Druhy dôkazov

Mgr. Jana Králiková

U: Čo vieš o logickej výstavbe matematiky?

Ž: *No, logika k matike patrí, ale tá výstavba - to myslíte akože tehlu k tehle?*

U: Áno, len tie tehly sa nazývajú ***axiómy***, ***definície***, ***vety***, ***dôkazy***.

Ž: *Aha. Niečo si spomínam.*

U: Začneme axiómami:
Axiómy (postuláty) sú také tvrdenia, ktoré považujeme za pravdivé bez dôkazu. Preto sa im hovorí aj základné vety.

Ž: *Tak to je skvelé. Vyslovíme vetu a nemusíme ju prácne dokazovať.*

U: Pojmy a vzťahy, ktoré axiómy obsahujú, sa nazývajú ***základné (primitívne) pojmy*** matematickej teórie. Tieto pojmy sa nedefinujú, ale pokladajú sa za zavedené, teda úplne charakterizované, sústavou axióm.

Ž: *Uvedieme si nejaký príklad?*

U: S axiómami si sa mohol stretnúť v rovinnej a priestorovej geometrii alebo aj v teórii čísel. Napríklad:

- Ak máme dané dva ***body***, tak existuje jediná ***priamka***, ktorá nimi prechádza.
- Všetky pravé uhly sú si ***rovné***.
- Pre každé reálne číslo a platí: $a = a$.
- Pre každé dve reálne čísla a, b platí práve jeden z nasledujúcich vzťahov: $a = b$, $a < b$, $a > b$.

Ž: *Takže axiómy sú niečo ako základy stavby. Používajú pojmy, ktoré sú nám akože jasné hneď.*

U: Áno. V euklidovskej geometrii sú to napríklad pojmy bod, priamka, rovina…

Ž: *Okrem takýchto základných pojmov je ale v matematike aj veľa ďalších pojmov.*

U: Správne. Ich zavedenie a vysvetlenie majú na starosti definície:
Definícia je zavedenie nového matematického pojmu, jeho názvu alebo označenia pomocou základných alebo skôr definovaných pojmov.

Ž: *Chcelo by to znova ukážku.*

U: Dobre:

- Kružnica ***je*** množina všetkých bodov roviny, ktoré majú od daného pevného bodu konštantnú vzdialenosť.
- Každá rovnica, ktorá sa dá vyjadriť v tvare $ax + b = 0$, kde a, b sú ľubovoľné dané reálne čísla, pričom $a \neq 0$, ***sa nazýva*** lineárna rovnica s neznámou x.

Ž: *Aha. Definícia kružnice sa opiera o základné pojmy bod a rovina. Definícia lineárnej rovnice využíva už skôr zadefinovaný pojem rovnice.*

U: Máš pravdu. Pri definovaní nového pojmu sa používajú slovné spojenia: ***je nazvaný***, ***nazýva sa***, ***hovorí sa mu***, … Podľa týchto slov poznáš, že ide o definíciu. V matematických vetách sa tieto slovesá nevyskytujú.

Ž: *Takže nasledujú matematické vety.*

U: Presne tak:

Matematická veta (teoréma) je také tvrdenie, ktorého platnosť sa dá dokázať pomocou axióm, definícií a už skôr dokázaných viet. Uvediem ti zopár príkladov matematických viet:

- $\sqrt{2}$ ***je*** iracionálne číslo.
- ***Ak*** je druhá mocnina prirodzeného čísla n nepárne číslo, ***potom*** aj n je nepárne číslo.
- Prirodzené číslo je deliteľné piatimi ***práve vtedy***, ak je zakončené na číslicu 0 alebo 5.
- ***Pre každé prirodzené číslo*** n platí: $1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + n\cdot n! = (n+1)! - 1$.

Ž: *Sú dosť rozmanité.*

U: Áno. Všimni si, že môžu byť v tvare jednoduchého (elementárneho) výroku alebo zloženého výroku – implikácie a ekvivalencie. Alebo môžu vyjadrovať vlastnosť nekonečne veľa čísel…

Ž: *O jednoduchých aj* **zložených výrokoch** *niečo viem.*

U: To je dobré, zíde sa ti to. Matematické vety sa totiž najčastejšie vyskytujú v tvare ***implikácie*** alebo ***ekvivalencie***.

Ž: *Implikácia $A \Rightarrow B$ znamená, že z výroku A vyplýva výrok B.*

U: Správne. Výrok A sa nazýva ***predpoklad vety*** alebo tiež ***postačujúca podmienka*** pre platnosť výroku B. No a výrok B sa nazýva ***záver***, ***tvrdenie*** alebo tiež ***nutná podmienka*** pre platnosť výroku A.

Ž: *Ekvivalencia je obojstranná implikácia. Aj sa značí obojstrannou šípkou $A \Leftrightarrow B$.*

U: Áno. V tomto prípade je výrok A nutnou aj postačujúcou podmienkou pre platnosť výroku B. A naopak.

Ž: *Teda aj výrok B je nutnou a postačujúcou podmienkou platnosti výroku A.*

U: Zhrniem to ešte raz v rámčekoch:

$$A \Rightarrow B$$

A … postačujúca podmienka pre platnosť B
B … nutná podmienka pre platnosť A

$$A \Leftrightarrow B$$

A … nutná a postačujúca podmienka pre platnosť B
B … nutná a postačujúca podmienka pre platnosť A

U: No a s matematickými vetami súvisia aj dôkazy ich pravdivosti:
Dôkaz matematickej vety je logické odvodenie jej platnosti pomocou axióm, definícií alebo už skôr dokázaných viet.

Ž: *Ukázali ste mi viac druhov matematických viet. Znamená to, že je aj viacero druhov dôkazov?*

U: Áno. Veľakrát tvar vety napovedá aký dôkaz je pre ňu vhodný.

Ž: *Aké teda poznáme dôkazy?*

U: Sú to:

- ***dôkazy jednoduchých výrokov (tvrdení): dôkaz priamy a dôkaz sporom,***
- ***dôkazy implikácií: dôkaz priamy, dôkaz nepriamy a dôkaz sporom,***
- ***dôkazy ekvivalencií,***
- ***dôkazy rovnosti množín***
- ***dôkaz matematickou indukciou.***

Ž: *No teda. Je toho dosť.*

U: Vysvetlíme si mechanizmus každého typu dôkazu.

U: Ako prvý si uvedieme ***dôkaz výroku - priamy:***
Pri priamom dokazovaní platnosti výroku V si zostavíme konečný reťazec implikácií

$$V_1 \Rightarrow V_2 \Rightarrow V_3 \Rightarrow V_4 \Rightarrow \cdots \Rightarrow V,$$

kde jednotlivé výroky $V_1, V_2, V_3 \ldots$ sú axiómy alebo už dokázané tvrdenia. Posledným členom reťazca je výrok V, ktorý sme mali dokázať.

Ž: *Keďže axiómy aj skôr dokázané tvrdenia sú pravdivé, tak aj jednotlivé implikácie $V_1 \Rightarrow V_2$, $V_2 \Rightarrow V_3$, $V_3 \Rightarrow V_4$,... sú pravdivé a teda aj posledný výrok V musí byť pravdivý.*

U: Správne. V rámčeku si pozri schému úsudku:

$$\boxed{\begin{array}{c} A \quad \text{platí} \\ A \Rightarrow B \quad \text{platí} \\ \hline B \quad \text{platí} \end{array}}$$

Výrok A v rámčeku predstavuje prvý výrok konečného reťazca implikácií. Implikácia $A \Rightarrow B$ predstavuje zostavený konečný reťazec. No a výrok B predstavuje posledný výrok tohto reťazca. V našom prípade je to dokazovaný výrok V.

U: Teraz si ukážeme ako prebieha ***dôkaz výroku - sporom:***
Ak chceme sporom dokázať platnosť výroku V, pomôžeme si jeho ***negáciou*** – výrokom V'.

