana rovnosti také musí být dělitelná třemi, tedy výraz $n_k + \cdots + n_0$, což je ciferný součet čísla n, musí také být dělitelný třemi. Tím je dokázána implikace zleva doprava.

2) Je-li ciferný součet přirozeného čísla n dělitelný třemi, pak je třemi dělitelné i n.
Jelikož byly úpravy provedené v první části důkazu ekvivalentní, můžeme opět tvrdit, že platí

$$n = n_k + \cdots + n_0 + n_k \cdot (9 \cdot 10^{k-1} + \cdots + 9) + \cdots + n_1 \cdot (9).$$

Vyjdeme-li nyní z předpokladu, že je ciferný součet přirozeného čísla n dělitelný třemi, pak je i celý součet na pravé straně rovnosti dělitelný třemi, a proto musí být třemi dělitelné i n.
Jelikož byly dokázány implikace oběma směry, je dokázána původní věta. □

Každou ekvivalenci dokazujeme jako implikaci zleva doprava a implikaci zprava doleva, jako je tomu ve větě 5. V této větě již musíme hodně argumentovat, nestačí pouze dokázat jednoduchou vlastnost či rovnost. Každý argument musí být podložen nějakým faktem, který už známe. Tím může být definice nebo již dokázaná věta či lemma. Také se můžeme opírat o axiomy, ale jelikož se budeme zabývat větami „hluboko“ v matematice, nebudeme axiomy využívat.

Lemma 2. *Pro všechna x a $y \in \mathbb{R}$ platí následující rovnosti:*

$$\begin{aligned} &(i) && \sin(x+y) = \sin x \cos y + \sin y \cos x, \\ &(ii) && \cos(x+y) = \cos x \cos y - \sin x \sin y, \\ &(iii) && \sin^2 x + \cos^2 x = 1. \end{aligned}$$

[Smý15, str. 11 a 52.]

Věta 6. *Pro všechna* $x \in \mathbb{R}$ *platí* $\sin 3x = 3\sin x - 4\sin^3 x$. [Smý15, str. 133.]

Důkaz. Opět dokazujeme rovnost výrazů. Vyjdeme z levé strany rovnosti a ekvivalentními úpravami vyvodíme stranu pravou. Úpravy provádíme na základě lemmatu 2.

$$\begin{aligned}
\sin 3x &= \sin(2x + x) \\
&= \sin 2x \cos x + \sin x \cos 2x \\
&= (\sin x \cos x + \sin x \cos x)\cos x + \sin x(\cos x \cos x - \sin x \sin x) \\
&= 2\sin x \cos^2 x + \sin x \cos^2 x - \sin^3 x \\
&= 3\sin x \cos^2 x - \sin^3 x \\
&= 3\sin x(1 - \sin^2 x) - \sin^3 x \\
&= 3\sin x - 4\sin^3 x
\end{aligned}$$

□

2.3 Důkaz sporem

Princip důkazu sporem

Důkaz sporem spočívá v tom, že ukážeme, že negace dokazované věty neplatí, tedy musí platit věta samotná.

Máme-li výrok V, použijeme jeho negaci $\neg$V jako předpoklad V_0 a dále postupujeme stejně jako u důkazu přímého. Podaří-li se nám pravdivými implikacemi odvodit nějaký výrok, o kterém víme, že není pravdivý, pak dle pravidla modus tollens nemůže náš předpoklad V_0 platit, musí tedy platit jeho negace neboli dokazovaný výrok V.

Nepravdivý výrok, který odvodíme, může být buď nějaká předchozí znalost, nebo také samotná dokazovaná věta, jelikož na začátku důkazu sporem předpokládáme, že je pravdivá její negace. [GT96, str. 173.]

Věty dokázané sporem

Definice 6. *Liché číslo je takové číslo* n*, které lze vyjádřit jako* $n = 2k - 1$*, kde* k *je celé číslo.* [OK04, str. 18.]

Věta 7. *Všechny dělitele lichého čísla jsou lichá čísla.*

Důkaz. Pro důkaz sporem uděláme negaci věty: Existuje dělitel lichého čísla, která je sudý. Tento výrok bereme jako náš výchozí předpoklad.
Nechť m je sudý dělitel libovolného lichého čísla n. Pak lze psát $n = m \cdot k$, kde k je nějaké přirozené číslo. Jelikož je m sudé, platí $m = 2 \cdot l$, kde l je nějaké přirozené číslo. Dosazením do vyjádření n dostáváme $n = 2 \cdot l \cdot k$. Jelikož $l \cdot k$ je opět přirozené číslo, splňuje n definici sudého čísla, je tedy sudé. To je spor s předpokladem, že n je liché. Negace dokazované věty neplatí, musí tedy platit věta samotná. □

Všimněte si, že jsme negaci věty 7 dokazovali přímým způsobem. Důkaz sporem se tedy od přímého důkazu liší pouze v prvním kroku – musíme utvořit negaci dokazované věty. To může být mnohdy nesnadné a je důležité neudělat v negaci chybu.

Definice 7. *<u>Druhá odmocnina</u> z nezáporného reálného čísla x je takové nezáporné reálné číslo $\sqrt{x}$, pro které platí $\sqrt{x} \cdot \sqrt{x} = x$.* [OK04, str. 59.]

Definice 8. *<u>Racionální číslo</u> je takové číslo, které lze vyjádřit jako podíl $\frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$ a p a q jsou nesoudělná. Čísla, která takto vyjádřit nelze, nazýváme <u>iracionální</u>.* [BC09, str. 18.]

Lemma 3. *Pro každé přirozené číslo n platí, že, pokud je n^2 dělitelné prvočíslem p, je tímto prvočíslem dělitelné také n.*

Věta 8. *$\sqrt{2}$ je iracionální číslo.* [Blo00, str. 71.]

Důkaz. Větu dokážeme sporem, tedy z negace věty vyvodíme spor.
Předpokládejme, že $\sqrt{2}$ je racionální číslo. Pak lze vyjádřit jako podíl $\sqrt{2} = \frac{p}{q}$, kde p a q jsou navzájem nesoudělná přirozená čísla a q ani p nejsou nula. Jelikož je q nenulové číslo, můžeme jím rovnost vynásobit a posléze rovnost umocnit na druhou. Dostaneme $2q^2 = p^2$. Jelikož je levá strana dělitelná dvěma, musí být rovněž pravá strana dělitelná dvěma. A jelikož p^2 je dělitelné dvěma, pak i p je dělitelné dvěma (lemma 3). Platí tedy, že $p = 2r$, kde r je nějaké přirozené číslo. Platí tedy $2q^2 = 4r^2$, neboli $q^2 = 2r^2$. Z této rovnosti plyne, že q^2 je dělitelné 2, tedy q je dělitelné 2. Odvodili jsme, že p i q jsou obě dělitelná dvěma, což je ovšem spor s tím, že p a q jsou nesoudělná. Náš původní předpoklad, že $\sqrt{2}$ je racionální, je tedy nesprávný, a proto je $\sqrt{2}$ iracionální číslo. □

Věta 8 je velmi oblíbenou příkladovou větou pro důkaz sporem a je tedy žádoucí, aby byla prezentována žákům středních škol. Často je v této větě ovšem opomíjena důležitost lemmatu 3, bez kterého by věta nešla takto dokázat.

Definice 9. *Čtvercové číslo* *je* n^2, *kde* n *je přirozené číslo.*

Lemma 4. *Nechť* $n \in \mathbb{N}$. *Je-li* n^2 *liché, pak je liché i* n.

Věta 9. *Neexistuje žádné čtvercové číslo* n^2 *ve tvaru* $n^2 = 8k + 5$, $k \in \mathbb{N}_0$.

Důkaz. Pro důkaz sporem předpokládejme, že existují n a k z přirozených čísel taková, že $n^2 = 8k + 5$. Pravá strana je lichá, podle lemmatu 4 je liché i n. Můžeme tedy psát $n = 2m - 1$, kde m je přirozené číslo. Dosazením získáme

$$\begin{aligned} n^2 &= 8k + 5, \\ (2m - 1)^2 &= 8k + 5, \\ 4m^2 - 4m + 1 &= 8k + 5, \\ 4(m^2 - m - 1) &= 8k, \\ m^2 - m - 1 &= 2k, \\ m(m - 1) - 1 &= 2k. \end{aligned}$$

Pro každé přirozené m je buď m nebo $m - 1$ sudé číslo, proto je levá strana rovnosti lichá. Obdobně pro každé přirozené k je $2k$ sudé, proto je pravá strana rovnosti sudá. Z toho plyne, že liché číslo se rovná sudému, což je spor. □

Výhoda věty 9 spočívá v tom, že se snadno přeformuluje do podobných tvrzení, která se můžeme pokoušet dokázat. Místo dvojice čísel 8 a 5 ve znění této věty můžeme nahradit nějakou jinou dvojicí přirozených čísel a pokusit se dokázat či vyvrátit platnost tohoto nového tvrzení.

Věta 10. *Žádné z čísel* $11, 111, 1111, \ldots$ *není čtvercové.* [PÓL09, str. 8.]

