Matematické dovednosti

Důkazové techniky

Důkaz (přímý)

Co je to důkaz?

Posloupnost (konečná) pravdivých tvrzení:

- axiomy, axiomy teorie
- dříve dokázaná tvrzení
- odvození nového tvrzení z již dokázaných (platí-li A a $A \Rightarrow B$, pak platí B)
- dedukce: dokázat $A \Rightarrow B$ v teorii T je totéž, jako dokázat B v teorii $T \cup \{A\}$
- tranzitivita implikace: platí-li $A \Rightarrow B$ a $B \Rightarrow C$, pak platí $A \Rightarrow C$
- končí dokazovaným tvrzením

AG nerovnost

Tvrzení

$$\forall x, y \in \mathbb{R}^+ : \frac{x+y}{2} \geq \sqrt{xy}$$

Důkaz:

$$\begin{aligned}
\frac{x+y}{2} &\geq \sqrt{xy} \\
\frac{(x+y)^2}{4} &\geq xy \\
(x+y)^2 &\geq 4xy \\
x^2 + 2xy + y^2 &\geq 4xy \\
x^2 - 2xy + y^2 &\geq 0 \\
(x-y)^2 &\geq 0
\end{aligned}$$

AG nerovnost

Tvrzení

$$\forall x, y \in \mathbb{R}^+ : \frac{x+y}{2} \geq \sqrt{xy}$$

Důkaz:

$$\begin{aligned}
\tfrac{x+y}{2} &\geq \sqrt{xy} \\
\tfrac{(x+y)^2}{4} &\geq xy \\
(x+y)^2 &\geq 4xy \\
x^2 + 2xy + y^2 &\geq 4xy \\
x^2 - 2xy + y^2 &\geq 0 \\
(x-y)^2 &\geq 0
\end{aligned}$$

$$\begin{aligned}
(x-y)^2 &\geq 0 \\
x^2 - 2xy + y^2 &\geq 0 \\
x^2 + 2xy + y^2 &\geq 4xy \\
(x+y)^2 &\geq 4xy \\
\tfrac{(x+y)^2}{4} &\geq xy \\
\tfrac{x+y}{2} &\geq \sqrt{xy}
\end{aligned}$$

Nepřímý důkaz

Tvrzení

Je-li součin dvou celých čísel lichý, jsou obě čísla lichá.

Důkaz:

$$2 \not\backslash (ab) \Rightarrow (2 \not\backslash a \wedge 2 \not\backslash b)$$

obměna implikace

$$(2 \backslash a \vee 2 \backslash b) \Rightarrow 2 \backslash (ab)$$

rozborem případů

$2 \backslash a$	$2 \backslash b$
$\exists k \in \mathbb{Z} : a = 2k$	$\exists \ell \in \mathbb{Z} : b = 2\ell$
$ab = (2k)b = 2(kb)$	$ab = a(2\ell) = 2(a\ell)$
$2 \backslash (ab)$	$2 \backslash (ab)$

Důkaz sporem

Tvrzení

Odmocnina ze dvou je iracionální.

Důkaz: pro spor ať $\sqrt{2} \in \mathbb{Q}$

$$
\begin{aligned}
&\exists p, q \in \mathbb{Z} : \sqrt{2} = \tfrac{p}{q}, NSD(p, q) = 1 \\
&2 = \tfrac{p^2}{q^2} \\
&2q^2 = p^2 \\
&2 \backslash p^2, 2 \backslash p \\
&\exists r \in \mathbb{Z} : p = 2r \\
&2q^2 = (2r)^2 = 4r^2 \\
&q^2 = 2r^2 \\
&2 \backslash q^2, 2 \backslash q \\
&NSD(p, q) \geq 2
\end{aligned}
$$

Matematická indukce

Tvrzení

Součet prvních n lichých přirozených čísel je n^2.

Důkaz: k-té liché číslo je $2k-1$, chceme dokázat $\sum_{k=1}^{n}(2k-1)=n^2$.
Matematickou indukcí dle n
$n=1$:

$$L_1=\sum_{k=1}^{1}(2k-1)=1=1^2=P_1$$

$n \to n+1$: „$L_n = P_n \Rightarrow L_{n+1} = P_{n+1}$“

$$\begin{aligned} L_{n+1} &= \sum_{k=1}^{n+1}(2k-1)=\sum_{k=1}^{n}(2k-1)+(2(n+1)-1)=L_n+(2n+1)= \\ &= P_n+(2n+1)=n^2+2n+1=(n+1)^2=P_{n+1} \end{aligned}$$

Silná indukce

Tvrzení
Každé přirozené číslo větší než jedna má prvočíselného dělitele.

Důkaz: Matematickou indukcí dle n

n prvočíslo: $n \backslash n$

ind. krok: „$\forall k < n T_k \Rightarrow T_n$“

n prvočíslo – viz. první krok

n složené – $\exists k, \ell \in \mathbb{Z} : k, \ell \geq 2 \wedge n = k\ell$
dle IP je pro $k < n$ tvrzení pravdivé, tedy ex. prvočíslo p dělící k
$p \backslash k \wedge k \backslash n \Rightarrow p \backslash n$

Minimální protipříklad

Tvrzení

Každé přirozené číslo větší než jedna má prvočíselného dělitele.

Důkaz: sporem – ať existuje $n \geq 2$ takové, že n nemá žádného prvočíselného dělitele

volme n minimální takové
určitě n není prvočíslo

n je složené – $\exists k, \ell \in \mathbb{Z} : k, \ell \geq 2 \wedge n = k\ell$
jelikož $k < n$, není k protipříklad
existuje prvočíslo p dělící k
$p \backslash k \wedge k \backslash n \Rightarrow p \backslash n$

Důkaz existence

Tvrzení
Pro každá dvě racionální čísla a, b*, kde* $a < b$*, existuje racionální číslo* x *splňující* $a < x < b$*.*

Důkaz:

$$x = \frac{a+b}{2}$$

musíme ukázat, že

- $x \in \mathbb{Q}$
- $a < x < b$

Tvrzení
Pro každá dvě reálná čísla a, b*, kde* $a < b$*, existuje* $x \in \mathbb{Q}$ *splňující* $a < x < b$*.*

Jednoznačnost

Tvrzení

Polynom $x^3 + x - 1$ *má práve jeden reálný kořen.*

Důkaz:

Existence:

$f(0) = -1$, $f(1) = 1$, tedy existuje $x \in (0,1)$ pro které je $f(x) = 0$

Jednoznačnost:

$f'(x) = 3x^2 + 1$ je vždy kladná a tedy f je ryze rostoucí na celém $\mathbb{R}$

Jednoznačnost

Tvrzení

Nechť $A \in \mathbb{R}^{n \times n}$ je regulární matice, pak pro $\forall b \in \mathbb{R}^n$ má rovnice $Ax = b$ právě jednořešení.

Důkaz:

Existence:

$x = A^{-1}b$ je řešením, neboť $Ax = A(A^{-1}b) = (AA^{-1})b = Ib = b$

Jednoznačnost:

ať x, y dvě řešení, tedy $Ax = b = Ay$, pak

$$A(x - y) = Ax - Ay = b - b = 0$$

takže $x - y$ je řešením $Az = 0$

z regularity A má taková rovnice pouze nulové řešení

tedy $x - y = 0$ a nutně $x = y$

Ftip