D ů k a z y

Pavel Miškovský
(říjen 2001, úpravy duben 2004, srpen 2005)

Obsah

Úvod

V matematice je zavedeno mnoho odborných termínů. Máme-li je úspěšně užívat při řešení praktických i teoretických úloh, musíme znát jejich přesný význam. Jeden pojem musí být vysvětlen pojmy, které jsou přesně určeny, a ty spočívají opět na dalších přesně vymezených pojmech. Toho však docílíme jen tehdy, jestliže základ celé soustavy pojmů spočívá na určité zvolené skupině slov, která jsou **nedefinovaná** (to znamená, že nejsou blíže vysvětlena a jejich obsah je chápán „intuitivně“). Tím se podstatně liší tento tzv. **deduktivní systém** od vysvětlování významu slov v běžném životě. Jen tímto způsobem se vyhneme vysvětlování slov kruhem. Stačí zvolit několik málo slov jako nedefinovaná, abychom se vyhnuli definicím v kruhu. Jsou to např. slova bod, přímka, množina apod. Volba těchto slov závisí na určité deduktivní soustavě, která má být vybudována. Pomocí nedefinovaných slov definujeme odborné termíny a pomocí nich utváříme termíny další. Kromě nedefinovaných slov předpokládáme, že máme k dispozici neodborná slova českého jazyka.

Za předpokladu, že je zvoleno několik slov jako slova nedefinovaná a že máme k dispozici neodborný český jazyk, můžeme se vyjadřovat o určitých matematických pojmech. Např. v planimetrii by se často vyskytovala tato posloupnost slov: ”množina skládající se ze dvou bodů A, B a ze všech bodů, které jsou mezi těmito body”. Vyjadřování by bylo neobratné, zdlouhavé a málo přehledné, zvláště když by další pojmy byly označeny obdobnými složenými výrazy. Vzhledem k důležitosti tohoto pojmu a k jeho častému výskytu, vede nás praxe k tomu, že je vhodné místo složitého slovního výrazu zavést jedno slovo - **odborný termín** ”úsečka”. Slovo ”úsečka” je pouhé zkrácené vyjádření rčení, které bylo uvedeno jako první. V textu lze oba výrazy zaměňovat, protože mají stejný význam (jsou ekvivalentní).

Pomocí nedefinovaných slov a pomocí definovaného termínu ”úsečka” můžeme zavést další odborné názvy. Význam každého z nových termínů je určen **definicí** pomocí termínů předcházejících. Definice je sdělení (resp. výrok, který považujeme za pravdivý), v němž se vyslovují charakteristické vlastnosti daného pojmu, které jej odlišují od ostatních. Aby se odlišila definice od **matematické věty**, která se musí dokazovat, vkládá se obvykle do definice slovo ”nazýváme”, a tím se zdůrazňuje, že definice značí v podstatě jen pojmenování matematického objektu. Definice je v podstatě rovnost dvou ekvivalentních výrazů, pro něž tedy platí oboustranná implikace. Např.: A. Jestliže se součin dvou čísel rovná jedné, pak tato čísla jsou reciproká. B. Jestliže jsou dvě čísla reciproká, pak se jejich součin rovná jedné.

Definice hrají v matematice významnou úlohu. Zjednodušují vyjadřování (místo komplikovaného větného výrazu se zavede zpravidla jedno slovo nebo symbol s týmž významem) a zavedení nového termínu má direktivní význam. Upozorňuje se, že pojem je tak důležitý, že stojí za to zavést pro něj samostatný termín.

Všechny definice lze v podstatě rozdělit do dvou skupin. Definice analytické zavádějí pro určité spojení známých pojmů pojem nový (Množina všech bodů M v rovině, které mají od daného bodu S této roviny vzdálenost $r > 0$, se nazývá kružnice se středem S a poloměrem r.). Název nového pojmu zavádí definice nominální-názvová. Konstruktivní definice nový pojem ”konstruuje” a rekurentní definici známe např. z definic posloupností.

Definice analytická vychází z definovaného pojmu a objasňuje jej pomocí pojmů známých (Kružnice o středu S a poloměru $r > 0$ je množina všech bodů M v rovině, které mají od daného bodu S této roviny vzdálenost r.). Do této kategorie patří rekurentní definice, definice abstrakcí, souvislostní definice. Příkladem analytické definice je definice čtverce - čtverec je pravoúhlý rovnostranný rovnoběžník.

Příklady definic: - Sudé číslo je číslo dělitelné dvěma.

- Kružnice je množina bodů, které mají od daného bodu konstantní vzdálenost.