Důkaz. Předpokládejme, že nějaké z čísel 11, 111, 1111, ... je čtvercové. Nechť je to číslo $11\ldots11$. Jelikož číslo $11\ldots11$ končí číslicí 1, musí jeho odmocnina končit buď číslicí 1, nebo 9. Pak existuje $k \in \mathbb{N}$ takové, že platí

$$\begin{aligned} 11\ldots11 &= (10k \pm 1)^2, \\ 11\ldots11 &= 100k^2 \pm 20k + 1, \\ 11\ldots10 &= 100k^2 \pm 20k, \\ 11\ldots1 &= 10k^2 \pm 2k. \end{aligned}$$

Pro libovolné přirozené k je výraz na pravé straně sudý, ovšem $11\cdots1$ je liché, což je spor. □

Ve větě 10 by nejspíš bylo vhodné rozdělit důkaz na dvě části – pro $(10k-1)$ a $(10k+1)$ zvlášť, toto zkracování je ovšem běžné, proto je zde uvedeno v této formě. Podobný důkaz by se dal také použít při důkazu silnějšího tvrzení, že žádné přirozené číslo, jehož poslední dvojčíslí je 11, není čtvercové.

Lemma 5 (základní věta aritmetiky)**.** *Každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel.* [Edw08, str. 34].

Věta 11. *Prvočísel je nekonečně mnoho.* [Ecc97, str. 285.]

Důkaz. Opět budeme pro důkaz sporem uvažovat, že platí negace dokazované věty. Vyjdeme z předpokladu, že prvočísel je konečně mnoho. Můžeme tedy všechna prvočísla vypsat do seznamu $p_1 = 2, p_2 = 3, \ldots, p_{n-1}, p_n$, kde n je počet prvočísel. Vytvořme nyní číslo a jako součin

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot p_n.$$

Potom číslo $a+1$ dává po dělení libovolným z vypsaných n prvočísel zbytek 1. Číslo $a+1$ musí být dle základní věty aritmetiky (lemma 5) dělitelné nějakým prvočíslem, které nemáme na seznamu. To je spor s tím, že náš seznam obsahoval všechna prvočísla. □

Věta 11 je další oblíbenou větou na středních školách, které se důkazy zabývají. Častou chybou bývá, že se o čísle $a+1$ řekne, že musí být novým prvočíslem, to ovšem není pravda, například $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 509 \cdot 59$, ovšem 59 i 509 nová prvočísla jsou.

2.4 Důkaz pomocí obměněné implikace

Princip důkazu pomocí obměněné implikace

V sekci 2.1 jsme se zmínili o obměněné implikaci. Implikace $\mathrm{V}_1 \Rightarrow \mathrm{V}_2$ je ekvivalentní s její obměněnou implikací $\neg\mathrm{V}_2 \Rightarrow \neg\mathrm{V}_1$. Chceme-li dokázat implikaci $\mathrm{V}_1 \Rightarrow \mathrm{V}_2$, stačí, když dokážeme její obměněnou implikaci. Výhodou tohoto postupu bývá snazší dokazatelnost obměněné implikace. Tu pak dokážeme buď přímo, nebo pomocí jiné dokazovací metody. [GT96, str. 167–168.]

Věty dokázané pomocí obměněné implikace

Věta 12. *Nechť n je přirozené číslo. Pokud n^2 je liché, pak n je liché.*

Důkaz. Tuto větu nejsnadněji dokážeme obměněnou implikací. Pokud n není liché, pak není liché ani n^2. Jelikož je n přirozené číslo, je toto vyjádření ekvivalentní s větou, je-li n sudé, pak n^2 je také sudé. Dostáváme větu ve formě implikace, kterou dokážeme přímo. Předpokládejme, že n je sudé. Pak existuje přirozené m takové, že $n = 2m$. Tedy

$$n^2 = (2m)^2 = 4m^2 = 2(2m^2),$$

kde $2m^2$ je přirozené číslo, což znamená, že n^2 je sudé, tedy není liché a obměněná implikace byla dokázána. □

Větu 12 už jsme v podstatě dokázali společně s větou 7, ovšem kdybychom tuto větu neměli dokázanou, větu 12 bychom museli dokázat zvlášť výše uvedeným způsobem. Obměněná implikace této věty je také méně obecnou verzí lemmatu 3.

Podobně jako u důkazu sporem se důkaz pomocí obměněné implikace od přímého důkazu liší pouze svým začátkem. Na rozdíl od důkazu sporem se ovšem nepokoušíme dokázat negaci, přestože to tak může na první pohled vypadat. Obměněná implikace sice využívá negovaných výroků, je ovšem ekvivalentní s implikací původní. Větu tedy pouze trochu pozměníme a následně dokazujeme přímo. Jelikož jsou důkaz sporem a důkaz pomocí obměněné implikace tolik podobné důkazu přímému, avšak jsou jistým způsobem převrácené, říká se těmto metodám důkaz nepřímý.

Definice 10. *Říkáme, že $f(x)$ je lichá funkce, pokud pro všechna reálná x platí: pokud je x v definičním oboru $f(x)$, pak i $-x$ je v jejím definičním oboru a platí $f(-x) = -f(x)$.* [Odv93, str. 50.]

Věta 13. *Pokud funkce $f(x)$ spojitá na $(-a, a), a \in \mathbb{R}^+$ neprochází počátkem, pak není lichá.*

Důkaz. Dokážeme obměněnou implikaci. Pokud je $f(x)$ lichá, pak prochází počátkem nebo není spojitá na $(-a, a), a \in \mathbb{R}^+$. Vyjdeme z předpokladu, že $f(x)$ je lichá. Platí tedy, že $f(-x) = -f(x)$ pro všechna x z definičního oboru $f(x)$. Pro $x = 0$ nastávají dvě možnosti:
1) buď $f(0) = -f(0)$, neboli $f(0) = 0$; nebo
2) $f(0)$ není definováno.
První případ znamená, že $f(x)$ prochází počátkem, druhý případ znamená, že $f(x)$ není spojitá na $(-a, a), a \in \mathbb{R}^+$. □

Všimněte si, že věta 13 je ve tvaru $(\mathrm{V}_1 \wedge \mathrm{V}_2) \Rightarrow \mathrm{V}$, její obměněná implikace je tedy ve tvaru $\neg\mathrm{V} \Rightarrow (\neg\, \mathrm{V}_1 \vee \neg\, \mathrm{V}_2)$.

2.5 Důkaz indukcí

Princip důkazu indukcí

Matematická indukce je metoda, která se využívá při dokazování vět s univerzálním kvantifikátorem, které mají platit pro všechna přirozená čísla rovna n_0 nebo vyšší, kde n_0 je přirozené číslo. Důkaz matematickou indukcí provádíme tak, že zjistíme, jestli výrok V platí pro nejmenší přirozené číslo, o kterém věta hovoří. Tomuto říkáme *první krok*. Dále zavedeme *indukční předpoklad* (v důkazu často zkracováno jako IP), že výrok V platí pro libovolně zvolené přirozené k. Následuje *indukční krok*, ve kterém dokážeme, že na základě platnosti pro k musí výrok V platit i pro $k+1$. Tím je věta dokázána.

Pokud platí první i indukční krok, platí celá věta. Z platnosti věty pro $n = n_0$ plyne platnost věty i pro $n = n_0 + 1$. A jelikož platí pro $n = n_0 + 1$, musí platit i pro $n = n_0 + 1 + 1 = n_0 + 2$. Takto bychom mohli pokračovat k libovolně velkému n většímu než n_0. Jelikož věta platí pro libovolné n od n_0 výše, můžeme říct, že platí pro všechna n z přirozených čísel větších nebo rovných n_0. [GT96, str. 239–243 a 252.]

Důkaz indukcí musí obsahovat všechny tři důležité části – první krok, indukční předpoklad a indukční krok. Všechny tyto prvky musí být v důkazu explicitně napsané.

Věty dokázané indukcí

Věta 14. *Součet prvních n přirozených čísel je dán vzorcem*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

[Pol72, str. 241.]

Důkaz. Věta se vztahuje k přirozeným číslům, nabízí se ji dokázat indukcí. Provedeme tři kroky důkazu indukcí.

(1) Dokážeme, že rovnost platí pro nejmenší přirozené číslo, na které se věta vztahuje.

Pro $n = 1$ je součet roven 1. Dosazením do vzorce dostaneme $\frac{1(1+1)}{2} = 1$. Rovnost je tedy pro $n = 1$ splněna.
(2) Předpokládejme, že vzorec

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

platí pro $n \in \{1, 2, \ldots, k\}$, kde $k \in \mathbb{N}$.
(3) Dokážeme, že z platnosti vzorce pro $n = k \in \mathbb{N}$ plyne platnost vzorce pro $n = k + 1$. Chceme odvodit

$$1 + 2 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2},$$

což provedeme následujícím způsobem.

$$\begin{aligned} 1 + 2 + \ldots + k + (k+1) &\overset{\text{IP}}{=} \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k^2+k}{2} + \frac{2k+2}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Tedy věta platí pro $n = 1$ a, pokud platí pro k, platí pro každé $k + 1$. Tedy věta platí pro každé $n \in \mathbb{N}$. □

U důkazu indukcí je velmi důležité zapsat všechny tři kroky. Bez libovolného z nich totiž důkaz není úplný. Často se stává, že je opomíjen krok druhý, ten je ovšem předpokladem v kroku třetím. Také je důležité si uvědomit, na které nejmenší číslo se věta vztahuje.

Ve třetím kroku důkazu vždy využíváme indukční předpoklad. Je zvykem označovat krok, ve kterém je tento předpoklad využit, nápisem IP nad znaménko rovnosti, jako je tomu v prvním kroku tohoto důkazu.

