Pomocný text

DŮKAZY

Milí řešitelé,

v tomto povídání si rozebereme základní důkazové metody: důkaz přímý, důkaz nepřímý, důkaz sporem a matematickou indukci. Jsou nezbytnou součástí matematikovy výbavy a je nutné, abyste v nich měli přehled. Kdo neví, ten se dozví. Ti z vás, kteří je už znají, získají jistotu v jejich používání. Pusťme se do toho!

Přímý důkaz

Tento typ důkazu je nám asi nejpřirozenější. Jak už název napovídá, postupujeme přímo. Tvrzení dokážeme pomocí na sebe navazujících logických postupů, definic, vět a dalších nástrojů.

Často potřebujeme dokázat nějakou implikaci, neboli výrok tvaru „Pokud platí A, pak platí B"(značíme $A \Rightarrow B$). Na začátku předpokládáme pravdivost výroku A, řetězcem implikací pak dojdeme k výroku B ($A \Rightarrow A_2 \Rightarrow \cdots \Rightarrow B$). Ukažme si na příkladu.

Pro celá čísla n dokažte, že pokud je n liché, pak je i n^2 liché.

Začínáme tedy z úvodního předpokladu, že n je liché. To je náš startovní výrok A. Pokračujeme dále: n se určitě dá vyjádřit ve tvaru $n = 2k + 1$, $k \in \mathbb{Z}$. Dosadíme do n^2:

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

A n^2 je tedy také liché. To je náš konečný výrok B.

Někteří z vás by spíše dokazovali výrok "pokud je n^2 sudé, pak je n sudé". Vskutku je tato implikace ekvivalentní s původní implikací. Ukažme si, proč tomu tak je.

2.1 Nepřímý důkaz

Nepřímý důkaz je založen na faktu, že následující výroky jsou ekvivalentní ($\neg A$ je negace výroku A):

$A \Rightarrow B$ - *„Pokud platí A, pak platí B."*

$\neg B \Rightarrow \neg A$ - *„Pokud neplatí B, pak neplatí A."*

Ne každému je asi úplně jasné, že tyto výroky jsou opravdu rovnocenné. Představme si následující situaci s Ňoumou a Koumou.

Ňouma se stal přes noc celebritou a z celého světa mu fanoušci a odpůrci posílají dopisy. Ty příznivé si Ňouma nechává, zatímco ty ošklivé háže do koše. I z Hloupětína mu přišli dopisy a Kouma má hypotézu, že všechny dopisy od hloupětínských jsou příznivé. Může na to jít přímo, projít všechny dopisy s adresou z Hloupětína. Dokazoval by tedy implikaci „Pokud přišel dopis z Hloupětína, pak je příznivý". Nebo na to může jít nepřímo. Stačí mu projít Ňoumův koš a kouknout se, jestli jsou opravdu všechny odjinud než z Hloupětína. Dokazoval by tedy implikaci „Pokud je dopis nepříznivý, pak není z Hloupětína". Opět si ukažme na příkladu:

Mějme prvočíslo p. Dokažte, že pokud je p^3+4 číslo složené, pak je i číslo p^2+8 složené.

Co s tím. Tady se úplně nabízí nepřímý důkaz. Pojďme radši dokazovat implikaci „Pokud je p^2+8 prvočíslo, pak je i p^3+4 prvočíslo". To vypadá hned lépe. Platí totiž $3 \mid p(p-1)(p+1)$. Pro p různé od tří navíc $3 \mid (p-1)(p+1) = p^2-1$. Nutně i $3 \mid p^2+8$. No ale pokud je p^2+8 prvočíslo, pak $p^2+8=3$, což zjevně nejde. Zbývá proto $p=3$, potom $p^3+4=27+4=31$ je opravdu prvočíslo. Jsme hotovi.

Nepřímý důkaz je tedy opravdu silná zbraň, na kterou není radno zapomínat. Někteří z vás by se opět vydali jinou cestou, použili důkaz sporem. Ale co to je?

2.2 Důkaz sporem

Občas se nám nějaké tvrzení nedaří dokázat. Skoro to vypadá, že to tvrzení neplatí. I touto cestou se lze vydat! Předpokládáme-li, že dokazované tvrzení neplatí a dojdeme postupně ke zřejmě nepravdivému tvrzení - sporu, pak používáme důkaz sporem.