Při definování pojmů je možné se dopustit mnoha chyb - definice nadbytečná, definice široká (obsahuje i objekty nežádoucí: pravidelný šestiúhelník je rovinný obrazec ohraničený

šesti shodnými úsečkami), definice úzká (mnohé objekty neobsahuje: Iracionální čísla jsou druhé odmocniny čísel, která nejsou druhými mocninami racionálních čísel. - chybí e, π), definice kruhem (dvě přímky jsou kolmé tehdy, když svírají pravý úhel) nebo definice neznámého neznámým (lat. ignotum per ignonum, elipsa je eliptická křivka).

Když jsme vytvořili dostatečnou zásobu odborných názvů - termínů, ať definovaných nebo nedefinovaných, jsme schopni vytvářet další výroky, ve kterých použijeme tyto odborné názvy a slovní zásobu běžného českého jazyka. O vytvořených výrocích pak můžeme uvažovat, zda jsou nebo nejsou pravdivé. V matematice pravdivost výroku nespočívá v souhlase se skutečností, ale v logické závislosti na výrocích jiných. (Význam tohoto sdělení pochopíme ve chvíli, kdy budeme studovat např. tzv. neeuklidovské geometrie.) Výroky jisté matematické teorie jsou navzájem vázány jeden na druhý a tvoří uzavřenou logickou soustavu. Určitý pravdivý výrok se stává předpokladem a implikací dostaneme tvrzení, toto tvrzení se stane předpokladem pro další implikaci atd. Získáme tak posloupnost implikací, kde pravdivost výroku přechází z jednoho na druhý. Jako v případě definic, tak i zde je nutno začít někde od pevného základu. Musíme zvolit několik málo základních výroků, o kterých prohlásíme, že jsou ”pravdivé” a z pravdivosti těchto výroků odvodíme pravdivost všech výroků dalších.

Základní výrok, o kterém prohlásíme, že je pravdivý, se nazývá axiom.

Axiom je jednoduché základní tvrzení, které je považováno bez důkazu za pravdivé. Na střední škole se s axiomy nebo s tvrzeními za axiomy označené nesetkáme. Pro úplnost však dodejme, že bez tzv. Peanových axiomů by neexistovala teorie přirozených čísel a bez jiných axiomů bychom nemohli používat běžné konstrukční postupy v rámci tzv. euklidovské geometrie. Tyto zmíněné axiomy tvoří tzv. axiomatický systém, který je základem pro tvorbu definic v dané oblasti matematiky (axiomy v axiomatickém systému musí být nezávislé, úplné a bezesporné).

Výrok s matematickým obsahem, jehož pravdivost je dokázána pomocí axiomů nebo pomocí dříve dokázaných výroků, se nazývá matematická věta.

Matematická věta je výrok, kterým charakterizujeme, vymezujeme nový poznatek o vlastnosti matematického pojmu. Pravdivost tohoto výroku se dokazuje pomocí axiomů, definic nebo již dříve dokázaných vět. Matematická věta může být vyslovena v podobě jednoduchého-atomárního výroku (Číslo 7 je prvočíslo.) nebo v podobě výroku složeného (nejčastěji implikace, je-li ve tvaru ekvivalence, je nutné dokazovat obě implikace).

Podmínka nutná a postačující ve větě - obojí se často nazývá kriterium.

Důkaz je prověřením pravdivosti (platnosti) matematické věty. Dokazování je založeno na usuzování. Každý důkaz se skládá z řady úsudků nebo je (v nejjednodušších případech) úsudkem jedním.

Vybraná skupina nedefinovaných slov a další slova, která jsou pomocí nich definována, skupina axiomů, o nichž se předpokládá, že jsou pravdivé, a skupina výroků - matematických vět, jejichž pravdivost se dokáže na základě axiomů a logických pravidel, se nazývá **deduktivní systém určité matematické teorie**.

Důkaz v matematice je logické odvození pravdivého výroku z jiných pravdivých výroků. Výroky, z nichž při důkazu vycházíme, se nazývají **předpoklady - premisy**, a výrok, ke kterému se nakonec dostaneme, se nazývá **závěr - tvrzení důkazu**. Za předpoklad důkazu může být použit kterýkoli axiom nebo matematická věta již dříve dokázaná. Důkaz se skládá z posloupnosti výroků, kde následující logicky plyne z výroku předcházejícího a kde odvozování je zaměřeno k dokázání pravdivosti výroku, který má být závěrem celého důkazu.

Jednotlivý krok, ve kterém se jeden výrok odvozuje z druhého, se nazývá úsudek.

Při dokazování věty je nutné rozlišovat, co je předpokladem, tedy z čeho vycházíme, a co je závěrem. Pravdivost závěru závisí na pravdivosti předpokladů a také na tom, zda jsme správně usuzovali. **Správný úsudek je takový úsudek, v němž není možné dostat z pravdivých výroků nepravdivý závěr.** (Pravdivostní tabulka implikace: ”Lží nelze dosíci pravdy.”)