Věta 15 (lemma 1)**.** *Pro n-tý člen geometrické posloupnosti platí*

$$a_n = a_1 \cdot q^{n-1}.$$

[Pol72, str. 313.]

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 1$ je levá strana rovna a_1 a pravá strana rovna $a_1 \cdot q^{1-1} = a_1$. Pro $n = 1$ tedy rovnost platí.
(2) Předpokládejme, že $a_n = a_1 \cdot q^{n-1}$ platí pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$.
(3) Dokážeme, že platnost pro $n = k$ implikuje platnost pro $n = k + 1$. Chceme dokázat, že $a_{k+1} = a_1 \cdot q^k$.

$$\begin{aligned} a_{k+1} &= a_k \cdot q && \text{(Z definice 3)} \\ &\overset{\text{IP}}{=} a_1 \cdot q^{k-1} \cdot q \\ &= a_1 \cdot q^k \end{aligned}$$

Věta platí pro $n = 1$ a platnost pro k implikuje platnost pro $k+1$, tedy věta platí pro všechna $n \in \mathbb{N}$. □

Ve třetím kroku důkazu indukcí většinou postupujeme obdobně jako u důkazu rovnosti přímým důkazem. Je tedy nutné zajistit, aby prováděné úpravy byly ekvivalentní.

Věta 16. *Pro každé přirozené n je výraz $7^n - 1$ dělitelný 6.*

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 1$ je výraz roven $7^1 - 1 = 6$, což 6 dělitelné je.
(2) Nechť výraz $7^n - 1$ je dělitelný 6 pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$, tedy $7^n - 1 = 6 \cdot m$, kde m je nějaké přirozené číslo.
(3) Použitím indukčního předpokladu chceme dokázat, že výraz $7^{k+1} - 1$ je dělitelný 6.

$$\begin{aligned} 7^{k+1} - 1 &= 7^k \cdot 7 - 1 \\ &= 7^k \cdot (6 + 1) - 1 \\ &= 7^k \cdot 6 + 7^k - 1 \\ &\overset{\text{IP}}{=} 7^k \cdot 6 + 6 \cdot m \\ &= 6 \cdot (7^k + m). \end{aligned}$$

Jelikož je součet $7^k + m$ nějaké přirozené číslo, vyjadřuje poslední řádek nějaký násobek 6. Tedy $7^{k+1} - 1$ je dělitelné 6.
Tvrzení platí pro $n = 1$ a z platnosti pro k plyne platnost pro $k + 1$, proto věta platí pro všechna $n \in \mathbb{N}$. □

Věta 16 je dalším příkladem věty, která se dá snadno přetvořit v podobné, snadno dokazatelné, či vyvratitelné tvrzení.

Věta 17. *Pro každé $n \in \mathbb{N}_0$ platí*
$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$
[Blo00, str. 314.]

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 0$ je levá strana $\binom{0}{0} = 1$ a pravá strana $2^0 = 1$. Pro $n = 0$ je rovnost splněna.
(2) Nechť rovnost
$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$
platí pro $n \in \{0, 1, 2, \ldots, k\}, k \in \mathbb{N}_0$.
(3) Dokažme, že platnost pro $n = k$ implikuje platnost pro $n = k + 1$. Chceme ukázat, že
$$\binom{k+1}{0} + \binom{k+1}{1} + \cdots + \binom{k+1}{k} + \binom{k+1}{k+1} = 2^{k+1}.$$

Pomocí věty 4 přepíšeme všechny kromě dvou krajních členů na součet dvou menších kombinačních čísel. Jelikož jsou krajní členy rovny 1, můžeme je přepsat pomocí jiného kombinačního čísla. Uzávorkování zde slouží pro lepší přehlednost, jak jednotlivé členy vznikly.
$$\begin{aligned}
&\binom{k+1}{0} + \binom{k+1}{1} + \binom{k+1}{2} + \\
&\cdots + \binom{k+1}{k-1} + \binom{k+1}{k} + \binom{k+1}{k+1} \\
&= \binom{k}{0} + \left[\binom{k}{0} + \binom{k}{1}\right] + \left[\binom{k}{1} + \binom{k}{2}\right] + \\
&\cdots + \left[\binom{k}{k-2} + \binom{k}{k-1}\right] + \left[\binom{k}{k-1} + \binom{k}{k}\right] + \binom{k}{k} \\
&= 2 \cdot \left[\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-2} + \binom{k}{k-1} + \binom{k}{k}\right] \\
&\overset{\text{IP}}{=} 2 \cdot 2^k = 2^{k+1}.
\end{aligned}$$

Tvrzení platí pro $n = 0$ a z platnosti pro k plyne platnost pro $k + 1$, proto věta platí pro všechna $n \in \mathbb{N}_0$. □

Je vhodné zde upozornit, že zápisy $1 + 2 + \cdots + (k - 1) + k$ a jemu podobné nejsou vhodnou zkratkou při formulování důkazů. Pro takovýto součet se využívá sumační znak Σ. Například součet prvních n přirozených čísel bychom zapsali

$$\sum_{i=1}^{n} i.$$

Tento zápis nám říká, že máme sčítat výraz i, kde za i postupně dosazujeme čísla od 1 do n.

Lemma 6. *Pro všechna $x, y \in \mathbb{R}$ platí následující vlastnosti:*

$$\begin{array}{ll} (i) & |x + y| \leq |x| + |y|; \\ (ii) & |x \cdot y| = |x| \cdot |y|. \end{array}$$

[Pol72, str. 30.]

Věta 18. *Pro všechna $x \in \mathbb{R}$ a všechna $n \in \mathbb{N}$ platí $|\sin nx| \leq n|\sin x|$.* [Ped94, str. 7.]

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 1$ nabývá nerovnost tvaru $|\sin x| \leq |\sin x|$, což zřejmě platí.
(2) Nechť platí $|\sin nx| \leq n|\sin x|$ pro $n \in \{1, 2, \cdots, k\}, k \in \mathbb{N}$.
(3) Chceme dokázat, že platí $|\sin(k + 1)x| \leq (k + 1)|\sin x|$.

$$\begin{aligned} |\sin(k+1)x| &= |\sin kx \cos x + \cos kx \sin x| && \text{(dle lemmatu 2)} \\ &\leq |\sin kx||\cos x| + |\cos kx||\sin x| && \text{(dle lemmatu 6)} \\ &\leq |\sin kx| + |\sin x| && (\forall x \in \mathbb{R} : |\cos x| \in [0, 1]) \\ &\overset{\text{IP}}{\leq} k|\sin x| + |\sin x| \\ &= (k + 1)|\sin x|. \quad \forall x \in \mathbb{R} \end{aligned}$$

Tvrzení platí pro $n = 1$ a z platnosti pro k plyne platnost pro $k + 1$, proto věta platí pro všechna $n \in \mathbb{N}$. □

Věta 18 je zajímavá tím, že pracuje s nerovnostmi. Pokud začínáme s tou stranou nerovnosti, která má být menší, můžeme výraz na druhé straně libovolně zvětšovat, dokud se nedostaneme ke kýženému závěru. Nesmíme ovšem v žádném kroku výraz zmenšit, jelikož bychom nevyužili tranzitivity nerovnosti menší nebo rovno (tranzitivita znamená, že, je-li $x \leq y$ a $y \leq z$, pak je $x \leq z$).

2.6 Další dokazovací metody

Důkaz uvedením příkladu

Také zvána konstrukční důkaz, metoda důkazu uvedením příkladu je vhodná pro důkaz věty, která obsahuje existenční kvantifikátor. Taková věta tvrdí, že existuje nějaký prvek s jistou vlastností. V některých případech může být nejjednodušší takový prvek prostě uvést nebo ukázat, jak je možné jej zkonstruovat.

Pokud tvrzení ještě není dokázané, není větou, ale hypotézou. V takovém případě můžeme hypotézu vyvrátit také nalezením protipříkladu. Taková hypotéza musí obsahovat univerzální kvantifikátor. Vyvrácením této hypotézy v podstatě dokazujeme její negaci, tedy tvrzení, které obsahuje kvantifikátor existenční. Jedná se tedy také o důkaz uvedením příkladu. [GT96, str. 186]

Věta 19. *Existují přirozená čísla a, b tak, že $32a + 21b$ je čtvercové číslo.*

Důkaz. Nechť $a = 8$ a $b = 5$. Pak $32a + 21b = 32 \cdot 8 + 21 \cdot 5 = 256 + 105 = 361 = 19^2$ a je čtvercové číslo. □

Lemma 7. *Pro každá dvě různá reálná čísla x a $y, x < y$, platí $\frac{x+y}{2} \in (x, y)$.*

Věta 20. *Mezi každými dvěma různými racionálními čísly je další racionální číslo.* [PED94, str. 20.]

Důkaz. Nechť x a y jsou dvě různá racionální čísla. Pak číslo $\frac{x+y}{2}$ je racionální a leží mezi nimi (dle lemmatu 7). □

Je pravda, že věta 20 a lemma 7 jsou v opačném pořadí, než v jakém by byly normálně odvozovány, ovšem pro účely tohoto textu je toto pořadí vyhovující.

Definice 11. *<u>Čtvercovou maticí řádu 2</u> budeme rozumět čtvercové schéma*

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix},$$

kde $a_{i,j} \in \mathbb{R}$ pro každé $i, j \in \{1, 2\}$. [BEČ05, str. 32.]

