Matematika – krátký přehled důkazových metod

Podobně jako prací chirurga je kromě zdravotní prevence i řezat a prací poštovního doručovatele je doručování korespondence, prací matematickou je kromě počítání i dokazování či zdůvodňování zákonitostí, které platí a na jejichž základě se dějí různé početní algoritmy a odehrává se veškerý svět matematických pojmů a skutečností.

Věnujme se v tomto krátkém přehledu čtyřem typům zdůvodnovacích-dokazovacích technik: 1) přímý důkaz implikace, 2) nepřímý důkaz implikace, 3) důkaz sporem, 4) důkaz úplnou matematickou indukcí.

Základní kategorie při výstavbě matematiky

Matematika je věda o přesném vyjadřování, a my se nyní tento jazyk budeme učit – jinými slovy, budeme se učit a) přesně formulovat pojmy, b) přesně formulovat, ze kterých jednoduchých a platných faktů vycházíme, c) dokazovat platnost nových faktů na základě faktů samozřejmých nebo dokázaných už dříve.

(matematická) definice je přesné vymezení pojmu, z něhož je patrno, které objekty toto vymezení splňují a které ne (např. bod, úsečka, přímka, kružnice, úhel, rovnoběžka ... to vše jsou pojmy, které musíme jednoznačně definovat v tzv. Euklidovské geometrii).

(matematický) axiom je tvrzení o vlastnostech pojmů či o vztazích mezi pojmy, které se nedokazuje, nýbrž všeobecně přijímá jako pravdivé (např. axiomy Euklidovské geometrie).

(matematická) věta je tvrzení o vlastnostech pojmů či vztazích mezi pojmy, které musíme dokázat pomocí axiomů, definic a vět dokázaných již dříve.

Typ důkazu číslo 01: Přímý důkaz implikace $A \Rightarrow B$.

Při přímém důkazu implikace $A \Rightarrow B$ vyjdeme z toho, že platí výrok A; na základě posloupnosti zřejmých implikací pak vyvozujeme další skutečnosti, až dospějeme k výroku B.

Příklad 1. Dokažte: Pro přirozená čísla a, b, c platí:

$$a|b \wedge a|c \Rightarrow a|(b+c)$$

(pro neznalce značek symbolických: Jestliže číslo a je dělitelem čísla b a současně číslo a je dělitelem čísla c, tak také číslo a je dělitelem součtu čísel $(b+c)$).

Důkaz: Uvedený výrok z oblasti dělitelnosti je celkem triviální a běžně ho používáme, ale i ten by matematický přístup měl dokázat zdůvodnit.

Výrok A v našem případě říká: $a|b \wedge a|c$.

Z toho zřejmě plyne: existují přirozená čísla k, l taková, že $b = k \cdot a$ a současně $c = l \cdot a$.

Z toho zřejmě plyne: zkoumejme nyní, zda je číslo $(b+c)$ dělitelné číslem a:

$$b + c = k \cdot a + l \cdot a = (k + l) \cdot a.$$

Z toho, že $(b+c) = a\cdot(k+l)$, plyne, že číslo a je dělitelem čísla $(b+c)$. Důkaz je hotov. $\square$

Typ důkazu číslo 2: NEpřímý důkaz implikace $A \Rightarrow B$.

Při NEpřímém důkazu implikace $A \Rightarrow B$ vlastně dokazujeme platnost logicky s ní ekvivalentní formy $\neg B \Rightarrow \neg A$.

Forma $\neg B \Rightarrow \neg A$ se nazývá obměna implikace $A \Rightarrow B$[1].

Příklad 2. Dokažte matematickou větu: Pro každé přirozené číslo n platí:

$$2|n^2 \quad \Rightarrow \quad 2|n$$

(pro neznalce matematických symbolů: jestliže číslo 2 je dělitelem čísla n^2, tak také je číslo 2 dělitelem čísla n).

Důkaz: Máme dokázat implikaci typu $A \Rightarrow B$. Někdy (a to bude právě v našem případě) je ovšem jednodušší dokazovat logickou obměnu $\neg B \Rightarrow \neg A$ neboli výrok

$$2 \not| n \quad \Rightarrow \quad 2 \not| n^2$$

(pro neznalce: Jestliže číslo 2 není dělitelem čísla n, tak také číslo 2 není dělitelem čísla n^2).

Vycházíme nyní z výroku $\neg B$: $2 \not| n$;

Z toho zřejmě plyne: tedy n je liché a lze je psát ve tvaru $n = 2k+1$, kde k je přirozené číslo nebo nula.

Z toho zřejmě plyne: n^2 lze vyjádřit ve tvaru

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1;$$

odtud je evidentní, že n^2 je číslo liché, a tedy není dělitelné dvěma. Důkaz je hotov: tím, že jsme prokázali platnost výroku $\neg B \Rightarrow \neg A$, prokázali jsme současně i platnost výroku k němu logicky ekvivalentního, tj. $A \Rightarrow B$. $\square$

Typ důkazu číslo 03: Důkaz sporem.

Předpokládáme platnost negace daného tvrzení a logicky správně z této negace pomocí řetězce přímých implikací (jako u důkazu přímého) odvozujeme další věci, které zřejmě platí, dokud nedojdeme k nesmyslu, který neplatí. Protože jsme pracovali logicky naprosto správně, tak kořen rozporu je ve startovacím předpokladu – nyní víme, že předpoklad $\neg A$ neplatí, a tedy platí výrok A.