Ž: *Viem, že výrok a jeho negácia majú opačnú* **pravdivostnú hodnotu**. *Ak platí výrok V, tak jeho negácia, teda výrok V' neplatí.*

U: Správne. Postupujeme tak, že predpokladáme, že výrok V' platí. Z neho potom odvodzujeme logické dôsledky, až kým nedôjdeme k tvrdeniu S, o ktorom vieme, že určite neplatí. Hovoríme, že sme prišli k sporu.

Ž: *Spor to je nejaký konflikt. Niečo čo neladí.*

U: Áno. Tvrdenie S môže byť v spore napríklad s axiómou alebo s už dokázaným tvrdením alebo s predpokladmi vety. V rámčeku je naznačená schéma takéhoto úsudku:

$$\boxed{\begin{array}{c} A' \Rightarrow S \quad \text{platí} \\ S \quad \text{neplatí} \\ \hline A' \quad \text{neplatí} \\ A \quad \text{platí} \end{array}}$$

Ž: *Tak ja si to zhrniem. Implikácia je pravdivá, jej záver je nepravdivý. To nastane len v tom prípade, ak predpoklad je tiež nepravdivý. Predpoklad je ale negáciou výroku A. Ak je táto negácia nepravdivá, tak to znamená, že pôvodný výrok je pravdivý.*

U: Ďalej si uvedieme ***dôkaz implikácie - priamy:***
V implikácii $A \Rightarrow B$ predpokladáme, že výrok A platí. Potom zostavíme reťazec

$$A \Rightarrow B_1 \Rightarrow B_2 \Rightarrow B_3 \Rightarrow \cdots \Rightarrow B.$$

Ž: *Vychádzame teda z predpokladu implikácie a priamym reťazcom sa dopracujeme k záveru implikácie. Keďže z pravdy sa dá logickým usudzovaním dôjsť opäť len k pravde, tak aj tvrdenie B bude pravdivé.*

U: Správne. V rámčeku je schéma úsudku:

$$\boxed{\begin{array}{c} A \quad \text{platí} \\ A \Rightarrow B \quad \text{platí} \\ \hline B \quad \text{platí} \end{array}}$$

U: Ďalší druh dôkazu je ***dôkaz implikácie - nepriamy:***
V ňom namiesto pravdivosti implikácie $A \Rightarrow B$ dokážeme pravdivosť ***obmenenej implikácie***. Vieš ešte ako vyzerá obmenená implikácia?

Ž: *Zameníme poradie výrokov A a B?*

U: Tak by si dostal len obrátenú implikáciu. Obmenenú dostaneš vtedy, ak nielenže zameníš poradie výrokov A a B, ale ešte vytvoríš aj ich negácie.

Ž: *Takže:*

$$\textit{pôvodná implikácia je:} \qquad A \Rightarrow B,$$

$$\textit{obmenená implikácia je:} \qquad B' \Rightarrow A'.$$

U: Výborne. Namiesto pôvodnej implikácie $A \Rightarrow B$ dokážeme jej obmenu $B' \Rightarrow A'$.

Ž: *A to môžeme?*

U: Môžeme. Implikácie $A \Rightarrow B$ a $B' \Rightarrow A'$ majú totiž rovnakú pravdivostnú hodnotu. Ak platí jedna z nich, platí aj druhá. A naopak.

Implikácia $A \Rightarrow B$ je ***ekvivalentná*** s implikáciu $B' \Rightarrow A'$.

Ž: *A ako dokážeme platnosť obmeny?*

U: Priamo alebo sporom. Pozri si ešte rámček:

$$\boxed{\begin{array}{c} A \Rightarrow B \\ \Leftrightarrow \\ B' \Rightarrow A' \end{array}}$$

U: A ostal nám ešte ***dôkaz implikácie - sporom:***
V tomto dôkaze využijeme to, že implikácia $A \Rightarrow B$ a jej negácia majú opačnú pravdivostnú hodnotu. Spomenieš si na negáciu implikácie?

Ž: *To je jednoduché. Malo by to byť $A' \Rightarrow B'$.*

U: No nemáš pravdu:

ak pôvodná implikácia je: $\quad A \Rightarrow B,$

tak jej negácia je: $\quad A \wedge B'.$

Ž: *Aha. A ako teraz využijem túto negáciu implikácie?*

U: Vyjdeme z predpokladu platnosti negácie a priamym dokazovaním pomocou nasledujúceho reťazca implikácií

$$(A \wedge B') \Rightarrow V_1 \Rightarrow V_2 \Rightarrow V_3 \Rightarrow V_4 \Rightarrow \cdots \Rightarrow S,$$

dôjdeme k výroku S, ktorý však neplatí.

Ž: *Aha, to je ten spor. Keďže z pravdy sa nedá logickým usudzovaním dôjsť k nepravde, tak to znamená, že predpoklad na začiatku je nepravdivý.*

U: Áno. Lenže ten nepravdivý predpoklad zo začiatku reťazca je negácia našej implikácie.

Ž: *Už mi je to jasné. Negácia implikácie je nepravdivá, teda pôvodná implikácia musí byť pravdivá.*

U: Je to tak. V tom spočíva dôkaz sporom. Pozri si aj rámčeky:

$$\boxed{\begin{array}{c} (A \Rightarrow B)' \\ \Leftrightarrow \\ A \wedge B' \end{array}}$$

$$\boxed{\begin{array}{c} A \Rightarrow B \\ \Leftrightarrow \\ (A \wedge B')' \end{array}}$$

U: Ďalší dôkaz v poradí je ***dôkaz ekvivalencie:***
Už si spomenul, že ekvivalencia je obostranná implikácia.

Ž: *Áno. Využijeme to nejak?*

U: Samozrejme. Dôkaz výroku v tvare ekvivalencie je totiž rozdelený do dvoch krokov:
1. Dokážeme platnosť implikácie $A \Rightarrow B$.
2. Dokážeme platnosť implikácie $B \Rightarrow A$.

Ž: *A na dôkaz implikácie použijeme niektorý vyššie uvedený dôkaz.*

U: Presne tak. Pozri si schému v rámčeku:

$$\boxed{\begin{array}{c} A \Leftrightarrow B \\ \hline A \Rightarrow B \\ B \Rightarrow A \end{array}}$$

U: A teraz niečo o ***dôkaze rovnosti množín:***
Vieš ako je definovaná rovnosť množín?

Ž: *Dve množiny sa rovnajú, ak majú rovnaké prvky. Ak sa zhodujú vo všetkých prvkoch.*

U: Presnejšie povedané, dve množiny A a B sa rovnajú práve vtedy, ak každá z nich je podmnožinou tej druhej množiny:

$$\boxed{A = B \quad \stackrel{def.}{\Longleftrightarrow} \quad A \subset B \quad \wedge \quad B \subset A}$$

Pozor. Nejde o matematickú vetu v tvare ekvivalencie. Preto je tam zapísané, že ekvivalencia sa chápe v zmysle definície.

Ž: *A ako to využijem pri dokazovaní rovnosti týchto množín?*

U: Dôkaz je opäť rozdelený do dvoch krokov:
1. Dokážeme, že $A \subset B$, teda že každý prvok množiny A je prvkom aj množiny B.
2. Dokážeme, že $B \subset A$, teda že každý prvok množiny B je prvkom aj množiny A.

Ž: *Mne dôkaz takejto rovnosti predsa len pripomína dôkaz ekvivalencie.*

U: Veď ekvivalencia nie je nič iné ako rovnocennosť. V rámčeku je opäť zhrnutie základnej myšlienky dôkazu rovnosti množín:

$$\boxed{\begin{array}{c} A = B \\ \hline A \subset B \\ B \subset A \end{array}}$$

U: Ako posledný uvediem špeciálny druh dôkazov, a to ***dôkaz matematickou indukciou:***

Ž: *Viem, že matematická indukcia sa používa, ak máme dokázať nejakú matematickú vetu pre všetky prirodzené čísla alebo pre prirodzené čísla väčšie alebo rovné ako nejaké dané prirodzené číslo.*

U: Správne. Metódou matematickej indukcie sa teda dokazujú vety typu:

$$\forall n \in \mathbb{N}, n \geqq n_0 : V(n),$$

kde $V(n)$ je daná ***výroková forma*** prirodzenej premennej n.