Definice 12. *Násobení čtvercových matic řádu* 2 *je definováno následovně. Nechť A a B jsou čtvercové matice $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ a $B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$, pak jejich součin je*

$$A \cdot B = \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} & a_{2,1}b_{1,2} + a_{2,2}b_{2,2} \end{pmatrix}.$$

[Beč05, str. 33.]

Věta 21. *Násobení čtvercových matic řádu* 2 *není komutativní, tedy obecně $A \cdot B \neq B \cdot A$, jsou-li A a B libovolné čtvercové matice řádu* 2. [Beč05, str. 34.]

Důkaz. Nechť $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ a $B = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Pak

$$A \cdot B = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1+2 & 1+4 \\ 3+1 & 3+2 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 4 & 5 \end{pmatrix}, \text{ ale}$$

$$B \cdot A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1+3 & 2+1 \\ 1+6 & 2+2 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 7 & 4 \end{pmatrix}.$$

Jelikož $\begin{pmatrix} 3 & 5 \\ 4 & 5 \end{pmatrix} \neq \begin{pmatrix} 4 & 3 \\ 7 & 3 \end{pmatrix}$, pak obecně $A \cdot B \neq B \cdot A$. □

Definice 11 a 12 a věta 21 jsou zjednodušeními svých obecných verzí, které se vyučují na vysokých školách. Tento důkaz však bude relevantní i pro obecně definované matice. Je tedy užitečné umět přemýšlet o jednoduchých důkazech i při dokazovaní na první pohled složitých matematických tvrzení.

Důkaz rozborem možností

Někdy je vhodné větu, která hovoří o nějaké množině objektů, rozdělit na několik snadněji dokazatelných vět, z nichž každá má za objekt zájmu jen část z objektů, o kterých hovoří původní věta. Dohromady musí tyto věty být ekvivalentní s větou původní, nesmíme tedy žádný objekt opomenout (jinak řečeno sjednocení množin objektů „podvět“ musí být rovno množině objektů původní věty). [GT96, str. 262–265.]

Příkladem mohou být věty, které mluví o vlastnostech všech celých čísel. Takovou větu můžeme rozdělit na tři, které se budou týkat postupně kladných celých čísel, nuly a záporných celých čísel. Větu o přirozených číslech můžeme rozdělit na větu o sudých a větu o lichých číslech.

Věta 22. *Nechť $n \in \mathbb{N}_0$ je čtvercové číslo. Pak $n = 3k$ nebo $n = 3k + 1$, kde $k \in \mathbb{N}_0$.* [Ecc97, str. 197.]

Důkaz. Věta je ve tvaru implikace, dokážeme ji přímo. Abychom si pomohli, rozdělíme důkaz na tři části.
Číslo n je čtvercové, existuje tedy m tak, že $n = m^2$. Číslo m může po dělení třemi dávat zbytek 0, 1, nebo 2. Podle těchto možností důkaz rozdělíme.

a) Nechť $m = 3l$, kde l je nějaké přirozené číslo. Pak $n = m^2 = (3l)^2 = 3(3l^2)$. Jelikož je $3l^2$ přirozené číslo, je $n = 3k$, kde k je nějaké přirozené číslo.

b) Nechť $m = 3l+1$, kde l je nějaké přirozené číslo. Pak $n = m^2 = (3l+1)^2 = 3(3l^2 + 2l) + 1$. Jelikož je $3l^2 + 2l$ přirozené číslo, je $n = 3k + 1$, kde k je nějaké přirozené číslo.

c) Nechť $m = 3l+2$, kde l je nějaké přirozené číslo. Pak $n = m^2 = (3l+2)^2 = 3(3l^2 + 4l + 1) + 1$. Jelikož je $3l^2 + 4l + 1$ přirozené číslo, je $n = 3k + 1$, kde k je nějaké přirozené číslo. □

Tato metoda se dá uplatnit v kombinaci s jakoukoliv jinou dokazovací metodou.

3 Cvičné úlohy

V první části této kapitoly jsou uvedena jednoduchá cvičení, která mají procvičit práci s logickými spojkami a výroky. Dále jsou zde také obsažena cvičení, která jsou svým způsobem důkazy k logickému pozadí některých důkazových metod.

Druhá část obsahuje množství jednoduchých i pokročilých tvrzení, která je ovšem možno snadno dokázat. Vyskytují se zde věty matematiky základní i střední školy, některé věty také zasahují do matematiky vysokoškolské.

Poslední sekce se věnuje chybným důkazům. Zde uvedené důkazy mohou být provedeny nevhodným způsobem nebo obsahovat faktické chyby či nepřesnosti.

Řešení všech úloh jsou uvedena v další kapitole.

3.1 Logika

Cvičení 1

Doplňte pravdivostní hodnoty spojených a negovaných výroků v tabulce 3.1 a přesvěčte se, že implikace $\mathrm{V}_1 \Rightarrow \mathrm{V}_2$ je ekvivalentní s její obměněnou implikací $\neg\mathrm{V}_2 \Rightarrow \neg\mathrm{V}_1$.

$\mathrm{P}(\mathrm{V}_1)$	$\mathrm{P}(\mathrm{V}_2)$	$\mathrm{P}(\neg\mathrm{V}_1)$	$\mathrm{P}(\neg\mathrm{V}_2)$	$\mathrm{P}(\mathrm{V}_1 \Rightarrow \mathrm{V}_2)$	$\mathrm{P}(\neg\mathrm{V}_2 \Rightarrow \neg\mathrm{V}_1)$
1	1				
1	0				
0	1				
0	0				

Tabulka 3.1: Pravdivostní hodnota implikace a obměněné implikace

Cvičení 2

Doplňte pravdivostní hodnoty spojených a negovaných výroků v tabulkách 4.2 až 4.4 a ověřte, že výroky uvedené v pravých dvou sloupcích tabulek si jsou navzájem negacemi.

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \wedge V_2)$	$P(\neg V_1 \vee \neg V_2)$
1	1				
1	0				
0	1				
0	0				

Tabulka 3.2: Pravdivostní hodnota negace konjunkce

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \vee V_2)$	$P(\neg V_1 \wedge \neg V_2)$
1	1				
1	0				
0	1				
0	0				

Tabulka 3.3: Pravdivostní hodnota negace disjunkce

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \Rightarrow V_2)$	$P(V_1 \wedge \neg V_2)$
1	1				
1	0				
0	1				
0	0				

Tabulka 3.4: Pravdivostní hodnota negace implikace

Cvičení 3

Znegujte následující výroky. Výroky nedokazujte.

V_1: „Číslo a je přirozené a dělitelné třemi nebo čtyřmi.“
V_2: „Je-li trojúhelník ABC pravoúhlý a rovnoramenný, pak není rovnostranný.“
V_3: „Funkce f je lichá nebo, pokud je spojitá, prochází bodem [0, 0].“
V_4: „Libovolný rovinný útvar je kružnice nebo je pravoúhlý a konvexní.“
V_5: „Existuje reálné číslo, které, pokud není menší než 5, je dokonalé, pokud je sudé.“

3.2 Důkazové metody

Dokažte následující věty vhodnou metodou. K důkazu vět využijte definice, věty a lemmata z kapitoly 2.

Věta 23. $\sqrt{3}$ *je iracionální číslo.*

Věta 24. 25 *je čtvercové číslo.*

Věta 25. *Pro všechna* $x \in \mathbb{R}$ *platí* $\cos 3x = -3\cos x + 4\cos^3 x$. [Smý15, str. 133.]

Věta 26. *Přirozené číslo n je dělitelné čtyřmi právě tehdy, je-li jeho poslední dvojčíslí dělitelné čtyřmi.* [BC09, str. 105.]

Věta 27. *Nechť n je přirozené číslo. Pokud je* n^2 *sudé, pak n je sudé.* [Hyu18, str. 1.]

Věta 28. *Jediná trojice po sobě jdoucích přirozených čísel* a, b, c*, která splňují rovnost* $a^2 + b^2 = c^2$*, je trojice* $3, 4, 5$. [Blo00, str. 69.]

Věta 29. *Pro všechna* $n, k \in \mathbb{N}_0$*,* $n > k$*, platí*

$$\binom{n}{k} = \binom{n}{n-k}.$$

[Pol72, str. 255.]

Věta 30. *Neexistuje nejmenší kladné racionální číslo.* [Ped94, str. 20.]

Věta 31. *Nechť n je přirozené číslo. Pak* 7 *dělí* $8^n - 1$.

Věta 32. *Nechť n a m jsou přirozená čísla. Pak* $m - 1$ *dělí* $m^n - 1$.

Definice 13. *Dokonalé číslo je takové přirozené číslo, které je rovno součtu všech svých dělitelů kromě sebe sama.*

Věta 33. 28 *je dokonalé číslo.*

Věta 34. *Součet druhých mocnin prvních n přirozených čísel* S_n *je dán vztahem*

$$S_n = \frac{n(n+1)(2n+1)}{6}.$$

[Ped94, str. 8.]

Definice 14. *Prvočíselná trojčata jsou taková tři po sobě jdoucí prvočísla, která se od svých sousedů liší právě o 2.*

Věta 35. *Existuje právě jedna trojice prvočíselných trojčat:* $3, 5, 7$.

Věta 36. *Nechť* n *je přirozené číslo. Pak platí následující součtový vzorec*

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1.$$

[Mas96, str. 7.]

Věta 37. *Nechť* n *je přirozené číslo. Pokud je* $\sqrt{20n - 15}$ *přirozené číslo, pak* $n = 10m + 2$, *kde* $m \in \mathbb{N}_0$.