Pojem důkazu je v matematice jeden ze základních pojmů. Deduktivním úsudkem odvozujeme z jedné platné věty věty další, a tak vytváříme a upevňujeme vzájemně vztahy mezi různými pojmy, definicemi a větami.

Neexistuje žádná snadná jediná metoda, jak se naučit provádět důkazy. Existují různé metody důkazů a pro každou úlohu je vhodný jiný.

Typy důkazů: - výčtem všech možných případů
- přímý
- nepřímý
- sporem
- kombinovaný
- matematickou indukcí
- jiné (např. geometrický, odvozením)

Nelze jednoznačně stanovit, kdy který důkaz použít. Žádný obecný ”poznávací” znak neexistuje. Při volbě ”správného” typu důkazu je nutné se řídit zkušeností, citem, intuicí. To vše lze získat jedinou cestou - provedením mnoha různých důkazů, absolvováním mnoha slepých cest a nalezením alespoň dílčích znaků ukazujících, který typ důkazu bude pravděpodobně tím ”pravým”.

V popisech jednotlivých typů důkazů se vychází z toho, že většina matematických vět je vyslovena ve tvaru implikace.

Poznámka 1: Vzhledem k omezenosti nabídky znaků je v dalším textu užito pro operaci ”nedělí” znaku ”#”.

Poznámka 2.: Každý důkaz ukončíme konstatováním ”cbd.” (což bylo dokázat, lat. quod erat demonstrandum - qed.)

A. Důkaz výčtem všech možných případů

Tohoto typu důkazu můžeme užít jen tehdy, je-li možných případů konečný počet, a to rozumně malý. Při větším počtu možných případů se důkaz stane příliš pracný. Při usuzování musíme být zvláště opatrní na to, abychom vyčerpali všechny možné případy.

Příklad A.1: Věta: Druhá mocnina kteréhokoli lichého čísla je liché číslo.

důkaz: kterékoli liché číslo může končit pouze jednou z číslic 1, 3, 5, 7, 9
je tedy třeba vyšetřit těchto pět případů
a) končí-li číslo číslicí 1, pak jeho druhá mocnina končí také číslicí 1
důkaz: toto číslo se dá napsat ve tvaru: $a.10 + 1$
pak $(a.10 + 1)^2 = a^2.100 + 2a.10 + 1^2$
b-e) důkaz probíhá analogicky
druhá mocnina lib. lichého čísla může končit jen jednou z číslic 1, 5, 9
cbd.

Příklad A.2: Věta: $(\forall n \in N)\ 3 \mid (n^3 + 2n)$

důkaz: vztah čísla n k dělitelnosti číslem 3 lze vyjádřit těmito vztahy:
a) $n = 3k$
b) $n = 3k + 1$
c) $n = 3k + 2$
pro všechny případy je nutné dokázat dělitelnost výrazu $n^3 + 2n$ třemi
a) $n = 3k \Rightarrow n^3 + 2n = (3k)^3 + 2(3k) = 27k^3 + 6k = 3(9k^3 + 2k) \Rightarrow 3 \mid (n^3 + 2n)$
b) $n = 3k + 1 \Rightarrow n^3 + 2n = (3k+1)^3 + 2(3k+1) =$
$= 27k^3 + 27k^2 + 9k + 1 + 6k + 2 = 3(9k^3 + 9k^2 + 5k + 1) \Rightarrow 3 \mid (n^3 + 2n)$
c) $n = 3k + 2 \Rightarrow n^3 + 2n = (3k+2)^3 + 2(3k+2) = 27k^3 + 54k^2 + 36k + 8 + 6k + 4 =$
$= 3(9k^3 + 18k^2 + 14k + 4) \Rightarrow 3 \mid (n^3 + 2n)$
cbd.

Poznámka k příkladu A.2: Větu lze dokazovat i matematickou indukcí.

Úlohy:
A.1. Dokaž větu: $(\forall n \in N)\ 3 \mid (n^2 + 3n) \Rightarrow 3 \mid n$

B. Přímý důkaz

Tento typ důkazu využívá toho, že z pravdivého předpokladu na základě pravdivých odvození nutně plyne (na základě pravdivostní tabulky implikace) pravdivé tvrzení. Samozřejmé je, že tato "cesta" existuje a je řešitelem nalezitelná - a nalezená.

Důkaz vychází z předpokladu, na jehož základě jsou odvozována dílčí tvrzení tak dlouho, až se dospěje k dokazovanému tvrzení. Všechny kroky jsou "správné", tedy pravdivé, a tedy i odvozovaná tvrzení jsou správná-pravdivá.

Schema důkazu: $P \Rightarrow T_1 \Rightarrow T_2 \Rightarrow T_3 \Rightarrow ... \Rightarrow T$

Příklad B.1: Věta: $(\forall n \in N)\ 3 \mid n \Rightarrow 3 \mid n^2$

důkaz: $3 \mid n \Rightarrow n = 3x \Rightarrow n^2 = (3x)^2 \Rightarrow n^2 = 9x^2 \Rightarrow n^2 = 3 . (3x^2) \Rightarrow 3 \mid n^2$
cbd.