Ž: *Čo môže byť tou výrokovou formou?*

U: Môže to byť napríklad nejaký vzorec, rovnosť alebo nerovnosť výrazov s premennou n ...

Ž: *Mohli by sme si zopakovať princíp aj tohto dôkazu?*

U: Samozrejme. Dôkaz matematickou indukciou spočíva v dvoch krokoch:
I.krok:
Dokážeme, že veta platí pre $n = n_0$, teda overíme platnosť tvrdenia:

$$V(n_0).$$

Ž: *Aha. Prirodzené číslo n_0 je najmenšie také prirodzené číslo, pre ktoré veta má platiť. Dosadením konkrétnej hodnoty n_0 za n sa z výrokovej formy stane výrok. Overiť jeho pravdivosť by som mal zvládnuť.*

U: *II.krok:*
Dokážeme, že pre ľubovoľné prirodzené číslo n platí implikácia

$$V(n) \quad \Rightarrow \quad V(n+1).$$

Ž: *A čo tým dosiahneme?*

U: Nemôžeme dokazovať platnosť tvrdenia $V(n)$ tak, že do neho budeme postupne dosadzovať všetky prirodzené čísla.

Ž: *To je jasné, veď tých čísel je nekonečne veľa.*

U: Preto sa využije vlastnosť implikácie, že ak predpoklad implikácie je pravdivý a z neho logickým usudzovaním vyplynie nejaký záver, tak aj tento záver implikácie je pravdivý.

Ž: *Takže ak napríklad v prvom kroku dokážem platnosť výroku pre prirodzené číslo $n = 1$, tak v druhom kroku z implikácie*

$$V(1) \quad \Rightarrow \quad V(2)$$

dokážem platnosť výroku $V(2)$. Ak platí výrok $V(2)$, tak pomocou implikácie

$$V(2) \quad \Rightarrow \quad V(3)$$

dokážem platnosť výroku $V(3)$. A tak by som mohol pokračovať. Lenže opäť by som mal nekonečne veľa implikácií, nič sa tým nezjednoduší.

U: Nebudeš dokazovať platnosť nekonečne veľa implikácií, ale len jednej:

$$V(n) \quad \Rightarrow \quad V(n+1).$$

Ž: *Mám teda pracovať so všeobecnými vyjadreniami?*

U: Presne tak. V prvom kroku dokážeš platnosť výroku pre jedno prvé konkrétne číslo a v druhom kroku dokážeš, že z platnosti výroku pre nejaké n vyplynie platnosť výroku pre $n+1$. To je indukcia. V slovníku cudzích slov nájdeš, medzi inými vysvetleniami, aj pojem – ***vzájomné pôsobenie***. Pozri si ešte schému v rámčeku:

$$\boxed{\begin{array}{c} V(1) \quad \text{platí} \\ V(n) \quad \text{platí} \\ V(n) \Rightarrow V(n+1) \quad \text{platí} \\ \hline V(n+1) \quad \text{platí} \end{array}}$$

Ž: *Čiže ak predpokladám, že platí $V(n)$ a podarí sa mi dokázať, že $V(n) \Rightarrow V(n+1)$, tak tým vlastne dokážem platnosť $V(n+1)$?*

U: Áno. Ešte by som poznamenal, že výrok $V(n)$ sa nazýva ***indukčný predpoklad*** a výrok $V(n+1)$ sa nazýva ***indukčné tvrdenie***.

Ž: *Aha. Z platnosti predpokladu $V(n)$ vyplynie platnosť tvrdenia $V(n+1)$.*

U: Dôkaz matematickou indukciou je ako ***búranie múru z dominových kociek***. Ak ***padne*** (platí) ***prvá kocka*** (vzorec pre n=1), ***narazí*** (implikuje) ***do druhej kocky*** (vzorec pre n=2), ***tá zrazí tretiu kocku*** (vzorec pre n=3), ***tretia kocka zrazí štvrtú kocku, a takto to pokračuje ďalej, až nejaká n-tá kocka zrazí*** $n+1$ ***kocku*** teda (zo vzorca pre ľubovoľné n vyplýva platnosť vzorca pre $n+1$) a tak ďalej …

Ž: *Pán učiteľ, videl som padať múriky z domina a keď všetky popadali – tatatatatata – vytvoril sa z nich nádherný obrazec. Bolo to super.*

U: Tak dúfam, že si rovnako očarený aj matematickou indukciou. Princíp je rovnaký.

Ž: *Všetky tieto typy dôkazov sme si uviedli len teoreticky.*

U: Áno. Ale môžeš si pozrieť aj riešené príklady. Pomocou nich si precvičíš každý typ dôkazu.

Príklad 1: *Pre každé reálne číslo a platí*

$$\frac{a^2}{a^4+1} \leqq \frac{1}{2}.$$

Dokážte toto tvrdenie priamo.

Ž: *V priamom dôkaze vychádzame z nejakého pravdivého výroku a odtiaľ sa logickými odvodeniami dostaneme až k výroku, ktorý chceme dokázať.*

U: Správne. Máš vytvoriť reťazec implikácií

$$V_1 \Rightarrow V_2 \Rightarrow V_3 \Rightarrow V_4 \Rightarrow \cdots \Rightarrow V,$$

kde jednotlivé výroky $V_1, V_2, V_3 \dots$ sú axiómy alebo už dokázané tvrdenia. Posledným členom reťazca je výrok V, ktorý sme mali dokázať.

Ž: *Náš výrok V má tvar*

$$V: \ \forall a \in \mathbb{R}: \ \frac{a^2}{a^4+1} \leqq \frac{1}{2}.$$

Problém je ale ten, že netuším, čo je výrok V_1. Z čoho mám vychádzať?

U: Pomôžem ti. V praxi veľakrát postupujeme naopak. Nevychádza sa z výroku V_1, ale z výroku V. Upravujeme teda ten vzťah, ktorý je daný. ***Evivalentnými úpravami*** sa potom dopracujeme k nejakému pravdivému vzťahu. Potom šípkou $\Uparrow$ naznačíme, že sa mohlo postupovať aj naopak.

Ž: *Upravovať daný vzťah zvládnem. Je to nerovnica s neznámou a. Odstránim zlomky na oboch stranách tak, že budem násobiť menovateľmi:*

$$\boxed{\begin{array}{c} \dfrac{a^2}{a^4+1} \leqq \dfrac{1}{2} \ / \cdot \left(a^4+1\right) \cdot 2 \\ 2a^2 \leqq a^4+1 \end{array}}$$

U: Je násobenie nerovnice ekvivalentnou úpravou?

Ž: *Dvojka je kladné číslo a štvrtá mocnina ľubovoľného čísla navyše zväčšená o 1 je tiež kladná. Násobil som teda kladným číslom, čo je ekvivalentnou úpravou.*

U: Dobre. Ako budeš pokračovať?

Ž: *Teraz by som prehodil všetky členy na jednu stranu:*

$$\boxed{\begin{array}{c} 2a^2 \leqq a^4+1 \ / - 2a^2 \\ 0 \leqq a^4 - 2a^2 + 1 \end{array}}$$

U: Zatiaľ je to v poriadku. Teraz si treba spomenúť na nejaký vzorec.

Ž: *Jasné. Mám tam rozpísanú druhú mocninu rozdielu:*

$$(A-B)^2 = A^2 - 2AB + B^2,$$

pričom $A = a^2$ a $B = 1$. Použijem to:

$$\boxed{\begin{gathered} 0 \leqq \left(a^2\right)^2 - 2a^2 + 1 \\ 0 \leqq \left(a^2 - 1\right)^2 \end{gathered}}$$

U: Je to pravda?

Ž: *Samozrejme! Druhá mocnina hocijakého reálneho čísla, aj keď je v tvare* $\left(a^2-1\right)^2$ *je nezáporná. Takže tento výrok je pravdivý.*

U: Správne. A to je presne ten výrok, ktorý mal byť na začiatku reťazca.

