Důkazy, značení, množiny, relace

Zdeněk Dvořák

3. října 2018

V matematice se nespoléháme na fakt, že něco platí ve všech pozorovaných případech.

Příklad 1.

$$A(n) = \left\lceil \frac{2}{\sqrt[n]{2}-1} \right\rceil$$

$$B(n) = \left\lfloor \frac{2n}{\log 2} \right\rfloor$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$A(n)$	2	5	8	11	14	17	20	23	25	28	31	34	37	40	43
$B(n)$	2	5	8	11	14	17	20	23	25	28	31	34	37	40	43

$$A(777451915729368) = 2243252046704767$$

$$B(777451915729368) = 2243252046704766$$

Důkaz: logické odvození z **axiomů**.

1 Typy důkazů

1.1 Sporem

Místo dokazování tvrzení „Platí A.“ vyvracíme tvrzení „Neplatí A.“

Věta 1. *Existuje nekonečně mnoho prvočísel.*

Důkaz. Pro spor předpokládejme, že existuje jen konečně mnoho prvočísel $p_1, \ldots, p_n$. Uvažujme číslo $k = p_1 p_2 \cdots p_n + 1$. Toto číslo není dělitelné $p_1, \ldots, p_n$. Ale každé přirozené číslo větší než 1 je dělitelné nějakým prvočíslem, což dává spor. Prvočísel tedy existuje nekonečně mnoho. □

Častou variantou je vyvrácení existence minimálního protipříkladu.

Lemma 2. *Každé přirozené číslo větší než* 1 *je dělitelné nějakým prvočíslem.*

Důkaz. Pro spor předpokládejme, že existuje nějaké přirozené číslo větší než 1, které není dělitelné žádným prvočíslem. Nechť n je nejmenší takové číslo. Jelikož n je dělitelné sebou samým, n není prvočíslo. Proto existuje nějaké přirozené číslo a různé od 1 a n, které dělí n. Jelikož $a < n$ (tedy a je menší než hypotetický nejmenší protipříklad na Lemma 2), číslo a je dělitelné nějakým prvočíslem p. Ale jelikož $p|a$ a $a|n$, dostáváme, že prvočíslo p dělí i n, což je spor. □

2 Matematickou indukcí

Mějme tvrzení $A(n)$ o přirozeném čísle n. Abychom dokázali, že $A(n)$ platí pro všechna přirozená čísla n, dokazujeme pro každé n „jestliže $A(m)$ platí pro všechna přirozená čísla $m < n$, pak platí $A(n)$“.

Lemma 3. *Každé přirozené číslo n různé od* 1 *je dělitelné nějakým prvočíslem.*

Důkaz. Nechť n je libovolné přirozené číslo různé od 1. Důkaz provedeme indukcí, předpokládáme tedy, že každé přirozené číslo menší než n a různé od 1 je dělitelné nějakým prvočíslem.

Jestliže n je prvočíslo, pak tvrzení zjevně platí, jelikož $n|n$. Jestliže n není prvočíslo, pak má nějakého dělitele a různého od 1 a n, a tedy $a < n$. Z indukčního předpokladu je a dělitelné nějakým prvočíslem p. Jelikož $p|a$ a $a|n$, máme $p|n$. □

Častá varianta: dokazujeme

- platí $A(1)$ a
- pro každé $n \geq 2$, jestliže platí $A(n-1)$, pak platí $A(n)$.

Lemma 4. *Pro každé přirozené číslo n platí*

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

Důkaz. Důkaz provedeme indukcí dle n. Pro $n = 1$ máme

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

tvrzení tedy platí. Uvažujme nyní libovolné $n \geq 2$. Z indukčního předpokladu máme

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

Pak

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

jak jsme měli dokázat. □

Pozor na „neúplnou indukci“.

Lemma 5 (Chybné!)**.** *Pro každá přirozená čísla $a, b \geq 1$ je $2a+b$ liché.*

Důkaz (Chybný!). Důkaz provedeme indukcí dle $n = a+b-1$. Budeme tedy dokazovat následující tvrzení.

> Pro každé přirozené číslo n a každá přirozená čísla $a, b \geq 1$ taková, že $n = a+b-1$, je $2a+b$ liché.