Příklad B.2: Věta: $(\forall n \in N)\ 6 \mid (n^3 - n)$

důkaz: $n^3 - n = n(n-1)(n+1) = (n-1)n(n+1)$ ... což je součin tří po sobě jdoucích přirozených čísel $\Rightarrow$ je nutně dělitelný dvěma a třemi zároveň $\Rightarrow$ $\Rightarrow$ číslo ve tvaru $n^3 - n$ je dělitelné šesti
cbd.

Poznámka k příkladu B.2: Tuto větu lze dokázat i matematickou indukcí.

Příklad B.3: Věta: $(\forall r \in R-\{0\})\ r^2 + 1/r^2 \geq 2$

důkaz: $r^2 + 1/r^2 \geq 2 \Rightarrow r^2 - 2 + 1/r^2 \geq 0 \Rightarrow (r - 1/r)^2 \geq 0 \Rightarrow$ druhá mocnina jakéhokoli čísla je nezáporná $\Rightarrow$ věta platí
cbd.

Příklad B.4: Věta (součtový vzorec pro kombinační čísla):

Pro všechna $n,k \in N$ taková, že $1 \leq k \leq n$ platí: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

důkaz: $\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{[(n-1)-(k-1)!(k-1)]} + \frac{(n-1)!}{(n-1-k)!k!} =$

$= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!} = \frac{(n-1)!}{(n-k)(n-k-1)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!(k-1)!} =$

$= \frac{k(n-1)!+(n-k)(n-1)!}{(n-k)(n-k-1)!k(k-1)!} = \frac{(k+n-k)(n-1)!}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$

cbd.

Úlohy:

B.1. Dokaž větu: $(\forall a,b \in N)\ 3 \mid a \vee 3 \mid b \Rightarrow 3 \mid ab$
B.2. Dokaž větu: $(\forall a,b \in N)(\forall k \in N)\ k \mid a \wedge k \mid b \Rightarrow k \mid (a+b)$
B.3. Dokaž větu: Součinem dvou libovolných lichých čísel je liché číslo.
B.4. Dokaž větu: Součtem dvou libovolných lichých čísel je sudé číslo.
B.5. Dokaž větu: $(\forall a,b \in N)\ a \mid b \Rightarrow a \mid b^2$
B.6. Dokaž větu: $(\forall a,b,c \in N)\ (a \mid b \wedge b \mid c) \Rightarrow a \mid c$
B.7. Dokaž větu: Druhá mocnina lichého čísla je liché číslo.

B.8. Dokaž větu: Nechť $0 \leq k \leq n$, kde $k, n \in N_0$. Pak platí: $\binom{n}{k} = \binom{n}{n-k}$

C. Nepřímý důkaz

Tento typ důkazu se používá tehdy, když užití přímého důkazu je příliš komplikované nebo nelze přímý důkaz provést.

Využívá se toho, že obměněná věta k větě v podobě implikace má stejnou pravdivostní hodnotu. Z toho plyne, že když se dokáže pravdivost obměněné věty, platí i věta původní.

Obměněná věta se dokazuje přímo.

Schema důkazu: $P \Rightarrow T$ ..... obměněná věta: $\neg T \Rightarrow \neg P$

Příklad C.1: Věta: $(\forall n \in N)\ 3 \mid n^2 \Rightarrow 3 \mid n$

přímý důkaz nelze v tomto případě použít

obměněná věta: $3 \# n \Rightarrow 3 \# n^2$

důkaz: $3 \# n \Rightarrow$ a) $n = 3k + 1$

$\Rightarrow n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 \Rightarrow 3 \# n^2$

b) $n = 3k + 2$

$\Rightarrow n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1 \Rightarrow 3 \# n^2$

z obou částí plyne $\Rightarrow 3 \# n^2$

cbd.

Úlohy:

C.1. Dokaž větu: $(\forall n \in N)\ 3 \mid (n^2 + 3n) \Rightarrow 3 \mid n$

C.2. Dokaž větu: $(\forall a,b \in N)\ 3 \mid ab \Rightarrow 3 \mid a \vee 3 \mid b$

D. Důkaz sporem (lat. reductio ad absurdum, dovedení k nesmyslu)

Tento typ důkazu se používá v případech, kdy nelze použít předchozí dva typy. Vychází z principu, že má-li platit vyslovená věta, nutně neplatí věta ve tvaru negace. V důkazu se tedy zaměřujeme na důkaz neplatnosti negované věty. Pokud se důkaz zdaří, plyne z toho, že původní věta platí. (Princip důkazu se dá také popsat jako ekvivalence těchto výroků: $\neg(P \Rightarrow T)$ a $P \wedge \neg T$.)