Ž: *Takže pravdivý výrok, z ktorého som mal vychádzať by bol*

$$V_1: \ \forall a \in \mathbb{R}: \ \left(a^2-1\right)^2 \geqq 0.$$

Na to by som nebol prišiel.

U: Preto sa postupuje od konca. Celý postup si pozri ešte raz v rámčeku. Šípkou je naznačený správny smer plynutia dôkazu.

$$\boxed{\begin{gathered} \frac{a^2}{a^4+1} \leqq \frac{1}{2} \\ \frac{a^2}{a^4+1} \leqq \frac{1}{2} \ / \cdot \left(a^4+1\right) \cdot 2 \\ 2a^2 \leqq a^4 + 1 \ / - 2a^2 \\ 0 \leqq a^4 - 2a^2 + 1 \\ 0 \leqq \left(a^2-1\right)^2 \quad \Uparrow \end{gathered}}$$

Nerovnice v jednotlivých riadkoch sú si navzájom ekvivalentné, preto sa môžeme vrátiť aj od posledného riadku späť k prvému. V rámčeku si ešte pozri, ako by mal dôkaz správne vyzerať:

$$\boxed{\begin{gathered} 0 \leqq \left(a^2-1\right)^2 \quad \Rightarrow \quad 0 \leqq a^4 - 2a^2 + 1 \quad \Rightarrow \quad 2a^2 \leqq a^4 + 1 \quad \Rightarrow \\ \Rightarrow \quad \frac{2a^2}{a^4+1} \leqq 1 \quad \Rightarrow \quad \frac{a^2}{a^4+1} \leqq \frac{1}{2}. \end{gathered}}$$

Ž: *Postačí aj ten prvý spôsob s naznačenou šípkou?*

U: Áno.

Úloha : *Pre každé reálne čísla a, b platí*

$$\frac{a^2+b^2}{2} \geqq ab.$$

Dokážte toto tvrdenie priamo.

Príklad 2: *Pre každé reálne číslo a platí*

$$\frac{a^2}{a^4+1} \leqq \frac{1}{2}.$$

Dokážte toto tvrdenie sporom.

Ž: *Ak chceme nejaké tvrdenie dokazovať sporom, potrebujeme najprv jeho negáciu. Potom sa budeme snažiť dokázať, že negovaný výrok je nepravdivý a teda platí pôvodný výrok.*

U: Pekne povedané. Poďme teda na vykonanie dôkazu.

Ž: *Pôvodný výrok V má tvar:*

$$V:\ \forall a \in \mathbb{R}:\ \frac{a^2}{a^4+1} \leqq \frac{1}{2}.$$

Ak ho chcem znegovať, tak vymením všeobecný kvantifikátor za existenčný a symbol nerovnosti $\leqq$ zamením za $>$:

$$V':\ \exists a \in \mathbb{R}:\ \frac{a^2}{a^4+1} > \frac{1}{2}.$$

U: Výborne. Teraz dokáž, že výrok V' je nepravdivý.

Ž: *A ako to mám urobiť?*

U: Máš z neho vyvodzovať nejaké logické dôsledky, až kým neprídeš k výroku, ktorý je sporný, nepravdivý. V praxi to znamená upravovať výraz alebo riešiť rovnicu, či nerovnicu, ktorá je vo výroku V'.

Ž: *Riešiť túto nerovnicu s neznámou a zvládnem. Najprv odstránim zlomky na oboch stranách tak, že budem násobiť menovateľmi:*

$$\boxed{\begin{array}{c} \dfrac{a^2}{a^4+1} > \dfrac{1}{2}\ \ / \cdot \left(a^4+1\right) \cdot 2 \\ 2a^2 > a^4+1 \end{array}}$$

U: Je násobenie nerovnice ekvivalentnou úpravou?

Ž: *Dvojka je kladné číslo a štvrtá mocnina hocijakého čísla navyše zväčšená o 1 je tiež kladná. Násobil som teda kladným číslom, čo je ekvivalentnou úpravou.*

U: Dobre. Ako budeš pokračovať?

Ž: *Teraz by som prehodil všetky členy na jednu stranu:*

$$\boxed{\begin{array}{c} 2a^2 > a^4+1\ \ / - 2a^2 \\ 0 > a^4 - 2a^2 + 1 \end{array}}$$

U: Zatiaľ je to v poriadku. Teraz si treba spomenúť na nejaký vzorec.

Ž: *Jasné. Mám tam rozpísanú druhú mocninu rozdielu:*

$$(A-B)^2 = A^2 - 2AB + B^2,$$

pričom $A = a^2$ a $B = 1$. Využijem to:

$$\boxed{\begin{gathered} 0 > \left(a^2\right)^2 - 2a^2 + 1 \\ 0 > \left(a^2 - 1\right)^2 \end{gathered}}$$

U: Je to pravda?

Ž: *Druhá mocnina čohosi je menšia ako nula. Nie, to nie je pravda!*

U: Práve si došiel k sporu. Neexistuje také reálne číslo a, pre ktoré by $\left(a^2 - 1\right)^2$ malo zápornú hodnotu. Logické dôsledky – to boli tie ekvivalentné úpravy nerovnice – ťa doviedli k spornému tvrdeniu. Ale z pravdy sa lož vyvodiť nedá.

Ž: *Znamená to teda, že výrok V' nie je pravdivý. Len z nepravdy môžem odvodiť nepravdu.*

U: Presne tak. Ale ak je výrok V' nepravdivý, tak je pravdivý výrok V.

Ž: *Jasné. Výrok a jeho negácia majú opačné pravdivostné hodnoty. Ak V' neplatí, tak V platí. Sporom sme teda dokázali, že výrok*

$$V: \ \forall a \in \mathbb{R}: \ \frac{a^2}{a^4+1} \leqq \frac{1}{2}$$

je pravdivý.

U: V rámčeku si ešte pozri, ako náš dôkaz prebiehal:

$$\boxed{\begin{gathered} \frac{a^2}{a^4+1} > \frac{1}{2} \quad \Rightarrow \quad 2a^2 > a^4 + 1 \quad \Rightarrow \quad 0 > a^4 - 2a^2 + 1 \quad \Rightarrow \\ \Rightarrow \quad 0 > \left(a^2 - 1\right)^2 \quad \ldots \quad SPOR \quad \Rightarrow \\ \hline \Rightarrow \qquad \frac{a^2}{a^4+1} \leqq \frac{1}{2}. \end{gathered}}$$

Úloha : *Pre každé reálne čísla a, b platí*

$$\frac{a^2 + b^2}{2} \geqq ab.$$

Dokážte toto tvrdenie sporom.

Príklad 3:

$\sqrt{2}$ je iracionálne číslo.

Dokážte toto tvrdenie sporom.

U: Ak chceme dokazovať pravdivosť výroku V sporom, vyjdeme z jeho negácie. Predpokladáme, že táto negácia platí a snažíme sa dokázať, že je to v spore so známymi tvrdeniami.

Ž: *Áno. Výrok a jeho negácia majú opačné pravdivostné hodnoty. Ak negácia neplatí, tak platí pôvodný výrok.*

U: Ako teda bude vyzerať negácia nášho výroku?

Ž: *Pôvodný výrok V má tvar:*

$$V: \ \sqrt{2} \textit{ je iracionálne číslo.}.$$

Ak ho chcem znegovať, tak namiesto spojenia **je** *použijem zápor* **nie je***:*

$$V': \ \sqrt{2} \textit{ nie je iracionálne číslo.}.$$

U: Dobre, ale môžeme to aj upresniť. Množina iracionálnych čísel $\mathbb{I}$ je podmnožinou množiny reálnych čísel $\mathbb{R}$. Negácia má zahŕňať všetky ostatné možnosti. Čo je teda doplnkom množiny iracionálnych čísel, ak základnou množinou je množina reálnych čísel?

