Nepřímý důkaz se používá pro některé výroky formulované jako implikace a je zahájen obměnou dokazované implikace. Další tvrzení se vyvozují podobně jako u přímého důkazu.

Při vytváření (matematické) teorie zpravidla vycházíme z hypotéz. **Hypotéza** je tvrzení, u něhož je evidentní, že může nabývat právě jedné pravdivostní hodnoty, pravdivostní hodnota však není v daném okamžiku známa. Hypotéza je tedy výrokem, u něhož se pravdivostní hodnota teprve hledá.

Úloha 14

Dokažte, že v oboru $\mathbf{N}$ platí:

a) Libovolné složené číslo lze rozložit alespoň na dva činitele různé od 1 a od sebe samého.
b) Nejmenší dělitel m libovolného složeného čísla s, který je různý od 1, musí být prvočíslem.

Řešení:
Nejprve je třeba nahlédnout zadání. Zvolme několik ukázek:
$4 = 2 \cdot 2,\ 99 = 3 \cdot 3 \cdot 11 = 3 \cdot 33 = 9 \cdot 11 = 3^2 \cdot 11,\ 35 = 5 \cdot 7$ a podobně. Všechna tři čísla lze rozložit alespoň na dva dělitele různé od 1, oba jsou menší než složené číslo, které rozkládáme. Nejmenší takový dělitel je prvočíslo (2, 3 a 5).

a) Důkaz (přímý):
Složené číslo s není prvočíslo, proto existuje alespoň jeden jeho dělitel různý od 1 a od s. Vyberme si nejmenšího takového dělitele m, který splňuje tyto podmínky. Po vydělení složeného čísla s jeho dělitelem m dostaneme podíl d $(s : m = d)$, který musí být menší než dělenec s, neboť dělitel m je větší než 1. Platí: $(s = m \cdot d \wedge 1 < m) \Rightarrow 1 \cdot d < m \cdot d \Rightarrow d < s$. Pro obě nalezená čísla m, d platí: $1 < m \leq d < s$. Skutečně tedy existují dva činitelé m a d splňující dané podmínky.

b) Důkaz (sporem):
Předpokládejme negaci tvrzení b), tedy že nejmenší dělitel m různý od 1 není prvočíslem. (Např. u čísla 99 bychom předpokládali, že jeho nejmenší dělitel je 9.) V předchozí úloze jsme již dokázali, že takové číslo m můžeme rozložit na součin dvou menších čísel různých od jedné $(m = m_1 \cdot d_1)$. Potom libovolné z těchto dvou čísel je rovněž dělitelem původního složeného čísla $(s = m \cdot d = m_1 \cdot d_1 \cdot d)$, a zároveň menším číslem, než byl předchozí dělitel m. Dělitel m tedy není nejmenší, což je spor. Proto nemůže být pravdivá negace tvrzení b), ale pravdivé je původní tvrzení.

Úloha 15

Je dána podmnožina přirozených čísel $A = \{n \in \mathbf{N};\ 16 \leq n \leq 26\}$.

a) Porovnej hodnotu každého složeného čísla s z množiny A s druhou mocninou m^2 jeho nejmenšího prvočinitele m, výsledky zobecni pro celou množinu A.
b) Pokud se domníváš, že stejné tvrzení by mělo platit v celém oboru přirozených čísel $\mathbf{N}$, vyslov jej jako hypotézu.
c) Dokaž platnost hypotézy z bodu b).

Řešení:

a)

Složené číslo s z množiny A	Rozklad čísla s na prvočinitele	Druhá mocnina nejmenšího prvočinitele m	Složené číslo s z množiny A	Rozklad čísla s na prvočinitele	Druhá mocnina nejmenšího prvočinitele m
16	2^4	4	22	$2 \cdot 11$	4
18	$2 \cdot 3^2$	4	24	$2^3 \cdot 3$	4
20	$2^2 \cdot 5$	4	25	5^2	25
21	$3 \cdot 7$	9	26	$2 \cdot 13$	4

V množině A platí $m^2 \leq s$.

b) Hypotéza: V oboru $\mathbf{N}$ platí, že v rozkladu libovolného složeného čísla s na prvočinitele je druhá mocnina nejmenšího prvočinitele nejvýše rovna danému číslu s.

c) Důkaz: Ke každému složenému číslu s a jeho nejmenšímu prvočiniteli m se najde podíl $d = \frac{s}{m}$, tedy $s = m \cdot d$, kde $1 < m \leq d < s$ (tvrzení z příkladu 14). Platí $m \leq d$, proto je $m^2 = m \cdot m \leq m \cdot d = s$, tedy platí $m^2 \leq s$.