Schema důkazu: $P \Rightarrow T$ ..... negace ..... $P \wedge \neg T$

Příklad 7: Věta: $(\forall n \in N)\ 2\#n^3 \Rightarrow 4\#n$
negace věty: $2\#n^3 \wedge 4 \mid n$
důkaz (nepravdivosti negované věty): $2\#n^3 \Rightarrow n^3 \neq 2k$ a zároveň $4 \mid n \Rightarrow n = 4k$
$\Rightarrow n^3 = 64k^3 \Rightarrow n^3 = 2 \cdot 32k^3 \Rightarrow 2 \mid n^3$
- spor - n^3 nemůže být číslo současně liché i sudé
platí původní tvrzení
cbd.

Příklad 8: Věta: $\sqrt{2}$ je iracionální číslo.
(tento důkaz je více než 2000 let starý)
negace věty: $\sqrt{2}$ je racionální číslo
důkaz (nepravdivosti negované věty): $\sqrt{2} \in Q \Rightarrow \sqrt{2} = p/q$ (p, q jsou nesoudělná) $\Rightarrow 2 = q^2/p^2 \Rightarrow 2p^2 = q^2 \Rightarrow 2 \mid p^2 \Rightarrow \underline{\mathbf{2 \mid p}} \Rightarrow p = 2k$
z toho, že $2p^2 = q^2$ a $p = 2k$ plyne, že $(2k)^2 = 2q^2 \Rightarrow 4k^2 = 2q^2 \Rightarrow q^2 = 2k^2 \Rightarrow \underline{\mathbf{2 \mid q}}$ ... což je spor, protože p, q jsou nesoudělná a současně jsou obě dělitelná dvěma $\Rightarrow$ negovaná věta neplatí $\Rightarrow$ platí věta původní
cbd.

E. Důkaz kombinovaný

Nejedná se o principiálně jiný typ důkazu. Některé matematické věty jsou vysloveny ve tvaru ekvivalence a je tedy nutné dokázat pravdivost konjunkce obou implikací, ze kterých je tato ekvivalence složena. Zmíněné implikace se většinou dokazují jiným postupem.

Příklad E.1: Věta: $(\forall\, n \in N)\ 3 \mid n \Leftrightarrow 3 \mid n^2$

důkaz: a) přímo $3 \mid n \Rightarrow 3 \mid n^2$
b) nepřímo $3 \mid n^2 \Rightarrow 3 \mid n$
(oba tyto důkazy již byly provedeny v předchozích oddílech)
cbd.

Poznámka k příkladu E.1: Část b) je možné dokazovat i sporem.

Příklad E.2: Věta: V oboru reálných čísel má rovnice $ax = b$ $(a \neq 0)$ jedno řešení.

důkaz: a) důkaz existence přímo: $ax = b \Rightarrow x = a^{-1}.b$
b) důkaz jednoznačnosti sporem: existují dvě různá řešení $x_1 \neq x_2$
$\Rightarrow ax_1 = b \wedge ax_2 = b \Rightarrow$
$\Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$
spor, ze kterého plyne, že řešení existuje jen jedno
cbd.

F. Matematická indukce

Vznik matematické indukce sahá do daleké minulosti. V jisté podobě se s ní lze setkat již u starověkých filosofů. Užíval ji Maurolies ze Sicílie (1494-1575), od něho ji přejal francouzský matematik a filozof Blaise Pascal (1623-1662) a podrobně se jí zabýval. Nezávisle na něm se zabýval matematickou indukcí švýcarský matematik Jacob Bernoulli (1654-1705). Hlavně jeho zásluhou se stala tato metoda důkazu známou.

Věty ve tvaru $(\forall n \in N)\ P(n)$ jsou v podstatě kvantifikovanými výrokovými formami, jejichž platnost má být dokázána pro všechna přirozená čísla. Žádnou z těchto vět nelze dokázat tak, že bychom ji postupně ověřovali na konečném množství případů, protože přirozených čísel je nekonečně mnoho. Je proto nutné použít jinou metodu důkazu - matematickou indukci.

Princip matematické indukce vychází z PA7, který říká, že pro libovolnou formuli φ popisující nějakou vlastnost přirozených čísel platí:

$$[\varphi(n_0) \wedge (\forall n \in N)(\varphi(n) \Rightarrow \varphi(n+1))] \Rightarrow (\forall n \in N)\varphi(n)$$

Z tohoto principu vyplývají tři kroky důkazu:

a) dokážeme, že věta platí pro $n = 1$, resp. $n = n_0 \geq 1$

b) předpokládáme pravdivost věty pro libovolné přirozené $k \geq 1$, resp. $k \geq n_0$

c) dokážeme na základě předpokladu pravdivost věty pro $k + 1$

a z toho plyne, že věta platí pro všechna přirozená čísla, resp. pro přirozená $n \geq n_0$