Ž: *Predsa množina racionálnych čísel $\mathbb{Q}$, pretože*

$$\mathbb{Q} \cup \mathbb{I} = \mathbb{R}.$$

U: Správne. Naša negácia môže mať teda tvar:

$$V': \ \sqrt{2} \text{ je racionálne číslo.}.$$

Ž: *Či iracionálne alebo racionálne, zdá sa mi to jedno. Ako mi to pomôže v dôkaze?*

U: Racionálne čísla sa predsa dajú vyjadriť v tvare zlomku.

Ž: *Máte pravdu. Takže existujú také čísla a a b, že sú čitateľom a menovateľom zlomku, ktorý má hodnotu $\sqrt{2}$.*

U: To by určite nestačilo. Musíš upresniť, aké sú to čísla.

Ž: *Asi prirodzené. Tak sa vyhnem nulovému menovateľu.*

U: Čitateľ by mohol byť aj celé číslo, tak by sme tam mali zahrnuté aj záporné znamienko. Ale nie je to nutné. Postačí, ak budú čísla a a b prirodzené. Predsa to však ešte trošku upresním. Každý zlomok sa dá napísať v základnom tvare, teda tak, aby čitateľ aj menovateľ boli ***nesúdeliteľné čísla***.

Ž: *Aby sa už nedali ďalej krátiť.*

U: Áno. Zatiaľ teda máme pripravené toto:

$$\sqrt{2} = \frac{a}{b}, \quad \text{kde } a, b \text{ sú nesúdeliteľné prirodzené čísla.}$$

Umocni vzniknutú rovnosť a potom odstráň zlomok.

Ž: *Najprv odstránim odmocninu a potom násobením menovateľom odstránim zlomok:*

$$\boxed{\begin{gathered}\sqrt{2}=\frac{a}{b}\ \ /\ ()^2\\ 2=\frac{a^2}{b^2}\ \ /\cdot b^2\\ 2\cdot b^2=a^2\end{gathered}}$$

U: Dobre. Teraz sa pozrieme, čo sme to vlastne dostali. Ak $a^2 = 2 \cdot b^2$, tak to znamená, že číslo a^2 je deliteľné číslom 2.

Ž: *Áno, lebo je druhým násobkom čísla b^2.*

U: Ak je teda číslom 2 deliteľné číslo a^2, tak je číslom 2 deliteľné aj číslo a.

Ž: *To je pravda. A ako to využijeme?*

U: Ak je číslo a deliteľné číslom 2, tak existuje také prirodzené číslo k, že

$$a = 2 \cdot k.$$

Toto vyjadrenie si teraz dosadíme do vzťahu $a^2 = 2 \cdot b^2$ a umocníme:

$$\boxed{\begin{gathered}a^2=2\cdot b^2\\ (2\cdot k)^2=2\cdot b^2\\ 4\cdot k^2=2\cdot b^2\ \ /:2\\ 2\cdot k^2=b^2\end{gathered}}$$

Ž: *Nezamotali sme sa?*

U: Vôbec nie! Ak $b^2 = 2 \cdot k^2$, tak to znamená, že číslo b^2 je deliteľné číslom 2.

Ž: *Lebo je druhým násobkom čísla k^2.*

U: Ak je teda číslom 2 deliteľné číslo b^2, tak je číslom 2 deliteľné aj číslo b.

Ž: *No ale pred chvíľkou sme si ukázali, že aj číslo a je deliteľné číslom 2. A teraz nám vyšlo, že aj číslo b je číslom 2 deliteľné.*

U: Čo nám z toho vyplýva?

Ž: *Aj a aj b sú deliteľné číslom 2, takže sú súdeliteľné!*

U: Ale podľa predpokladu vety sú nesúdeliteľné. Došli sme teda k sporu.

Ž: *Aha. Dve čísla nemôžu byť súčasne súdeliteľné aj nesúdeliteľné. To znamená, že znegovaný výrok neplatí. Potom ale platí pôvodné tvrdenie*

$$\sqrt{2} \textit{ je iracionálne číslo}.$$

U: Správne. V rámčeku si ešte pozri ako prebiehal celý dôkaz:

$$\sqrt{2} \text{ je racionálne číslo} \quad \Rightarrow$$

$$\Rightarrow \quad \exists a, b \in \mathbb{N},\ a, b \ \text{ sú nesúdeliteľné čísla} : \sqrt{2} = \frac{a}{b} \quad \Rightarrow$$

$$\Rightarrow \quad 2 = \frac{a^2}{b^2} \quad \Rightarrow \quad a^2 = 2b^2 \quad \Rightarrow$$

$$\Rightarrow \quad 2 \mid a^2 \quad \Rightarrow \quad 2 \mid a \quad \Rightarrow \quad \exists k \in \mathbb{N} : a = 2k \quad \Rightarrow$$

$$\Rightarrow \quad 2b^2 = (2k)^2 \quad \Rightarrow \quad b^2 = 2k^2 \Rightarrow \quad 2 \mid b^2 \quad \Rightarrow \quad 2 \mid b \quad \Rightarrow$$

$$\Rightarrow \quad a, b \ \text{ sú súdeliteľné čísla} \quad \dots \quad SPOR \quad \Rightarrow$$

$$\Rightarrow \qquad \sqrt{2} \text{ je iracionálne číslo.}$$

Úloha : *Dokážte sporom nasledujúce tvrdenia:*
a) $\sqrt{5}$ *je iracionálne číslo,*
b) $\log 2$ *je iracionálne číslo.*

Návod:
b) Nech $\log 2 = \frac{a}{b}$, *kde* $a, b \in \mathbb{N} \quad \Rightarrow \quad 2 = 10^{\frac{a}{b}} \quad \Rightarrow \quad 2 = (2 \cdot 5)^{\frac{a}{b}} \quad \Rightarrow$
$\Rightarrow \quad 2^b = 2^a \cdot 5^a \quad \Rightarrow \quad 2^{b-a} = 5^a$,
rovnosť nastane len v prípade, že $a = b = 0$, *čo je spor s predpokladom, že* $a, b \in \mathbb{N}$.

Príklad 4: *Nasledujúcu vetu dokážte priamo:*

Druhá mocnina nepárneho čísla je tiež nepárne číslo.

U: Pokús sa túto vetu preformulovať tak, aby bola v tvare implikácie.

Ž: *Skúsim to: Ak máme nepárne číslo, tak jeho druhá mocnina je tiež nepárne číslo.*

U: Celkom dobre. A o ktorom nepárnom čísle sa vo vete hovorí?

Ž: *No asi o každom.*

U: Áno. Ale ako budeš pracovať s každým nepárnym číslom?

Ž: *Mohol by som si zaviesť nejakú premennú, napríklad x a táto premenná by mi predstavovala všetky nepárne čísla.*

U: To by si naozaj mohol. Preformuluj teraz našu vetu tak, aby obsahovala premennú x.

Ž: *Ak je x nepárne číslo, potom x^2 je tiež nepárne číslo.*

U: Ale v matematickej vete musí byť jasné, aký je ***definičný obor*** premennej x.

Ž: *Mohol by to byť obor prirodzených čísel.*

U: Aj číslo -3 môžeme považovať za nepárne.

Ž: *Dobre. Takže definičným oborom bude obor celých čísel a veta má tvar:*

$$\forall x \in \mathbb{Z}: \quad x \text{ je nepárne číslo} \quad \Rightarrow \quad x^2 \text{ je nepárne.}$$

U: Sformuloval si to pekne. V rámčeku si pozri symbolický zápis tohto tvrdenia:

$$\boxed{\forall x \in \mathbb{Z}: \quad 2 \nmid x \quad \Rightarrow \quad 2 \nmid x^2}$$

Teraz to už len dokázať.

Ž: *Pri priamom dôkaze implikácie mám zostaviť reťazec pravdivých implikácií. Ale ako?*

U: Vyjdeš z predpokladu vety. Tým je prvá časť vety, teda, že x je nepárne číslo.

Ž: *A ako to mám využiť?*

U: Ak x je nepárne číslo, potom určite existuje také celé číslo y, že $x = 2y + 1$.