Věta 38. *Přirozené číslo je dělitelné* 12 *právě tehdy, splňuje-li pravidlo dělitelnosti třemi a čtyřmi.* [BC09, str. 107.]

3.3 Chybné důkazy

V této sekci jsou prezentovány důkazy několika hypotéz. Některé z těchto hypotéz jsou dokazatelné, jiné vyvratitelné. U každé je ovšem důkaz formulován špatně. Najděte v důkazech těchto hypotéz chyby a, pokud je to možné, opravte je tak, aby byla hypotéza dokázaná. Pokud je hypotéza nesprávná, dokažte její negaci.

Hypotéza 1. *Nechť* $n \in \mathbb{N}$. *Pak platí sumační vzorec*

$$1 - \frac{1}{2} + 2 - \frac{1}{2} + 3 - \frac{1}{2} + \cdots + n - \frac{1}{2} = \frac{n^2 - 1}{2}.$$

Důkaz. Provedeme důkaz indukcí. Uděláme tři kroky.
(1) Ověříme, že vzorec platí pro $n = 0$. Součet $0 - \frac{1}{2} = -\frac{1}{2}$, vzorec dává $\frac{0^2-1}{2} = -\frac{1}{2}$, vzorec tedy pro $n = 0$ platí.
(2) Provedeme indukční předpoklad, že

$$1 - \frac{1}{2} + 2 - \frac{1}{2} + 3 - \frac{1}{2} + \cdots + n - \frac{1}{2} = \frac{n^2 - 1}{2}$$

platí pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$.
(3) Dokážeme, že z předpokladu vyplývá platnost pro $n = k + 1$. Chceme tedy ukázat, že platí

$$1 - \frac{1}{2} + 2 - \frac{1}{2} + 3 - \frac{1}{2} + \cdots + k - \frac{1}{2} + (k+1) - \frac{1}{2} = \frac{(k+1)^2 - 1}{2}.$$

$$
\begin{aligned}
1-\frac{1}{2}+2-\frac{1}{2}+3-\frac{1}{2}+&\\
\cdots+k-\frac{1}{2}+(k+1)-\frac{1}{2} &\overset{\mathrm{IP}}{=} \frac{k^2-1}{2}+(k+1)-\frac{1}{2}\\
&= \frac{(k+1)(k-1)+2(k+1)-1}{2}\\
&= \frac{(k+1)(k-1+2)-1}{2}\\
&= \frac{(k+1)(k+1)-1}{2}\\
&= \frac{(k+1)^2-1}{2}
\end{aligned}
$$

Tvrzení platí pro $n = 1$ a z platnosti pro $n = k$ plyne platnost pro $n = k+1$. Tím je věta dokázána. $\square$

Hypotéza 2. *Pro každé prvočíslo p platí, že výraz* $p^2 + 1$ *je dělitelný* 5 *nebo že výraz* $p^2 + 4$ *je dělitelný* 5.

Důkaz. Prvočísla mohou končit pouze na číslice 1, 3, 7 a 9. Po umocnění na druhou jsou možné koncové cifry pouze 1 a 9. Pokud je poslední cifra 1, pak $p^2 + 4$ je dělitelné 5. Pokud je poslední cifra 9, pak $p^2 + 1$ je dělitelné 5. $\square$

Lemma 8. *Přirozené číslo je dělitelné dvěma právě tehdy, když je jeho poslední cifra 0, 2, 4, 6, nebo 8.* [BC09, str. 105.]

Hypotéza 3. *Přirozené číslo je dělitelné* 8 *právě tehdy, splňuje-li pravidlo dělitelnosti dvěma a čtyřmi.*

Důkaz. Věta je ekvivalence, dokážeme obě implikace.

1) Pokud je přirozené číslo dělitelné 8, pak splňuje pravidla dělitelnosti dvěma a čtyřmi.
Nechť $n \in \mathbb{N}$ je dělitelné 8. Pak $n = 8 \cdot k, k \in \mathbb{N}$. Přepišme tuto rovnost do tvaru $n = 2 \cdot (4k)$. Jelikož je $4k$ přirozené číslo, n je dělitelné dvěma a dle lemmatu 8 splňuje pravidlo dělitelnosti dvěma. Rovnost $n = 12 \cdot k$ nyní přepišme do tvaru $n = 4 \cdot (2k)$. Jelikož je $2k$ přirozené číslo, n je dělitelné čtyřmi a dle věty 26 splňuje pravidlo dělitelnosti čtyřmi.

2) Pokud přirozené číslo splňuje pravidla dělitelnosti dvěma a čtyřmi, pak je dělitelné 8. Nechť $n \in \mathbb{N}$ splňuje pravidla dělitelnosti dvěma a čtyřmi.

Pak je dvěma a čtyřmi dělitelné. Platí tedy $n = 2k = 4l$, kde k a l jsou nějaká přirozená čísla. Jelikož je $2k = 4l$ a l je přirozené číslo, je $2k$ dělitelné čtyřmi. Vzhledem k tomu, že čtyři nedělí dva, musí čtyři dělit k. Proto platí $2k = 2 \cdot 4m$, kde m je nějaké přirozené číslo. Tedy $n = 2 \cdot 4m = 8m$, kde m je přirozené číslo, a proto je n násobkem 8 a je tedy 8 dělitelné. Obě implikace byly dokázány, původní věta ve formě ekvivalence byla tedy také dokázána. $\square$

Hypotéza 4. $\sqrt{4}$ *je iracionální číslo.*

Důkaz. Větu dokážeme sporem, tedy z negace věty vyvodíme spor.
Předpokládejme, že $\sqrt{4}$ je racionální číslo. Pak lze vyjádřit jako podíl $\sqrt{4} = \frac{p}{q}$, kde p a q jsou navzájem nesoudělná přirozená čísla a q ani p nejsou nula. Jelikož je q nenulové číslo, můžeme jím rovnost vynásobit a posléze rovnost umocnit na druhou. Dostaneme $4q^2 = p^2$. Jelikož je levá strana dělitelná čtyřmi, musí být rovněž pravá strana dělitelná čtyřmi. A jelikož p^2 je dělitelné čtyřmi, pak i p je dělitelné čtyřmi (lemma 3). Platí tedy, že $p = 4r$, kde r je nějaké přirozené číslo. Platí tedy $4q^2 = 16r^2$, neboli $q^2 = 4r^2$. Z této rovnosti plyne, že q^2 je dělitelné 4, tedy q je dělitelné 4. Odvodili jsme, že p i q jsou obě dělitelná čtyřmi, což je ovšem spor s tím, že p a q jsou nesoudělná. Náš původní předpoklad, že $\sqrt{4}$ je racionální, je tedy nesprávný, a proto je $\sqrt{4}$ iracionální číslo. $\square$

Hypotéza 5. $1 = 0,999\ldots.$

Důkaz. Napíšeme $\frac{1}{3} = 0,333....$ Víme, že $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$. Desetinný rozvoj sečteme pod sebou.

$$\begin{array}{r} 0,3333333\ldots \\ +0,3333333\ldots \\ +0,3333333\ldots \\ \hline 0,9999999\ldots, \end{array}$$

tedy $0.999\ldots = 1$. $\square$

4 Řešení úloh

Tato kapitola obsahuje řešení všech úloh z kapitoly 3.

4.1 Logika

Cvičení 1

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \Rightarrow V_2)$	$P(\neg V_2 \Rightarrow \neg V_1)$
1	1	0	0	1	1
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	1	1

Tabulka 4.1: Pravdivostní hodnota implikace a obměněné implikace (řešení)

Cvičení 2

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \wedge V_2)$	$P(\neg V_1 \vee \neg V_2)$
1	1	0	0	1	0
1	0	0	1	0	1
0	1	1	0	0	1
0	0	1	1	0	1

Tabulka 4.2: Pravdivostní hodnota negace konjunkce (řešení)

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \vee V_2)$	$P(\neg V_1 \wedge \neg V_2)$
1	1	0	0	1	0
1	0	0	1	1	0
0	1	1	0	1	0
0	0	1	1	0	1

Tabulka 4.3: Pravdivostní hodnota negace disjunkce (řešení)

$P(V_1)$	$P(V_2)$	$P(\neg V_1)$	$P(\neg V_2)$	$P(V_1 \Rightarrow V_2)$	$P(V_1 \wedge \neg V_2)$
1	1	0	0	1	0
1	0	0	1	0	1
0	1	1	0	1	0
0	0	1	1	1	0

Tabulka 4.4: Pravdivostní hodnota negace implikace (řešení)

Výroky v pravých dvou sloupcích tabulek 4.2 až 4.4 nabývají ve všech případech opačných hodnot, jsou si tedy negacemi.

Cvičení 3

V_1: „Číslo a je přirozené a dělitelné třemi nebo čtyřmi."
$\neg V_1$: „Číslo n není přirozené nebo není dělitelné ani třemi, ani čtyřmi."

V_2: „Je-li trojúhelník ABC pravoúhlý a rovnoramenný, pak není rovnostranný."
$\neg V_2$: „Trojúhelník ABC je pravoúhlý, rovnoramenný a rovnostranný."

V_3: „Funkce f je lichá nebo, pokud je spojitá, prochází bodem [0, 0]."
$\neg V_3$: „Funkce f není lichá, je spojitá a neprochází bodem [0, 0]."

V_4: „Libovolný rovinný útvar je kružnice nebo je pravoúhlý a konvexní."
$\neg V_4$: „Existuje rovinný útvar, který není kružnice a není pravoúhlý nebo konvexní."