Příklad F.1: Věta: $(\forall n \in N)\ 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$

důkaz: a) pro $n = 1$ $L = 1$
$P = 1$
$L = P$

b) pro $k > 1$ $1 + 2 + 3 + ... + k = 0{,}5k(k+1)$
předpokládáme platnost

c) pro $k + 1$ $1 + 2 + 3 + ... + k + (k + 1) = 0{,}5(k + 1)(k + 2)$
na základě předpokladu dokážeme platnost tohoto tvrzení
$L = (1 + 2 + 3 + ... + k) + (k + 1) = 0{,}5k(k+1) + (k + 1) =$
$= 0{,}5(k + 1)(k + 2)$
$P = 0{,}5(k + 1)(k + 2)$
$L = P$

cbd.

Příklad F.2: Věta: $(\forall n \in N)\ 1 + 3 + 5 + ... + (2n-1) = n^2$

důkaz: a) pro $n = 1$ $L = 1$
$P = 1$
$L = P$

b) pro $k > 1$ $1 + 3 + 5 + ... + (2k-1) = k^2$
předpokládáme platnost

c) pro $k + 1$ $1 + 3 + 5 + ... + (2k-1) + (2k + 1) = (k + 1)^2$
na základě předpokladu dokážeme platnost tohoto tvrzení
$L = (1 + 3 + 5 + ... + (2k-1)) + (2k + 1) = k^2 + (2k + 1) =$
$= k^2 + 2k + 1$
$P = k^2 + 2k + 1$
$L = P$

cbd.

Matematickou indukcí lze dokazovat i složitější úlohy, které se týkají dělitelnosti a které se ”klasicky” dokazují přímo, nepřímo nebo sporem.

Příklad F.3: Věta: $(\forall n \in N)\ 4 \mid (n^4 + 3n^2)$

důkaz: a) pro n = 1 $n^4 + 3n^2 = 1 + 3 = 4$
$4 \mid 4$
b) pro k > 1 $4 \mid (k^4 + 3k^2)$
předpokládáme platnost
c) pro k + 1 $4 \mid ((k+1)^4 + 3(k+1)^2)$
na základě předpokladu dokážeme platnost tohoto tvrzení
$(k+1)^4 + 3(k+1)^2 = k^4 + 4k^3 + 6k^2 + 4k + 1 + 3k^2 + 6k + 3 =$
$= k^4 + 4k^3 + 9k^2 + 10k + 4 = (k^4 + 3k^2) + \underline{(4k^3 + 6k^2 + 10k + 4)}$
součet dvou sčítanců je dělitelný 4 právě tehdy, když je 4 dělitelný každý ze sčítanců, ”stačí” tedy dokázat, že je 4 dělitelný čtyřčlen $(4k^3 + 6k^2 + 10k + 4)$, protože dvojčlen $(k^4 + 3k^2)$ je 4 dělitelný na základě předpokladu
$4k^3 + 6k^2 + 10k + 4 = (4k^3 + 4) + \underline{(6k^2 + 10k)}$
na základě stejného principu stačí dokázat, že je 4 dělitelný dvojčlen $(6k^2 + 10k)$
důkaz provedeme indukcí:
a) pro n = 1 $6k^2 + 10k = 6 + 10 = 16$
$4 \mid 16$
b) pro k > 1 $4 \mid (6k^2 + 10k)$
předpokládáme platnost
c) pro k + 1 $4 \mid (6(k+1)^2 + 10(k+1))$
na základě předpokladu dokážeme platnost tohoto tvrzení
$(6(k+1)^2 + 10(k+1)) = 6k^2 + 12\,k + 6 + 10k + 10 =$
$= 6k^2 + 22k + 16 = (6k^2 + 10k) + \underline{(12k + 16)}$
součet dvou sčítanců je dělitelný 4 právě tehdy, když je 4 dělitelný každý ze sčítanců, ”stačí” tedy dokázat, že je 4 dělitelný dvojčlen (12k + 16), protože dvojčlen $6k^2 + 10k$ je 4 dělitelný na základě předpokladu
$12k + 16 = 4(3k + 4)$
$\Rightarrow$ všechny mnohočleny jsou po řadě dělitelné 4, dílčí důkazy jsou provedeny, a tím je věta dokázána

cbd.

Poznámka k příkladu F.3: Tuto větu lze dokazovat i přímo - vztah čísla n k dělitelnosti číslem 4

lze vyjádřit čtyřmi vztahy: a) n = 4k
b) n = 4k + 1
c) n = 4k + 2
d) n = 4k + 3

Pro každý případ zvlášť se dokáže, že číslo n je v daném tvaru dělitelné čtyřmi.