Ž: *Jasné. Dvojnásobok čísla y je párne číslo a ak k párnemu číslu pripočítam jednotku, tak dostanem nepárne číslo. A čo ďalej?*

U: Ak $x = 2y + 1$, tak $x^2 = (2y + 1)^2$. Myslím, že umocniť dvojčlen zvládneš aj sám.

Ž: *Samozrejme:*

$$x^2 = (2y + 1)^2 = 4y^2 + 4y + 1.$$

U: Vyšlo ti párne alebo nepárne číslo?

Ž: *Nepárne, pretože $4y^2$ a $4y$ sú párne a ak k ich súčtu pridám ešte jednotku, tak výsledok je nepárne číslo.*

U: Máš pravdu. Súčet $4y^2 + 4y$ je párny, lebo ho vieme napísať ako násobok dvojky:

$$4y^2 + 4y = 2 \cdot \left(2y^2 + 2y\right).$$

Ž: *Môžem teda dokončiť dôkaz:*

$$x^2 = 2 \cdot \left(2y^2 + 2y\right) + 1,$$

čo je nepárne číslo. Dôkaz je tým vykonaný.

U: Dobre. V rámčeku si ešte raz pozri reťazec implikácií, ktorý nás doviedol od predpokladu k záveru:

$$\boxed{\begin{array}{l} x \text{ je nepárne číslo} \quad \Rightarrow \\ \Rightarrow \quad \exists y \in \mathbb{Z}: \; x = 2y + 1 \quad \Rightarrow \\ \Rightarrow \quad x^2 = (2y+1)^2 = 4y^2 + 4y + 1 = 2 \cdot \left(2y^2 + 2y\right) + 1, \\ \qquad\quad \text{kde } 2y^2 + 2y \in \mathbb{Z} \quad \Rightarrow \\ \Rightarrow \quad x^2 \text{ je nepárne číslo.} \end{array}}$$

Úloha : *Nasledujúce vety dokážte priamo:*

a) Súčet dvoch nepárnych čísel je párne číslo,

b) $\forall n \in \mathbb{N} : 16 \mid (n^2 + 4n) \quad \Rightarrow \quad 2 \mid n.$

Návod:

b) $n^2 + 4n = n \cdot (n+4)\,, \quad 16 \mid n \cdot (n+4) \quad \Rightarrow \quad \exists k \in \mathbb{N} : n \cdot (n+4) = 16k = 2 \cdot (8k).$
Previesť úvahu, že súčin $n \cdot (n+4)$ je párny práve vtedy, ak oba jeho činitele sú párne. (Čísla n a $n+4$ sú obe súčasne párne alebo obe súčasne nepárne. Ak je ich súčin párny, tak obe musia byť párne.)

Príklad 5: *Nasledujúcu vetu dokážte nepriamo:*

$$\forall n \in \mathbb{N} : 5 \mid \left(n^2 + 1\right) \quad \Rightarrow \quad 5 \nmid n.$$

U: Ako sa postupuje pri nepriamom dôkaze implikácie?

Ž: *Vytvoríme si* **obmenu implikácie** *a tú potom priamo dokážeme.*

U: A ako dostaneme obmenenú implikáciu?

Ž: *Prehodíme poradie* **predpokladu** *a* **záveru implikácie***?*

U: Nie. To nestačí. Vytvoríš ***negáciu*** predpokladu aj záveru a prehodíš poradie týchto negácií. Takto:

$$\text{pôvodná implikácia je:} \qquad A \Rightarrow B,$$

$$\text{obmenená implikácia je:} \qquad B' \Rightarrow A'.$$

Ž: *Aha. Stále si to pletiem. Výrok A v našej implikácii je, že číslo 5 delí výraz v zátvorke. Výrok B je, že číslo 5 nedelí prirodzené číslo n. Ich negácie vytvorím ľahko, len sa deliteľnosť zamení za nedeliteľnosť a naopak. Dostanem tak:*

$$\textit{pôvodná implikácia:} \qquad \forall n \in \mathbb{N} : \quad 5 \mid \left(n^2 + 1\right) \quad \Rightarrow \quad 5 \nmid n,$$

$$\textit{obmenená implikácia:} \qquad \forall n \in \mathbb{N} : \quad 5 \mid n \quad \Rightarrow \quad 5 \nmid \left(n^2 + 1\right).$$

U: Správne. A teraz dokážeme priamo túto obmenu. Vyjdeš z predpokladu, že prirodzené číslo n je deliteľné číslom 5.

Ž: *Je teda jeho násobkom.*

U: Áno. Znamená to, že existuje také prirodzené číslo k, že platí:

$$n = 5k.$$

Ž: *Aha. Teraz by som mohol vytvoriť $n^2 + 1$ a využiť pri tom, že $n = 5k$.*

U: Urob to.

Ž: *Takže:*

$$n = 5k \quad \Rightarrow \quad n^2 + 1 = (5k)^2 + 1 = 25k^2 + 1.$$

U: Dobre. Ja to ešte upravím takto:

$$25k^2 + 1 = 5 \cdot \left(5k^2\right) + 1.$$

Je tento výraz deliteľný piatimi?

Ž: *Nie, nie je. Násobkom päťky je $25k^2$ a ďalší násobok päťky je od tohto čísla o 5 väčší. Výraz $25k^2 + 1$ je od násobku päťky väčší len o 1, takže nie je piatimi deliteľný.*

U: Ale to je presne to, čo sme chceli dokázať:

$$\forall n \in \mathbb{N} : \quad 5 \mid n \quad \Rightarrow \quad 5 \nmid \left(n^2 + 1\right).$$

Ostáva už len pripomenúť, že obmenená a pôvodná implikácia majú rovnakú pravdivostnú hodnotu.

Ž: *Ak teda platí obmenená implikácia, platí aj pôvodná:*

$$\forall n \in \mathbb{N}: \quad 5 \mid \left(n^2+1\right) \quad \Rightarrow \quad 5 \nmid n.$$

U: V rámčeku si môžeš ešte raz pozrieť, ako dôkaz prebiehal:

$$\frac{\forall n \in \mathbb{N}: \quad 5 \mid n \quad \Rightarrow \quad 5 \nmid \left(n^2+1\right)}{5 \mid n \quad \Rightarrow \quad \exists k \in \mathbb{N}: \ n = 5k \quad \Rightarrow}$$

$$\Rightarrow \quad n^2+1 = (5k)^2 + 1 = 25k^2 + 1 = 5 \cdot \left(5k^2\right) + 1 \quad \Rightarrow$$

$$\Rightarrow \quad 5 \nmid \left(n^2+1\right).$$

Úloha : *Nasledujúce vety dokážte nepriamo:*

a) $\forall n \in \mathbb{N}: 3 \mid (n^2+1) \quad \Rightarrow \quad 6 \nmid n$,
b) $\forall n \in \mathbb{N}: 3 \nmid (n^4+2) \quad \Rightarrow \quad 3 \mid n$,
c) $\forall n \in \mathbb{N}: 2 \nmid (n^2-10) \quad \Rightarrow \quad 2 \nmid n$.

Návod:
b) $3 \nmid n \quad \Rightarrow \quad \exists k \in \mathbb{N}: \ n = 3k+1 \ \vee \ n = 3k+2$. *Rozobrať obe možnosti.*

Príklad 6: *Nasledujúcu vetu dokážte sporom:*

Pre každé celé číslo m platí: Ak je m^2 nepárne číslo, tak je aj m nepárne číslo.

U: Najprv si zapíšeme našu vetu pomocou matematických symbolov:

$$\forall m \in \mathbb{Z}: \ m^2 \text{ je nepárne číslo} \quad \Rightarrow \quad m \text{ je nepárne číslo}.$$

Ako sa postupuje pri dokazovaní implikácie sporom?

Ž: *Vytvoríme si jej* **negáciu** *a tú sa pokúsime dokázať. Mali by sme dôjsť k nejakému spornému tvrdeniu, k nepravde.*

U: Dobre. Ako vyzerá negácia implikácie?