Příklad 3. Dokažte, že $\log_2 3$ není racionální číslo.

[1]Obměna implikace je tedy výrok s touto implikací logicky ekvivalentní, tj. provést nepřímý důkaz implikace $A \Rightarrow B$ vlastně znamená provést přímý důkaz její obměny $\neg B \Rightarrow \neg A$.

Důkaz: budeme předpokládat negaci zadaného výroku, tj. že $\log_2 3$ je racionální číslo, tj. lze tuto hodnotu vyjádřit zlomkem:

$$\log_2 3 = \frac{m}{n}$$

pro $m \in Z$ a $n \in N$.

Potom z definice logaritmu plyne

$$2^{\frac{m}{n}} = 3.$$

Z toho zřejmě plyne umocněním vztahu na n-tou:

$$2^m = 3^n,$$

a na obou stranách této rovnosti se přitom vyskytují přirozená čísla.

Odtud zřejmě plyne: Protože číslo 2 je dělitelem čísla 2^m a platí $2^m = 3^n$, musí být číslo 2 také dělitelem čísla 3^n – ale to je spor se známým faktem, že číslo 2 není dělitelem žádného lichého čísla (a číslo 3^n jako násobek n lichých čísel je liché).

Naprosto korektními úvahami jsme přišli k nesmyslu, tj. nesprávný byl náš výchozí předpoklad – a tedy platí jeho negace: $\log_2 3$ není racionální číslo. $\square$

Typ důkazu číslo 04: Důkaz úplnou matematickou indukcí.

Při matematické indukci dokazujeme tzv. univerzální výrok, který platí většinou pro všechna přirozená čísla, která jsou větší nebo rovna přirozenému číslu n_0, tj. výroky typu

$$\forall n \geq n_0 : V(n).$$

Platnost tohoto univerzálního výroku dokazujeme ve dvou krocích:

a) Dokážeme platnost výroku $V(n_0)$ pro nejmenší možné přirozené číslo, pro které výrok platí. Obvykle $n_0 = 1$.

b) Dokážeme platnost implikace $V(n) \Rightarrow V(n+1)$.

Pokud platí obě tyto věci, bude tím dokázána platnost výroku $V(n)$ pro jakékoli přirozené číslo n.

Příklad 4. Dokažte indukcí: Pro každé přirozené číslo n platí: $3|(n^3 + 2n)$ (číslo 3 je dělitelem čísla $(n^3 + 2n)$).

Důkaz:

a) $V(1)$: pro $n = 1$ ... $3|(1^3 + 2 \cdot 1)$ ... tento výrok evidentně platí.

b) Dokážeme platnost implikace $V(n) \Rightarrow V(n+1)$. Pro výrok tohoto příkladu implikace nabývá tvar

$$3|(n^3 + 2n) \quad \Rightarrow \quad 3|((n+1)^3 + 2(n+1)).$$

Dokažme tuto implikaci některým ze způsobů důkazu implikace, většinou to bude důkaz typu 1, tj. důkaz přímý: Předpokládejme, že $3|(n^3+2n)$ a chceme pomocí řetězce zřejmých implikací dokázat platnost výroku $3|((n+1)^3+2(n+1))$:

Prozkoumejme blíže číslo $((n+1)^3+2(n+1))$:

$((n+1)^3+2(n+1) = n^3+3n^2+3n+1+2n+2 = (n^3+2n)+(3n^2+3n+3)$.

A nyní: první z obou sčítaných závorek je dělitelná třemi, na základě toho, že jsme tuto skutečnost předpokládali na začátku tohoto důkazu (jedná se o výrok $V(n)$). Druhá z obou sčítaných závorek je dělitelná třemi proto, že ji lze upravit do tvaru $3\cdot(n^2+n+1)$. A tedy (podle tvrzení v příkladu 1) i součet dvou těchto závorek je dělitelný třemi.

Příklad 5. Dokažte indukcí: Pro každé přirozené číslo n platí:

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

Důkaz:

i) $n=1$ – dosadíme do obou stran rovnosti: $1 = \frac{1\cdot 2}{2}$ ... platí[2]

ii) Předpokládáme platnost indukčního předpokladu: Vzorec platí pro n, tj.

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

A odtud nyní dokážeme platnost vztahu (= chceme dokázat) pro $(n+1)$:

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

Zkusme upravit levou stranu dokazované rovnosti s využitím pravé strany indukčního předpokladu (a poté převedeme na společného jmenovatele a vytkneme člen $(n+1)$ v čitateli):

$$\underbrace{1+2+\cdots+n}_{=\frac{n(n+1)}{2}}+(n+1) \overset{ind.p.}{=} \frac{n\cdot(n+1)}{2}+(n+1) = \frac{n\cdot(n+1)+2\cdot(n+1)}{2} = \frac{(n+1)\cdot(n+2)}{2}.$$

A to jsme chtěli dokázat, důkaz je hotov. S využitím platnosti vztahu pro n jsme jej dokázali pro $(n+1)$.

[2]Při tomto prvním kroku důkazu indukcí stačí dokázat platnost pro $n=1$; podívejme se ovšem nyní už „mimo plán“ na případy $n=2$, $n=3$, protože z nich bude zřejmé, jak se pak konstruuje rovnice pro obecné n:

$n=2$ – dosadíme do obou stran: $1+2 = \frac{2\cdot 3}{2}$ ... platí.

$n=3$ – dosadíme do obou stran: $1+2+3 = \frac{3\cdot 4}{2}$ ... platí.