V_5 = „Existuje reálné číslo, které, pokud není menší než 5, je dokonalé, pokud je sudé."
$\neg V_5$= „Žádné sudé reálné číslo větší než pět není dokonalé."

4.2 Důkazové metody

Věta 23. $\sqrt{3}$ *je iracionální číslo.*

Důkaz. Větu dokážeme sporem, tedy z negace věty vyvodíme spor. Předpokládejme, že $\sqrt{3}$ je racionální číslo. Pak lze vyjádřit jako podíl $\sqrt{3} = \frac{p}{q}$, kde p a q jsou navzájem nesoudělná přirozená čísla a q ani p nejsou nula. Jelikož je q nenulové číslo, můžeme jím rovnost vynásobit a posléze rovnost umocnit na druhou. Dostaneme $3q^2 = p^2$. Jelikož je levá strana dělitelná třemi, musí být rovněž pravá strana dělitelná třemi. A jelikož p^2 je dělitelné třemi, pak i p je dělitelné třemi (lemma 3). Platí tedy, že $p = 3r$, kde r je nějaké přirozené číslo. Platí tedy $3q^2 = 9r^2$, neboli $q^2 = 3r^2$. Z této rovnosti plyne, že q^2 je dělitelné 3, tedy q je dělitelné 3. Odvodili jsme, že p i q jsou obě dělitelná třemi, což je ovšem spor s tím, že p a q jsou nesoudělná. Náš původní předpoklad, že $\sqrt{3}$ je racionální, je tedy nesprávný, a proto je $\sqrt{3}$ iracionální číslo. □

Věta 24. 25 *je čtvercové číslo.*

Důkaz. Číslo 25 se dá přepsat na součin $25 = 5 \cdot 5 = 5^2$. Jelikož je 5 přirozené číslo, splňuje číslo 25 definici 9 a je čtvercovým číslem. □

Věta 25. *Pro všechna* $x \in \mathbb{R}$ *platí* $\cos 3x = 4\cos^3 x - 3\cos x$.

Důkaz. Dokazujeme rovnost výrazů. Vyjdeme z levé strany rovnosti a ekvivalentními úpravami vyvodíme stranu pravou. Úpravy provádíme na základě lemmatu 2.

$$\begin{aligned}
\cos 3x &= \cos(2x + x) \\
&= \cos 2x \cos x - \sin 2x \sin x && \text{(dle lemmatu 2)} \\
&= (\cos x \cos x - \sin x \sin x) \cos x - (\sin x \cos x + \sin x \cos x) \sin x \\
&= \cos^3 x - \cos x \sin^2 x - 2\sin^2 x \cos x \\
&= \cos^3 x - 3\cos x \sin^2 x \\
&= \cos^3 x - 3\cos x(1 - \cos^2 x) \\
&= 4\cos^3 x - 3\cos x
\end{aligned}$$

□

Věta 26. *Přirozené číslo n je dělitelné čtyřmi právě tehdy, je-li jeho poslední dvojčíslí dělitelné čtyřmi.*

Důkaz. Věta je ekvivalence, dokážeme každou implikaci zvlášť.

1) Pokud je přirozené číslo n dělitelné čtyřmi, je jeho poslední dvojčíslí dělitelné čtyřmi. Každé přirozené číslo n lze zapsat ve tvaru

$$n = k \cdot 100 + m,$$

kde k je přirozené číslo vyjadřující počet stovek čísla n a m je přirozené koncové dvojčíslí čísla n. Součin na pravé straně rovnosti upravíme tak, aby bylo zřetelné, že je dělitelný 4. Dostaneme

$$n = k \cdot 25 \cdot 4 + m.$$

Z předpokladu, že n je dělitelné čtyřmi, plyne, že i pravá strana rovnosti je dělitelná čtyřmi, tedy aby součet na pravé straně byl dělitelný 4, musí být 4 dělitelné i poslední dvojčíslí m.

2) Je-li poslední dvojčíslí m přirozeného čísla n dělitelné čtyřmi, lze psát

$$m = 4 \cdot j,$$

kde j je nějaké přirozené číslo. Číslo $n-m$ je výraz, jehož poslední dvě číslice jsou 0, můžeme ho tedy vyjádřit jako

$$n - m = k \cdot 100,$$

kde k je nějaké přirozené číslo. Z tohoto zápisu také vidíme, že $n - m$ je dělitelné čtyřmi. Jelikož m a $n-m$ jsou dělitelná 4, je i jejich součet dělitelný 4 a tedy

$$m + n - m = l \cdot 4, \text{neboli}$$

$$n = 4 \cdot l,$$

kde l je nějaké přirozené číslo. Číslo n je tedy dělitelné 4. □

Věta 27. *Nechť n je přirozené číslo. Pokud je n^2 sudé, pak n je sudé.*

Důkaz. Větu dokážeme obměněnou implikací. Ta říká, že, pokud n není sudé, pak není sudé n^2. Nebo ekvivalentně, je-li n liché, je n^2 liché. Tuto implikaci dokážeme přímo. Vyjdeme z předpokladu, že n je liché. To znamená, že lze zapsat ve tvaru $n = 2k - 1$, $k \in \mathbb{N}$. Číslo n^2 potom nabývá podoby $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$, což znamená, že je liché, tedy že není sudé a obměněná implikace byla dokázána. □

Věta 28. *Jediná trojice po sobě jdoucích přirozených čísel* a, b, c*, která splňují rovnost* $a^2 + b^2 = c^2$*, je trojice* $3, 4, 5$.

Důkaz. Větu dokážeme sporem. Nechť existuje alespoň jedna další trojice po sobě jdoucích přirozených čísel a, b, c, která splňuje rovnost $a^2 + b^2 = c^2$, než $3, 4, 5$. Víme, že a, b, c jsou po sobě jdoucí přirozená čísla, proto můžeme psát $b = a + 1$ a $c = a + 2$. Platí tedy

$$\begin{aligned} a^2 + (a+1)^2 &= (a+2)^2, \\ a^2 + a^2 + 2a + 1 &= a^2 + 4a + 4, \\ a^2 - 2a - 3 &= 0, \\ (a+1)(a-3) &= 0, \\ a &= 3 \vee a = -1. \end{aligned}$$

Jelikož chceme jinou trojici než 3, 4, 5, a se nesmí rovnat 3. Také musí a být přirozené číslo, což -1 není. Neexistuje tedy žádná další trojice po sobě jdoucích přirozených čísel, která splňuje rovnost $a^2 + b^2 = c^2$, což je spor s tím, že taková trojice existuje. □

Věta 29. *Pro všechna* $n, k \in \mathbb{N}_0$, $n > k$*, platí*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Důkaz. Tuto rovnost výrazů dokážeme přímo. Vyjádříme obě kombinační čísla pomocí faktoriálů a porovnáme.

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!\,(n-k)!} \\ \binom{n}{n-k} &= \frac{n!}{(n-k)!\,(n-(n-k))!} = \frac{n!}{(n-k)!\,k!} \end{aligned}$$

Oba výrazy se rovnají, věta byla dokázána. □

Věta 30. *Neexistuje nejmenší racionální číslo.*

Důkaz. Větu dokážeme sporem. Uvažujme, že platí negace tvrzení, tedy že existuje nejmenší kladné racionální číslo. Označme toto číslo s. Víme, že toto číslo je racionální, tedy $s = \frac{p}{q}$, kde p a q jsou přirozená čísla. Nyní uvažme číslo $\frac{s}{2} = \frac{p}{2q}$. Toto číslo je zjevně kladné, racionální a menší než s, což je spor s tím, že s je nejmenší kladné racionální číslo. □

Věta 31. *Nechť n je přirozené číslo. Pak 7 dělí $8^n - 1$.*

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 1$ je výraz roven $8^1 - 1 = 7$, což 7 dělitelné je.
(2) Nechť výraz $8^n - 1$ je dělitelný 7 pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$, tedy $8^n - 1 = 7 \cdot m$, kde m je nějaké přirozené číslo.
(3) Použitím indukčního předpokladu chceme dokázat, že výraz $8^{k+1} - 1$ je dělitelný 7.

$$\begin{aligned} 8^{k+1} - 1 &= 8^k \cdot 8 - 1 \\ &= 8^k \cdot (7 + 1) - 1 \\ &= 8^k \cdot 7 + 8^k - 1 \\ &\overset{\text{IP}}{=} 8^k \cdot 7 + 7 \cdot m \\ &= 7 \cdot (8^k + m) \end{aligned}$$

Jelikož je součet $8^k + m$ nějaké přirozené číslo, vyjadřuje poslední řádek nějaký násobek 6. Tedy $8^{k+1} - 1$ je dělitelné 7.
Tvrzení platí pro $n = 1$ a z platnosti pro k plyne platnost pro $k + 1$, proto věta platí pro všechna $n \in \mathbb{N}$. □

Věta 32. *Nechť n a m jsou přirozená čísla. Pak $m - 1$ dělí $m^n - 1$.*

Důkaz. Provedeme tři kroky důkazu indukcí.
(1) Pro $n = 1$ je výraz roven $m^1 - 1 = m - 1$, což $m - 1$ dělitelné je.
(2) Nechť výraz $m^n - 1$ je dělitelný $m - 1$ pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$, tedy $m^n - 1 = (m - 1) \cdot l$, kde l je nějaké přirozené číslo.
(3) Použitím indukčního předpokladu chceme dokázat, že výraz $m^{k+1} - 1$ je dělitelný $m - 1$.

$$\begin{aligned} m^{k+1} - 1 &= m^k \cdot m - 1 \\ &= m^k \cdot (m - 1 + 1) - 1 \\ &= m^k \cdot (m - 1) + m^k - 1 \\ &\overset{\text{IP}}{=} m^k \cdot (m - 1) + (m - 1) \cdot l \\ &= (m - 1) \cdot (m +^k + l) \end{aligned}$$

Jelikož je součet $m^k + l$ nějaké přirozené číslo, vyjadřuje poslední řádek nějaký násobek 6. Tedy $m^{k+1} - 1$ je dělitelné $(m - 1)$.
Tvrzení platí pro $n = 1$ a z platnosti pro k plyne platnost pro $k + 1$, proto věta platí pro všechna $n \in \mathbb{N}$. □

Věta 33. 28 *je dokonalé číslo.*

Důkaz. Vypíšeme všechny dělitele čísla 28 a sečteme je. Dostaneme

$$1 + 2 + 4 + 7 + 14 = 28,$$

tedy 28 splňuje definici 13. $\square$

Věta 34. *Součet druhých mocnin prvních n přirozených čísel S_n je dán vztahem*

$$S_n = \frac{n(n+1)(2n+1)}{6}.$$

Důkaz. Tuto větu dokážeme indukcí. Provedeme všechny tři kroky důkazu indukce.