Hypotéza je pravdivá.

Předchozí hypotézu je možné zformulovat do následující věty:

Uvažujme libovolné přirozené číslo n a množinu P všech prvočísel p, jejichž kvadrát p^2 je nejvýše roven číslu n, tedy $p^2 \leq n$. Je-li dané číslo n složené, pak je dělitelné alespoň jedním prvočíslem p z uvedené množiny P. (Např. číslo 221 je složené, je dělitelné číslem 13 a platí $13^2 = 169 < 221$. Podobně i 289 je číslo složené, je dělitelné číslem 17 a platí $17^2 = 289$.)

Úloha 16

Vyslov obměnu výše uvedené věty.

Řešení:

Obměnu lze vytvořit k implikaci, která je ve druhé části uvedené věty. První část zůstává beze změny:

Uvažujme libovolné přirozené číslo n a množinu P všech prvočísel p, jejichž kvadrát p^2 je nejvýše roven číslu n, tedy $p^2 \leq n$. Jestliže přirozené číslo n není dělitelné žádným z prvočísel p uvedené množiny P, pak n není číslem složeným. (Číslo n je prvočíslo nebo číslo 1.).

Úloha 17

a) Dokažte, že číslo 211 je prvočíslem.
b) Zjistěte, je-li číslo 1001 prvočíslem.

Řešení:

a) Využij předchozí věty. Nejprve urči největší prvočíslo p takové, že $p^2 \leq 211$. Hledané číslo je 13. (Prvočíslo 13 je nejbližší menší prvočíslo k číslu $\sqrt{211}$, neboť $\sqrt{211} \doteq 14{,}5$.) Nyní mezi prvočísly od 2 do 13 hledej dělitele čísla 211. Podle základních znaků dělitelnosti snadno vyloučíš čísla 2, 3 a 5, zbývá tedy číslo 211 vydělit postupně čísly 7, 11 a 13. Při dělení vždy dostaneš nenulový zbytek. Žádné ze zkoumaných prvočísel není dělitelem čísla 211, proto je toto číslo prvočíslem.
b) $\sqrt{1001} \doteq 31{,}6$, zkus dělit číslo 1001 postupně prvočísly od 2 do 31. Číslo 1001 je dělitelné číslem 7, není tedy prvočíslem.

Pro obě tvrzení byl použit přímý důkaz využívající výše uvedenou větu, případně její obměny.

1.7 Důkaz matematickou indukcí

Úloha 18

V Kocourkově na louce se konala slavnost. Měla začít až v okamžiku, kdy přijde všech 99 obyvatel. Nikdo však neuměl počítat. Nechalo se vyrobit 99 triček a kapesníky s čísly od 1 do 99. Na slavnost si každý oblékl tričko, k němuž měl přišpendlený kapesník s číslem o 1 vyšším než na tričku. Tričko s číslem 1 získal nejpotrhlejší občan. Aby ho každý poznal, lišilo se od ostatních nápadně zářivou barvou. Vrchní rada, který slavnost zahajoval, si oblékl tričko s nejvyšším číslem. Kapesník pana rady měl výjimečně číslo 1. Občané se celou hodinu trousili na louku. Každý z nich měl na paměti radu, kterou se bezpodmínečně řídil. Jako poslední přišel pan rada. Zadíval se na louku. Když se do trávy usadil i poslední občan, pan rada poznal, že jsou na louce všichni. Jakou radou se Kocourkovští řídili a co musel rada zkontrolovat, aby si byl jist přítomností všech obyvatel?