Řekněme, že chceme dokázat implikaci $A \Rightarrow B$ sporem. Měli bychom tedy předpokládat, že neplatí. Co je opak implikace? Obecně platí, že negace implikace *„Pokud platí A, pak platí B."* je výrok *„Platí A a neplatí B."* (formálně značíme $A \wedge \neg B$). V důkazu bychom proto předpokládali, že platí zároveň A a $\neg B$. Tím se ocitneme v novém světě lží a nepravd, nám stačí jen nějakou tu nepravdu najít a prohlásit „Spor!". Ujasníme si to na příkladu.

Pokud a je racionální číslo a b iracionální, pak je i $a+b$ iracionální číslo.

Dokazujme tedy sporem. Uvažujme negaci zadané implikace, tj. a je racionální, b je iracionální a $a+b$ je racionální. Jestliže jsou a a $a+b$ racionální, pak jdou vyjádřit ve formě zlomku. Existují proto celá p, x a přirozená q, y, že

$$a = \frac{p}{q} \quad a+b = \frac{x}{y}.$$

Víme, že b si vyjádřit jako zlomek nemůžeme, protože je iracionální. Ale co to?

$$b = \frac{x}{y} - \frac{p}{q} = \frac{xq-yp}{qy}$$

To je nějaký nesmysl, b nemůže být zároveň iracionální a racionální. To je spor.

2.3 Matematická indukce

Tato metoda se používá zpravidla v případech, kdy potřebujeme dokázat, že nějaké tvrzení $T(n)$ platí pro nekonečně mnoho hodnot n. Bylo by celkem nešikovné dosazovat nekonečně mnoho čísel, proto používáme matematickou indukci. Myšlenka je, že pokud dokážeme udělat první krok a pokud dokážeme po libovolném kroku udělat jeden navíc, pak dokážeme udělat libovolný počet kroků.

Recept na matematickou indukci je:

1. Dokaž, že výrok $T(n)$ platí pro nějaké nejmenší n_1 (často $n_1 = 1$).
2. Dokaž implikaci $T(n) \Rightarrow T(n+1)$.

Proč to funguje? Tvrzení platí pro n_1, pak ale díky druhému bodu platí i pro $n_1 + 1$, poté i pro $n_1 + 2$ atd. Jako domino se to rozjede a důkaz nám platí pro nekonečně mnoho n. Nutno podotknout, že můžeme indukci používat jen pro hodnoty n přirozené (případně celé a zdola omezené). Rozhodně to nefunguje obecně pro reálná n.
Zkusme si matematickou indukci na příkladu:

Mějme $n \in \mathbb{N}$ přímek v rovině. Dokaž, že tyto přímky dělí rovinu na nejvýše $\frac{1}{2}n(n+1)+1$ oblastí.

Postupujme podle návodu. Dokažme tvrzení pro nejmenší $n = 1$. Jedna přímka dělí rovinu na dvě poloroviny a opravdu $\frac{1}{2} \cdot 1 \cdot (1 + 1) + 1 = 2$.
V druhém kroku dokazujeme implikaci „Pokud n přímek dělí rovinu na nejvýše $\frac{1}{2}n(n+1)+1$ oblastí, pak $n + 1$ přímek dělí rovinu na nejvýše $\frac{1}{2}(n + 1)(n + 2) + 1$ oblastí."
To už není tak těžké dokázat. Je jasné, že každá konfigurace $n+1$ přímek v rovině vznikne z nějaké konfigurace n přímek přidáním jedné další. Mějme n přímek, maximálně $\frac{1}{2}n(n+1)+1$ oblastí a přidejme další přímku. Tuto novou přímku rozdělí původních n přímek nejvýše na $n + 1$ částí. Každá tato část bude rozdělovat nějakou oblast na dvě. Přibyde nám tedy maximálně $n + 1$ oblastí:

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

Jsme hotovi.

Ještě si řekneme pár slov o úplné matematické indukci. Je na ní velmi podobný recept:
1. Dokaž, že výrok $T(n)$ platí pro nějaké nejmenší n_1 (často $n_1 = 1$).
2. Dokaž implikaci „Pokud platí $T(k)$ pro všechna $k \in \{n_1, n_1+1, ..., n\}$, pak platí $T(n+1)$.
Druhý bod nám říká: Předpokládej, že všechna tvrzení $T(n_1), T(n_1+1), T(n_1+2), ..., T(n)$ platí a dokaž, že i $T(n+1)$ platí. Je to taková silnější indukce (v angličtině „strong mathematical induction"). V klasické indukci totiž předpokládáme platnost jen tvrzení $T(n)$. Jako cvičení si pomocí úplné matematické indukce dokažte, že každé přirozené číslo větší než jedna lze jednoznačně (až na pořadí) rozložit na součin prvočísel (Základní věta aritmetiky).

Hodně štěstí při řešení úloh!