Ž: **Predpoklad implikácie** *ostane nezmenený. A má platiť súčasne s negáciou* **záveru implikácie**. *Takto:*

$$\textit{pôvodná implikácia je:} \qquad A \Rightarrow B,$$

$$\textit{negácia implikácie je:} \qquad A \wedge B'.$$

U: Správne. A v našom prípade?

Ž: *Predpoklad implikácie, teda výrok A je, že m^2 je nepárne číslo. Záver implikácie, teda výrok B je, že m je tiež nepárne číslo. Ten znegujem.*

U: A čo ***kvantifikátor***?

Ž: *Všeobecný kvantifikátor $\forall$ zamením za existenčný $\exists$.*

$$\textit{pôvodná implikácia:} \qquad \forall m \in \mathbb{Z}: \ m^2 \textit{ je nepárne číslo} \quad \Rightarrow \quad m \textit{ je nepárne číslo},$$

$$\textit{negácia implikácie:} \qquad \exists m \in \mathbb{Z}: \ m^2 \textit{ je nepárne číslo} \quad \wedge \quad m \textit{ je párne číslo}.$$

U: Dobre. Všetko sme si pripravili, môžeme začať so samotným dôkazom negácie.

Ž: *Predpokladáme teda, že existuje také párne číslo m, že jeho druhá mocnina je nepárne číslo. Ale ak m je párne, tak existuje také celé číslo k, že*

$$m = 2k.$$

Druhá mocnina čísla m je

$$m^2 = (2k)^2 = 4k^2.$$

U: Vytvorené číslo zapíšeme takto:

$$4k^2 = 2 \cdot \left(2k^2\right).$$

Je to párne alebo nepárne číslo?

Ž: *Samozrejme, že párne.*

U: Predpokladali sme, že existuje také párne celé číslo, že jeho druhá mocnina je nepárna a došli sme k tomu, že jeho druhá mocnina je párna.

Ž: *To je predsa hlúposť. Žiadne číslo, ani ak ide o druhú mocninu, nemôže byť párnym aj nepárnym naraz.*

U: To je to sporné, nepravdivé tvrdenie, ku ktorému sme chceli dôjsť. Keďže negácia našej vety vedie k sporu, znamená to, že nie je pravdivá.

Ž: *A teda pravdivá je pôvodná veta:*

$$\forall m \in \mathbb{Z}: \ m^2 \textit{ je nepárne číslo} \quad \Rightarrow \quad m \textit{ je nepárne číslo}.$$

U: Dobre. V rámčeku si ešte raz pozri, ako prebiehal dôkaz:

$$\boxed{\begin{array}{l}
\exists m \in \mathbb{Z}: \ m^2 \text{ je nepárne číslo} \quad \wedge \quad m \text{ je párne číslo} \quad \Rightarrow \\
\Rightarrow \quad m^2 \text{ je nepárne číslo} \quad \wedge \quad \exists k \in \mathbb{Z}: m = 2k \quad \Rightarrow \\
\Rightarrow \quad m^2 \text{ je nepárne číslo} \quad \wedge \quad m^2 = (2k)^2 = 4k^2 \quad \Rightarrow \\
\Rightarrow \quad m^2 \text{ je nepárne číslo} \quad \wedge \quad m^2 = 2 \cdot \left(2k^2\right) \quad \Rightarrow \\
\underline{\Rightarrow \quad m^2 \text{ je nepárne číslo} \quad \wedge \quad m^2 \text{ je párne číslo} \ldots SPOR} \quad \Rightarrow \\
\forall m \in \mathbb{Z}: \ m^2 \text{ je nepárne číslo} \quad \Rightarrow \quad m \text{ je nepárne číslo}
\end{array}}$$

Úloha : *Nasledujúce vety dokážte sporom:*

a) $\forall m \in \mathbb{Z}$: *Ak je* m^2 *párne číslo, tak je aj* m *párne číslo,*

b) $\forall n \in \mathbb{N}: \ 5 \mid (n^2+1) \quad \Rightarrow \quad 10 \nmid n$,

c) $\forall n \in \mathbb{N}: \ 10 \mid (n^2+6) \quad \Rightarrow \quad 5 \nmid n$.

Príklad 7: *Nasledujúcu vetu dokážte matematickou indukciou:*

$$\forall n \in \mathbb{N}: \ 3 \mid \left(n^3 + 23n\right).$$

U: Pomocou ***matematickej indukcie*** máme dokázať platnosť výrokovej formy:

$$V(n): \ 3 \mid \left(n^3 + 23n\right),$$

pre ľubovoľné prirodzené číslo n.

Ž: *Dôkaz matematickou indukciou spočíva v dvoch krokoch:*
I.krok: *Za premennú n si dosadíme najmenšie prirodzené číslo, pre ktorú má veta platiť. V našom prípade je to číslo 1.*

U: Dosadením hodnoty 1 za n sa z výrokovej formy stane výrok. Overiť jeho pravdivosť by pre teba nemal byť problém.

Ž: *Jasné:*
pre $n = 1$ dostaneme $1^3 + 23 \cdot 1 = 1 + 23 = 24$,

$$V(1): \ 3 \mid 24 \quad \textit{platí.}$$

U: Dobre. Bolo to jednoduché, však? Môžeme teda prejsť na druhý krok dôkazu.

Ž: *II.krok*: *Dokážeme, že pre ľubovoľné prirodzené číslo n platí implikácia*

$$V(n) \quad \Rightarrow \quad V(n+1).$$

U: A čo tým vlastne dosiahneš?

Ž: *Rozumiem tomu tak, že v prvom kroku sme* **dokázali platnosť vety pre jedno konkrétne číslo**. *A v druhom kroku* **predpokladáme platnosť vety pre nejaké číslo** n *a dokážeme, že potom* **veta platí aj pre číslo** $n+1$.

U: Teoreticky ti to ide. Poďme teda na praktickú časť.

Ž: *Najprv si pripravím* **indukčný predpoklad** *a* **indukčné tvrdenie***:*
$V(n): \ 3 \mid (n^3 + 23n) \ \ldots$ *indukčný predpoklad,*
$V(n+1): \ 3 \mid \left[(n+1)^3 + 23 \cdot (n+1)\right] \ \ldots$ *indukčné tvrdenie.*

U: Vyjdeme teraz z výrazu, ktorý je v indukčnom tvrdení:

$$(n+1)^3 + 23 \cdot (n+1).$$

Nože ho trošku uprav.

Ž: *Prvú zátvorku umocním na tretiu podľa vzorca*

$$(A+B)^3 = A^3 + 3A^2B + 3AB^2 + B^3,$$

pričom $A = n$ a $B = 1$. A druhú zátvorku len roznásobím:

$$\boxed{(n+1)^3 + 23 \cdot (n+1) = n^3 + 3n^2 + 3n + 1 + 23n + 23}$$

U: Dobre. Ja zmením poradie sčítancov, sčítam čísla 1 a 23 a z niektorých sčítancov vyberiem pred zátvorku číslo 3:

$$\boxed{\begin{aligned} n^3 + 23n + 3n^2 + 3n + 1 + 23 &= \\ = n^3 + 23n + 3n^2 + 3n + 24 &= \\ = n^3 + 23n + 3 \cdot \left(n^2 + 3n + 24\right) & \end{aligned}}$$

Ž: *A prečo práve takáto úprava?*

U: Teraz totiž môžeme na prvé dva sčítance využiť indukčný predpoklad:

$$\boxed{\underbrace{\color{red}{n^3 + 23n}}_{3|(n^3+23n)} + \underbrace{3 \cdot \left(n^2 + 3n + 24\right)}_{3|3\cdot(n^2+3n+24)}}$$

Ž: *Aha. Podľa indukčného predpokladu číslo* 3 *delí výraz* $n^3 + 23n$*. A z tých ďalších sčítancov sa trojka vybrala pred zátvorku, takže číslo* 3 *delí aj výraz* $3 \cdot (n^2 + 3n + 24)$.

U: Áno. A ak sú dva sčítance deliteľné číslom 3, tak je týmto číslom deliteľný aj ich súčet.