(1) Ověříme, že vzorec platí pro nejnižší číslo, kterého se tvrzení týká. Věta mluví o přirozených číslech, proto za n dosadíme 1. Součet 1^2 je 1. Vzorec dává $S_n = \frac{1(1+1)(2+1)}{6} = 1$, tedy tvrzení platí pro $n = 1$.

(2) Utvoříme předpoklad, že vzorec

$$S_n = \frac{n(n+1)(2n+1)}{6}$$

platí pro $n \in \{1, 2, \ldots, k\}, k \in \mathbb{N}$.

(3) Dokážeme, že platnost vzorce pro $n = k$ implikuje platnost vzorce pro $n = k + 1$. Chceme tedy

$$S_{k+1} = \frac{(k+1)(k+2)(2k+3)}{6}.$$

$$
\begin{aligned}
1^2+2^2+3^2\ldots+k^2+(k+1)^2 &\overset{\mathrm{IP}}{=} \frac{k(k+1)(2k+1)}{6}+(k+1)^2\\
&= \frac{k(k+1)(2k+1)}{6}+\frac{6(k+1)^2}{6}\\
&= \frac{k(k+1)(2k+1)+6(k+1)^2}{6}\\
&= \frac{(k+1)(k(2k+1)+6(k+1))}{6}\\
&= \frac{(k+1)(2k^2+k+6k+6}{6}\\
&= \frac{(k+1)(2k^2+7k+6}{6}\\
&= \frac{(k+1)(k+2)(2k+3)}{6}
\end{aligned}
$$

Tvrzení platí pro $n = 1$ a z platnosti pro $n = k$ plyne platnost pro $n = k+1$. Tím je věta dokázána. □

Věta 35. *Existuje právě jedna trojice prvočíselných trojčat: 3, 5, 7.*

Důkaz. Větu dokážeme sporem. Předpokládejme, že existuje kromě trojice $3, 5, 7$ ještě alespoň jedna trojice prvočíselných trojčat. Podle definice 14 se dají tato trojčata zapsat jako trojice $n, n+2, n+4$. Číslo n po dělení třemi dá zbytek buď 0, 1, nebo 2. Podle těchto možností rozdělíme důkaz na tři části.

1) Nechť $n = 3k, k \in \mathbb{N}$, pak $n = 3k$ je buď číslo složené, nebo 3. Pokud by $n = 3$, pak $n+2 = 5$ a $n+4 = 7$, což není nová trojice prvočíselných trojčat.

2) Nechť $n = 3k+1, k \in \mathbb{N}$, pak $n+2 = 3k+3 = 3(k+1)$ je buď číslo složené, nebo 3. Pokud by $n+2 = 3$, pak by $n = 1$ nebylo prvočíslo.

3) Nechť $n = 3k+2, k \in \mathbb{N}$, pak $n+4 = 3k+6 = 3(k+2)$ je buď číslo složené, nebo 3. Pokud by $n+4 = 3$, pak by $n = -1$ nebylo prvočíslo.

Všechny tři možnosti byly dokázány, byla tedy dokázána věta samotná. □

Věta 36. *Nechť n je přirozené číslo. Pak platí následující součtový vzorec.*

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$$

Důkaz. Dokážeme indukcí. Provedeme tří indukční kroky.
(1) Pro $n = 1$ je levá strana rovna $1 \cdot 1! = 1$ a pravá $(1+1)! - 1 = 2 - 1 = 1$, tedy pro $n = 1$ vzorec platí.
(2) Předpokládejme, že $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$ pro $n \in \{1, 2, 3, \ldots, k\}, k \in \mathbb{N}$.
(3) Dokážeme, že z platnosti pro $n = k$ plyne platnost pro $n = k + 1$. Chceme dokázat $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot k! + (k+1) \cdot (k+1)! = (k+2)! - 1$

$$\begin{aligned} 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \\ \cdots + n \cdot k! + (k+1) \cdot (k+1)! &\overset{\mathrm{IP}}{=} (k+1)! - 1 + (k+1) \cdot (k+1)! \\ &= (k+1)! \cdot (1 + k + 1) - 1 \\ &= (k+1)! \cdot (k+2) - 1 \\ &= (k+2)! - 1 \end{aligned}$$

Tvrzení platí pro $n = 1$ a z platnosti pro $n = k$ plyne platnost pro $n = k + 1$. Tím je věta dokázána. □

Věta 37. *Nechť n je přirozené číslo. Pokud je $\sqrt{20n - 15}$ přirozené číslo, pak $n = 10m + 2$, kde $m \in \mathbb{N}_0$.*

Důkaz. Větu dokážeme sporem. Předpokládejme negaci věty, tedy že pro přirozené n je $\sqrt{20n - 15}$ přirozené číslo a $n \neq 10m + 2$, $m \in \mathbb{N}_0$. Pak musí $n = 10m + i$, $m \in \mathbb{N}_0$ a $i \in \{0, 1, 3, 4, 5, 6, 7, 8, 9\}$. Platí

$$\sqrt{20n - 15} = k,$$

kde $k \in \mathbb{N}$. Dosadíme za n a upravíme.

$$\begin{aligned} \sqrt{200m + 20i - 15} &= k \\ 200m + 20i - 15 &= k^2 \end{aligned}$$

Levá strana je dělitelná 5, proto je 5 dělitelné i k (dle lemmatu 3), proto $k = 5l, l \in \mathbb{N}$.

$$\begin{aligned} 200m + 20i - 15 &= 25l^2 \\ 40m + 4i - 3 &= 5l^2 \end{aligned}$$

Pravá strana je dělitelná 5; proto, aby byla levá strana také dělitelná 5, musí být výraz $4i - 3$ dělitelný 5.

Nyní ověříme všechny možnosti. Snadným dosazením za i zjistíme, že i musí být 7. Dosadíme do rovnosti.

$$\begin{aligned} 40m + 4 \cdot 7 - 3 &= 5l^2 \\ 40m + 25 &= 5l^2 \\ 8m + 5 &= l^2 \end{aligned}$$

Levá strana této rovnosti je lichá, l tedy musí být také liché. Proto $l = 2j-1$, kde $j \in \mathbb{N}$.

$$\begin{aligned} 8m + 5 &= (2j-1)^2 \\ 8m + 5 &= 4j^2 - 4j + 1 \\ 8m + 4 &= 4j^2 - 4j \\ 2m + 1 &= j^2 - j \\ 2m + 1 &= j(j-1) \end{aligned}$$

Levá strana rovnosti je lichá. Na pravé straně je součin, ve kterém je jeden činitel lichý a druhý sudý, součin je tedy sudý. Dostáváme, že liché číslo se rovná sudému, což je spor.

□

Věta 38. *Přirozené číslo je dělitelné* 12 *právě tehdy, splňuje-li pravidlo dělitelnosti třemi a čtyřmi.*

Důkaz. Věta je ekvivalence, dokážeme obě implikace.

1) Pokud je přirozené číslo dělitelné 12, pak splňuje pravidla dělitelnosti třemi a čtyřmi.
Nechť $n \in \mathbb{N}$ je dělitelné 12. Pak $n = 12 \cdot k, k \in \mathbb{N}$. Přepišme tuto rovnost do tvaru $n = 3 \cdot (4k)$. Jelikož je $4k$ přirozené číslo, n je dělitelné třemi a dle věty 5 splňuje pravidlo dělitelnosti třemi. Rovnost $n = 12 \cdot k$ nyní přepišme do tvaru $n = 4 \cdot (3k)$. Jelikož je $3k$ přirozené číslo, n je dělitelné čtyřmi a dle věty 26 splňuje pravidlo dělitelnosti čtyřmi.