Příklad F.4: Věta: $(\forall n \in N\text{-}\{1\})\ 7 \mid (n^6 - 1)$

důkaz: zde zatím není

Příklad F.5: Věta: $(\forall n \in N)\ 9 \mid (10^n - 1)$

důkaz: a) pro $n_0 = 2$ $10^n - 1 = 99 \Rightarrow 9 \mid 99$
b) pro $k > 2$ $9 \mid (10^k - 1) \Rightarrow 10^k - 1 = 9a \Rightarrow 10^k = 9a + 1$
předpokládáme platnost
c) pro $k + 1$ $9 \mid (10^{k+1} - 1) \Rightarrow 10^{k+1} - 1 = 10 \,.\, 10^k - 1 = 10(9a + 1) - 1 =$
$= 90a + 10 - 1 = 90a + 9 = 9(10a + 1) \Rightarrow 9 \mid (10^n - 1)$
cbd.

Příklad F.6: Věta: $(\forall n \in N\text{-}\{1\})\ 3 \mid (10^n + 4^n - 2)$

důkaz: a) pro $n_0 = 2$ ... $10^n + 4^n - 2 = 100 + 16 - 2 = 114 \Rightarrow 3 \mid 114$
b) pro $k > 2$ .. $3 \mid (10^k + 4^k - 2) \Rightarrow 10^k + 4^k - 2 = 3a \Rightarrow 10^k = 3a - 4^k + 2$
předpokládáme platnost
c) pro $k + 1$ ... $3 \mid (10^{k+1} + 4^{k+1} - 2) \Rightarrow 10^{k+1} + 4^{k+1} - 2 = 10.10^k + 4^{k+1} - 2$
$= 10(3a - 4^k + 2) + 4^{k+1} - 2 = 30a - 10.4^k + 20 + 4.4^k - 2 = 30a - 6.4^k =$
$= 3(10a - 2.4^k) \Rightarrow$ tento součin je dělitelný třemi $\Rightarrow$ věta byla dokázána
cbd.

Příklad F.7: Věta: $(\forall n \in N)\ 31 \mid (5^{n+1} + 6^{2n-1})$

důkaz: a) pro $n_0 = 1$ $5^{n+1} + 6^{2n-1} = 25 + 6 = 31 \Rightarrow 31 \mid 31$
b) pro $k > 1$ $31 \mid (5^{k+1} + 6^{2k-1}) \Rightarrow 5^{k+1} + 6^{2k-1} = 31a \Rightarrow$
$\Rightarrow 5.5^k + 36^k/6 = 31a \Rightarrow 30.5^k + 36^k = 186a \Rightarrow$
$\Rightarrow 36^k = 186a - 30.5^k$
předpokládáme platnost
c) pro $k + 1$ $31 \mid (5^{k+2} + 6^{2(k+1)-1}) \Rightarrow 5^{k+2} + 6^{2k+1} = 25.5^k + 6.6^{2k} =$
$= 25.5^k + 6.36^k = 25.5^k + 6(186a - 30.5^k) =$
$= 25.5^k + 1116a - 180.5^k = -155.5^k + 1116a = 31(36a - 5.5^k) \Rightarrow$
$\Rightarrow 31 \mid 5^{n+1} + 6^{2n-1}$
cbd.

Příklad F.8: Věta: $(\forall n \in N\text{-}\{1;2\})\ 2^n > 2n + 1$

důkaz: a) pro $n_0 = 3$ $8 > 7$
b) pro $k > 3$ $2^k > 2k + 1$
předpokládáme platnost
c) pro $k + 1$ $2^{k+1} > 2(k+1) + 1 \Rightarrow 2^{k+1} > 2k + 3$
z předpokladu $2^k > 2k + 1$ dostaneme po vynásobení dvěma
$2^{k+1} > 4k + 2 \Rightarrow P = 4k + 2 = 2k + 2k + 2 > 2k + 3$, protože
$k > 1 \Rightarrow 2^{k+1} > 2k + 3$
cbd.

Úlohy:

F.1. Dokaž větu: $(\forall n \in N)\ 1.2.3 + 2.3.4 + 3.4.5 + ... + n(n+1)(n+2) = \dfrac{n(n+1)(n+2)(n+3)}{4}$

F.2. Dokaž větu: $(\forall n\in N)\ 1^2 + 3^2 + 5^2 + ... (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$

F.3. Dokaž větu: $(\forall n\in N)\ \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}$

F.4. Dokaž větu: $(\forall n\in N)\ 1.1! + 2.2! + 3.3! + ... + n.n! = (n+1)! - 1$

F.5. Dokaž větu: $(\forall n\in N)\ 2 + 4 + 6 + ... + 2n = n(n+1)$

F.6. Dokaž větu: $(\forall n\in N)\ 15 \mid (n^5 - 5n^3 + 4n)$

F.7. Dokaž větu: $(\forall n\in N)\ 6 \mid (2n^3 + 3n^2 + n)$

F.8. Dokaž větu: $(\forall n\in N)\ 1.2 + 2.3 + ... + n(n+1) = \frac{n(n+1)(n+2)}{3}$

F.9. Dokaž větu: $(\forall n\in N)\ 1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$

F.10. Dokaž větu: $(\forall n\in N_0)\ \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+...+\binom{n}{n} = 2^n$

F.11. Dokaž, že pro počet úhlopříček p_n v konvexním n-úhelníku (n>3) platí vzorec $p_n = \frac{1}{2}n(n-3)$.