Ž: *To ale znamená, že číslo* 3 *delí výraz* $n^3 + 23n + 3 \cdot (n^2 + 3n + 24)$*. Ten sme ale dostali úpravou výrazu* $(n+1)^3 + 23 \cdot (n+1)$.

U: A to je to, čo sme chceli dokázať. Využitím indukčného predpokladu sme dokázali platnosť indukčného tvrdenia. Ak platí $V(n)$, tak platí aj $V(n+1)$.

Ž: *V našom prípade, ak teda* $3 \mid (n^3 + 23n)$*, tak* $3 \mid \left[(n+1)^3 + 23 \cdot (n+1)\right]$.

U: Dokázali sme pravdivosť implikácie. A vďaka prvému kroku máme číslo, pre ktoré výrok platí určite.

Ž: *Ak teda platí pre číslo* $n = 1$*, tak platí aj pre* $n = 2$*. Ak platí pre* $n = 2$*, tak platí aj pre* $n = 3$*. A tak ďalej.*
Pre každé prirodzené číslo n platí, že $3 \mid (n^3 + 23n)$.

Úloha : *Nasledujúce vety dokážte matematickou indukciou:*
a) $\forall n \in \mathbb{N} : \ 6 \mid (10^n + 2)$,
b) $\forall n \in \mathbb{N} : \ 3 \mid (n^3 + 2n)$.

Príklad 8: *Nasledujúcu vetu dokážte matematickou indukciou:*

$$\forall n \in \mathbb{N} : \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{n}{n\cdot(n+1)}=\frac{n}{n+1}.$$

U: Pomocou ***matematickej indukcie*** máme dokázať platnosť výrokovej formy:

$$V(n) : \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1},$$

pre ľubovoľné prirodzené číslo n.

Ž: *Dôkaz matematickou indukciou spočíva v dvoch krokoch:*
I.krok: *Za premennú n si dosadíme najmenšiu hodnotu, pre ktorú má veta platiť a zistíme, či naozaj platí.*

U: A čo je tou najmenšiou hodnotou?

Ž: *Najmenšie prirodzené číslo je 1. Dosadením hodnoty 1 za n sa z výrokovej formy stane výrok. Overiť jeho pravdivosť by som mal zvládnuť. Dosadím si do ľavej aj pravej strany nášho tvrdenia hodnotu 1 a zistím, či sa rovnajú:*

$$\boxed{\begin{aligned}&V(1): \frac{1}{1\cdot(1+1)} \stackrel{?}{=} \frac{1}{1+1}\\ &Ľ=\frac{1}{1\cdot(1+1)}=\frac{1}{1\cdot 2}=\frac{1}{2},\\ &P=\frac{1}{1+1}=\frac{1}{2},\\ &Ľ=P \Rightarrow V(1)\ \textit{platí.}\end{aligned}}$$

U: Dobre. Pre prirodzené číslo $n = 1$ teda tvrdenie $V(n)$ zo zadania úlohy platí. To bola tá jednoduchšia časť dôkazu. Teraz príde tá krajšia.

Ž: *II.krok*: *Dokážeme, že pre ľubovoľné prirodzené číslo n platí implikácia*

$$V(n) \quad \Rightarrow \quad V(n+1).$$

U: A čo tým vlastne dosiahneš?

Ž: *Rozumiem tomu tak, že v prvom kroku sme* **dokázali platnosť vety pre jedno konkrétne číslo**. *A v druhom kroku ukážeme, že ak* **veta platí pre nejaké číslo** n, *tak potom* **platí aj pre číslo** $n+1$.

U: Teoreticky ti to ide. Poďme teda na praktickú časť.

Ž: *Najprv si pripravím* **indukčný predpoklad** $V(n)$ *a* **indukčné tvrdenie** $V(n+1)$*:*

$$V(n): \quad \frac{1}{1\cdot2}+\frac{1}{2\cdot3}+\frac{1}{3\cdot4}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$$

$$V(n+1): \quad \frac{1}{1\cdot2}+\frac{1}{2\cdot3}+\frac{1}{3\cdot4}+\cdots+\frac{1}{n\cdot(n+1)}+\frac{1}{(n+1)\cdot(n+1+1)}=\frac{n+1}{n+1+1}$$

U: Dobre. Indukčné tvrdenie si môžeš ešte trošku upraviť, aby si vedel, k čomu máš dôjsť.

Ž: *Jasné, sčítam tie jednotky v poslednom zlomku:*

$$\boxed{V(n+1):\ \ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}+\frac{1}{(n+1)\cdot(n+2)}=\frac{n+1}{n+2}}$$

U: A teraz sa pokúsime dostať od indukčného predpokladu k indukčnému tvrdeniu.

Ž: *Teda z jednej rovnice dostať druhú.*

U: Áno. Všimni si najprv ľavé strany oboch rovníc. Čím sa líšia?

Ž: *Na ľavej strane indukčného tvrdenia je navyše jeden sčítanec.*

U: Dobre. Pripočítame ho teda k rovnici v indukčnom predpoklade. Ale, aby si nemusel toľko opisovať, tak súčet prvých n sčítancov si označíme ako S – tento súčet je rovnaký v indukčnom predpoklade aj v indukčnom tvrdení:

$$\boxed{\underbrace{\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}}_{S}\,.}$$

Ž: *Môžeme teda písať:*

$$V(n):\quad S=\frac{n}{n+1},$$
$$V(n+1):\ S+\frac{1}{(n+1)\cdot(n+2)}=\frac{n+1}{n+2}.$$

K rovnici v indukčnom predpoklade teraz pripočítam zlomok $\frac{1}{(n+1)\cdot(n+2)}$*:*

$$\begin{aligned} S&=\frac{n}{n+1}\ \Big/+\frac{1}{(n+1)\cdot(n+2)}\\ S+\frac{1}{(n+1)\cdot(n+2)}&=\frac{n}{n+1}+\frac{1}{(n+1)\cdot(n+2)}\end{aligned}$$

U: Dobre. Ľavá strana tejto rovnice je už rovnaká ako ľavá strana indukčného tvrdenia. Treba ešte zistiť, či po úprave pravej strany tejto rovnice sa aj ona bude rovnať pravej strane indukčného tvrdenia.

Ž: *Aha. Tak budem upravovať už len pravú stranu. Zlúčim tie dva zlomky, ktoré tam mám, na spoločného menovateľa:*

$$\boxed{S+\frac{1}{(n+1)\cdot(n+2)}=\frac{n\cdot(n+2)+1}{(n+1)\cdot(n+2)}}$$

U: Teraz roznásob zátvorku v čitateli. Menovateľa už neupravuj.

Ž: *Dobre:*

$$\boxed{S+\frac{1}{(n+1)\cdot(n+2)}=\frac{n^2+2n+1}{(n+1)\cdot(n+2)}}$$

U: V čitateli pravej strany sme dostali rozklad druhej mocniny výrazu $(n+1)$.

Ž: *Tak to tam napíšem:*

$$\boxed{\begin{array}{c} S+\dfrac{1}{(n+1)\cdot(n+2)}=\dfrac{(n+1)^2}{(n+1)\cdot(n+2)} \\ S+\dfrac{1}{(n+1)\cdot(n+2)}=\dfrac{n+1}{n+2} \end{array}}$$

Na pravej strane som ešte vykrátil čitateľa aj menovateľa výrazom $n+1$.

U: Tak sa pozrime, čo sme to vlastne dostali. Ekvivalentnými úpravami sme z rovnice, ktorá predstavovala indukčný predpoklad, dostali rovnicu, ktorá je indukčným tvrdením. Z platnosti indukčného predpokladu sme dokázali platnosť indukčného tvrdenia. Tým je dôkaz matematickou indukciou hotový.

Ž: **Tvrdenie**

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{n}{n\cdot(n+1)}=\frac{n}{n+1}$$

platí teda pre každé prirodzené číslo n.

Úloha : *Nasledujúcu vetu dokážte matematickou indukciou:*

$$\forall n\in\mathbb{N}:\ 1^2+2^2+3^2+\cdots+n^2=\frac{n\cdot(n+1)\cdot(2n+1)}{6}.$$