Když $n = 1$, pak $a = b = 1$ a $2a+b = 3$, tvrzení tedy platí. Uvažme nyní libovolné $n \geq 2$, a předpokládejme, že tvrzení platí pro $n-1$. Tedy pro každá přirozená čísla $a', b' \geq 1$ tž. $a'+b'-1 = n-1$ je $2a'+b'$ liché. Nechť $a = a'+1$ a $b = b'$. Pak platí

$$2a+b = 2(a'+1)+b' = (2a'+b')+2.$$

Jelikož $2a'+b'$ je liché, o 2 větší číslo $2a+b$ je také liché. Navíc $a+b-1 = a'+b' = n$, tvrzení tedy platí i pro n. □

3 Značení

Aritmetika:

- Běžné operace $+$, $-$, $\cdot$, $/$ na různých oborech, rovnost $=$, nerovnost $\neq$.
- Číselné obory:
  - $\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$
  - $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  - $\mathbb{Q}$ racionální čísla
  - $\mathbb{R}$ reálná čísla, $\mathbb{R}_0^+$ nezáporná reálná čísla
  - $\mathbb{C}$ komplexní čísla
- x^n a $\sqrt[n]{y}$ pro $n \in \mathbb{N}$, $x \in \mathbb{R}$, $y \in \mathbb{R}_0^+$, $\sqrt{y} = \sqrt[2]{y}$.
- e^x, $\exp(x)$ pro $x \in \mathbb{R}$, $\log(y) = \ln(y)$, $\log_b(y)$ pro $y > 1$.

- $\lfloor x \rfloor$, $\lceil x \rceil$

Součty a součiny:

- $a_m + a_{m+1} + \ldots + a_n = \sum_{i=m}^{n} a_i$.
- $a_m \cdot a_{m+1} \cdot \ldots \cdot a_n = \prod_{i=m}^{n} a_i$.
- $\sum_{i \in I} a_i$: součet přes všechny indexy v množině I.
- $\sum_{i=1}^{0} a_i = \sum_{i \in \emptyset} a_i = 0$.
- $\prod_{i=1}^{0} a_i = \prod_{i \in \emptyset} a_i = 1$.

Příklad 2.

$$\prod_{i=1}^{n} x = x^n$$

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\sum_{i=1}^{n} (2i+3) = 2\sum_{i=1}^{n} i + \sum_{i=1}^{n} 3 = n(n+1) + 3n$$

$$\sum_{1 \le i < j \le n} ij = \sum_{i=1}^{n} \sum_{j=i+1}^{n} ij = \sum_{i=1}^{n} i \sum_{j=i+1}^{n} j$$

Definujeme-li $\mathbb{D}_n$ jako množinu čísel dělitelných pouze prvočísly menšími nebo rovnými n, pak

$$\prod_{p \le n \text{ prvočíslo}} \frac{1}{1 - 1/p} = \sum_{k \in \mathbb{D}_n} \frac{1}{k}.$$

Logika:

- Operace $\wedge$, $\vee$, $\neg$, $\implies$, $\Leftrightarrow$.
- Kvantifikátory $\forall$, $\exists$.

Příklad 3.

$$(A \implies B) \Leftrightarrow (\neg A \vee B)$$

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$$

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

$$(A \implies B) \Leftrightarrow (\neg B \implies \neg A)$$

$$(\forall n \in \mathbb{N}_0)(\exists a, b, c, d \in \mathbb{N}_0)\, n = a^2 + b^2 + c^2 + d^2$$

Množiny:

- $\emptyset$
- Běžné operace $\cap$, $\cup$, $\setminus$, $\in$, $\notin$, $\subset$, $\subseteq$, $\subsetneq$, $\not\subseteq$, $|x|$.
- Doplněk: je-li A podmnožina nějaké (z kontextu známé) množiny B, pak $\overline{A} = B \setminus A$.
- $\{x \in X : x$ splňuje vlastnost $\ldots\}$, $\{f(x) : x \in X, x$ splňuje vlastnost $\ldots\}$
- Množina všech podmnožin množiny X: 2^X, $\mathcal{P}(X)$
- Množina všech k-prvkových podmnožin: $\binom{X}{k} = \{y \in 2^X : |y| = k\}$
- Dvojice x, y neuspořádaná $\{x, y\}$, uspořádaná (x, y)
- Uspořádaná k-tice $(a_1, a_2, \ldots, a_k)$
- Kartézský součin $X \times Y = \{(x, y) : x \in X, y \in Y\}$