2) Pokud přirozené číslo splňuje pravidla dělitelnosti třemi a čtyřmi, pak je dělitelné 12. Nechť $n \in \mathbb{N}$ splňuje pravidla dělitelnosti třemi a čtyřmi. Pak je třemi a čtyřmi dělitelné. Platí tedy $n = 3k = 4l$, kde k a l jsou nějaká přirozená čísla. Jelikož je $3k = 4l$ a l je přirozené číslo, je $3k$ dělitelné čtyřmi. Vzhledem k tomu, že čtyři a tři nemají společného dělitele, musí čtyři dělit k. Proto platí $3k = 3 \cdot 4m$, kde m je nějaké přirozené číslo. Tedy $n = 3 \cdot 4m = 12m$, kde m je přirozené číslo, a proto je n násobkem 12 a je tedy 12 dělitelné. Obě implikace byly dokázány, původní věta ve formě ekvivalence byla tedy také dokázána. □

4.3 Chybné důkazy

Hypotéza 1. *Nechť $n \in \mathbb{N}$. Pak platí sumační vzorec*

$$1-\frac{1}{2}+2-\frac{1}{2}+3-\frac{1}{2}+\cdots+n-\frac{1}{2}=\frac{n^2-1}{2}.$$

Důkaz. V důkazu je mylně udělaný první krok. Platnost tvrzení ověřujeme pro nejmenší číslo, kterého se věta týká. V tomto případě věta hovoří o přirozených číslech, tedy v prvním kroku ověřujeme platnost pro $n = 1$. Součet dává $1 - \frac{1}{2} = \frac{1}{2}$, ze vzorce vychází $\frac{1^2-1}{2} = 0$. Tedy tvrzení neplatí pro $n = 1$ a nemá smysl dál v důkazu pokračovat. □

Hypotéza 2. *Pro každé prvočíslo p platí, že výraz $p^2 + 1$ je dělitelný 5 nebo že výraz $p^2 + 4$ je dělitelný 5.*

Důkaz. Důkaz není úplný, jelikož chybí rozbor případu, kdy $p = 2$. Pak $p^2 + 1 = 2^2 + 1 = 4 + 1 = 5$, což dělitelné 5 je, takže věta platí. □

Hypotéza 3. *Přirozené číslo je dělitelné 8 právě tehdy, splňuje-li pravidlo dělitelnosti dvěma a čtyřmi.*

Důkaz. Ve druhé části špatného důkazu dostáváme, že $2k$ je dělitelné čtyřmi. Z tohoto je chybně odvozeno, že čtyři musí dělit k. To není pravda. Jediné, co víme, je, že $2k = 4l$. Po zkrácení dvěma dostáváme $k = 2l$, tedy k je nutně dělitelné dvěma, nikoliv však čtyřmi.
Větu můžeme snadno vyvrátit protipříkladem. Číslo $4 = 4 \cdot 1 = 2 \cdot 2$, je tedy dělitelné čtyřmi i dvěma, ale nikoliv osmi, jelikož $4 = 8 \cdot 0,5$ a $0,5$ není přirozené číslo, 4 tedy nesplňuje definici 2 pro násobek osmi a tedy osmi dělitelné není. □

Hypotéza 4. *$\sqrt{4}$ je iracionální číslo.*

Důkaz. Chyba se v tomto důkaze schovává ve špatném použití lemmatu 5. Jelikož číslo 4 není prvočíslo, není možné na něj lemma aplikovat. Hypotéza je samozřejmě chybná, snadno dokážeme její negaci.

$$4 = 2 \cdot 2, \qquad \text{tedy} \qquad \sqrt{4} = 2,$$

a to je racionální číslo. □

Lemma 9. *Nechť* $\{a_i\}_{i=1}^{\infty}$ *je geometrická posloupnost s reálným kvocientem* $q \in (-1, 1)$. *Pak se součet všech členů této posloupnosti nazývá geometrická řada a je roven*

$$a_1 + a_2 + a_3 + \cdots = \frac{a_1}{1-q}.$$

Hypotéza 5. $1 = 0,999\ldots.$

Důkaz. Poskytnutý důkaz není správně, protože sčítání pod sebou provádíme zprava doleva. Jelikož není kde začít, nemůžeme takto sčítat. Správný důkaz využívá součtu geometrické řady.
Číslo $0,999\ldots$ přepíšeme jako geometrickou řadu

$$0,999\ldots = 0,9 + 0,09 + 0,009 + \cdots$$

s kvocientem $q = 0,1$ a prvním členem $a_1 = 0,9$. Dle lemmatu 9 je součet této řady roven

$$0,9 + 0,09 + 0,009 + \cdots = \frac{0,9}{1 - 0,1} = \frac{0,9}{0,9} = 1.$$

Tím je věta dokázána. □

Závěr

Vzhledem k nedostatečnému zastoupení předvádění důkazů žákům na střední škole jsou studenti prvních ročníků matematických vysokých škol mnohdy zaskočeni postupem, kterým se matematika na těchto školách vyučuje. Z tohoto důvodu jsem se v této bakalářské práci zaměřil na to, abych potenciálním studentům matematické vysoké školy usnadnil přestup z jednoho způsobu vyučování na druhý. Věnoval jsem se důkazům, které jsou – vedle schopnosti řešit matematické úlohy – podstatnou součástí studia na matematických vysokých školách. Mým cílem v této práci bylo popsat základní důkazové metody. Popsal jsem důkaz přímý, důkaz sporem, důkaz pomocí obměněné implikace a důkaz indukcí. Také jsem se věnoval vedlejším důkazovým strategiím, a to důkazu uvedením příkladu a důkazu rozborem možností. Celkem jsem zpracoval 22 vět se vzorovým důkazem, na kterých jsou jednotlivé důkazové metody rozebrány. Dále jsem uvedl celkem 16 vět, které má čtenář řešit samostatně, a 5 důkazů hypotéz, které obsahují chybu a čtenář je má opravit. Řešení k těmto cvičením jsem uvedl v samostatné kapitole práce.

Hlavní část práce je kapitola 2, ve které jsou vzorově vyřešené věty pomocí popisovaných důkazových metod. Struktura této kapitoly odpovídá struktuře matematických textů, které slouží jako studijní materiály na vysoké škole. Tímto přispívám k tomu, aby si žák utvořil představu o tom, jak probíhá výuka na vysoké škole se zaměřením na matematiku, a nebyl pro něj přechod z jednoho výukového systému do druhého příliš náhlý.

Tato práce by se dala dále rozšířit o další příkladové věty, které si má žák sám dokázat. Ukázalo se, že najít vhodné věty, které se od sebe budou dostatečně lišit a žák je bude na střední škole schopen dokazovat, je obtížné. Zdroje, které se důkazy zabývají, tyto důkazy prezentují na vesměs stejných větách. Středoškolské učebnice obsahují jen velmi málo vět, které jsou dokazované jinak než jednoduchým přímým důkazem z definic. Internetové zdroje, které obsahují seznam vět například pro důkaz sporem, mívají uvedené věty, které jsou v principu všechny stejné a nehodily se tedy do této práce.

Literatura

[BC09] Bušek, Ivan a Emil Calda, 2009. *Matematika pro gymnázia: Základní poznatky z matematiky.* 4. vydání. Praha: Prometheus. ISBN 978-80-7196-366-0.

[Beč05] Bečvář, Jindřich, 2005. *Lineární algebra.* 3. vydání. Praha: Matfyzpress. ISBN 80-86732-57-6.

[Blo00] Bloch, Ethan D., 2000. *Proofs and Fundamentals: A First Course in Abstract Mathematics.* Boston: Birkhäuser. ISBN 0-8176-4111-4.

[Ecc97] Eccles, Peter J., 1997. *An Introduction to Mathematical Reasoning.* Cambridge: Cambridge University Press. ISBN 0-521-59718-8.

[Edw08] Edward, Harold M., 2008. *Higher Arithmetics: An Alhorithmic Introduction to Number Theory.* Providence, R. I.: American Mathematical Society. ISBN 978-0-8218-4439-7.

[GT96] Garnier, Rowan a John Taylor, 1996. *100% Mathematical Proof.* New York: Wiley. ISBN 0-471-96199-X.

[Hyu18] Hyunyoung, Lee, 2018. *Notes on Proof By Contrapositive and Proof by Contradiction.* [online]. [24. 4. 2018]. Dostupné z: http://faculty.cse.tamu.edu/hlee/csce222/proofs-contradiction-contrapositive.pdf.

[Mas96] Mason, John, 1996. *Twenty-six Years of Problem Posing: Mathematical Investigations Used in Open University Mathematics Summer Schools.* [online]. [8. 5. 2018]. Dostupné z: http://www.peterliljedahl.com/wp-content/uploads/Mason-26-Years.pdf.

[Odv93] Odvárko, Oldřich, 1993. *Matematika pro gymnázia: Funkce.* 3. vydání. Praha: Prometheus. ISBN 978-80-7196-164-2.

[OK04] ODVÁRKO, Oldřich a Jiří KADLEČEK, 2004. *Přehled matematiky pro základní školy a nižší ročníky víceletých gymnázií.* Praha: Prometheus. ISBN 80-7196-276-7.

[PED94] PEDRICK, George, 1994. *A First Course in Analysis.* New York: Springer-Verlag. ISBN 0-387-94108-8.

[POL72] POLÁK, Josef, 1972. *Přehled středoškolské matematiky.* Praha: Státní pedagogické nakladatelství. Publikace č. 15-19-07.

[PÓL09] PÓLYA, George a Jeremy KILPATRIC, 2009. *The Stanford mathematics problem book: with hints and solutions.* Dover edition. New York: Dover Publications, Inc. ISBN 978-0-486-46924-9.

[SMÝ15] SMÝKALOVÁ, Radka, 2015. *Goniometrické funkce v elementární matematice.* Brno: Nadace Universitatis, Scintilla. ISBN 978-80-7204-937-0.

Seznam tabulek