F.12. Dokaž větu: $(\forall n\in N)\ \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$

G. Jiné důkazové postupy

Do této kapitoly lze zařadit důkazové postupy, které jsou netradiční, netypické, které se nepodařilo ”zařadit” do některého z předešlých oddílů.

Příklad G.1: Věta: $(\forall n\in N)\ 3 \mid (n^2 + 2) \Rightarrow 3 \# n$
obměněná věta: $3 \mid n \Rightarrow 3 \# (n^2 + 2)$
její negace: $3 \mid n \wedge 3 \mid (n^2 + 2)$

důkaz: dokazujeme obměněnou větu sporem
$3 \mid n \Rightarrow n = 3k \Rightarrow n^2 = 9k^2 \Rightarrow n^2 + 2 = 9k^2 + 2 \Rightarrow 3 \# (n^2 + 2)$ ... což je spor, protože obě části konjunkce mají platit, tedy má $3 \mid (n^2 + 2) \Rightarrow$
$\Rightarrow$ neplatí negovaná věta $\Rightarrow$ platí věta obměněná $\Rightarrow$ platí věta původní
cbd.

Příklad G.2: Věta: Číslo je dělitelné čtyřmi tehdy, když je čtyřmi dělitelné „poslední“ dvojčíslí.

důkaz: k důkazu věty využijeme větu, o jejíž platnosti se důvtipný čtenář těchto řádků může sám přesvědčit (viz úloha 2):
$(\forall a,b,n\in N)\ n \mid a \wedge n \mid b \Rightarrow n \mid (a + b)$
libovolné přirozené číslo lze zapsat ve tvaru $a_n a_{n-1} a_{n-2} \ldots\ldots a_2 a_1 a_0$, kde a_i značí jednotlivé cifry čísla
$a_n a_{n-1} a_{n-2} \ldots\ldots a_2 a_1 a_0 = 100 \cdot a_n a_{n-1} a_{n-2} \ldots\ldots a_2 + a_1 a_0 =$
$= 4 \cdot (25 \cdot a_n a_{n-1} a_{n-2} \ldots\ldots a_2) + a_1 a_0 \Rightarrow 4 \mid (4 \cdot 25 \cdot a_n a_{n-1} a_{n-2} \ldots\ldots a_2)$ a k tomu, aby číslo $a_n a_{n-1} a_{n-2} \ldots\ldots a_2 a_1 a_0$ bylo dělitelné čtyřmi je třeba, aby i číslo $a_1 a_0$ bylo dělitelné čtyřmi, což je ovšem vyslovený znak dělitelnosti
cbd.

Úlohy:
G.1. Dokaž Pythagorovu větu.
G.2. Dokaž Eukleidovy věty.
G.3. Dokaž větu: Součet vnitřních úhlů v trojúhelníku je roven přímému úhlu.
G.4. Dokaž Thaletovu větu.
G.5. Dokaž větu o středovém a obvodovém úhlu. (Zvol ”nejjednodušší” variantu.)
G.6. Dokaž větu: Kvadratická rovnice $ax^2 + bx + c = 0$ má dva různé reálné kořeny tehdy, když $b^2\text{-}4ac > 0$.
G.7. Dokaž: $\lim_{x\to 0} \frac{\sin x}{x}$
G.8. Dokaž: $(\forall r,s\in R^+)(\forall a\in R^+\text{-}\{1\})\ \log_a(r.s) = \log_a r + \log_a s$
G.9. Dokaž větu: Číslo je dělitelné osmi tehdy, když je osmi dělitelné „poslední“ trojčíslí.
G.10. Dokaž větu: Číslo je dělitelné třemi tehdy, když je třemi dělitelný ciferný součet tohoto čísla. (Zvol „důkaz“ pro pěticiferné číslo.)
G.11. Dokaž, že číslo $a = \sqrt{7\sqrt{7\sqrt{7\sqrt{7\sqrt{\ldots}}}}} \in Z$
G.12. Dokaž, že prvočísel je nekonečně mnoho (tzv. Eukleidův důkaz existence nekonečné řady prvočísel).
G.13. Dokaž, že součet prvních n členů aritmetické posloupnosti je $s_n = \frac{n}{2}(a_1 + a_n)$

G.14. Dokaž, že součet prvních n členů geometrické posloupnosti je $s_n = a_1 \frac{1-q^n}{1-q}$