# Matematická indukce 3

3. seriálová série | Termín odeslání: 4. dubna 2022

Úloha 1. (5 bodů)
Nechť $d$ je největší společný dělitel přirozených čísel $m_1$ a $m_2$. Dokažte, že pokud je $n$ přirozené číslo různé od nuly, je $nd$ největším společným dělitelem čísel $nm_1$ a $nm_2$. V důkazu vycházejte jen z definic a tvrzení ze seriálu.

Úloha 2. (5 bodů)
Ukažte, že pro kladná celá čísla $a$, $b$ platí rovnost

$$\mathrm{NSD}\left(2^a - 1,\ 2^b - 1\right) = 2^{\mathrm{NSD}(a,b)} - 1,$$

kde $\mathrm{NSD}(x, y)$ je největší společný dělitel čísel $x$, $y$.

Úloha 3. (5 bodů)
Nechť $a$ a $b$ jsou kladná celá čísla. Definujme tento algoritmus.

Začneme s dvojicí $(a, b)$. Dokud $a > 0$, budeme provádět následující krok:

(1) Pokud $a < b$, pak dvojici $(a, b)$ nahradíme dvojicí $(2a, b - a)$.
(2) Pokud $a \geq b$, pak dvojici $(a, b)$ nahradíme dvojicí $(a - b, 2b)$.

Pro jaké vstupní hodnoty se algoritmus po nějakém čase zastaví?

# Matematická indukce 3

3. seriálová série — Vzorové řešení

## Úloha 1.

*Nechť $d$ je největší společný dělitel přirozených čísel $m_1$ a $m_2$. Dokažte, že pokud je $n$ přirozené číslo různé od nuly, je $nd$ největším společným dělitelem čísel $nm_1$ a $nm_2$. V důkazu vycházejte jen z definic a tvrzení ze seriálu.* *(Kateřina Panešová)*

Řešení:
Bez újmy na obecnosti předpokládejme, že $m_1 \geq m_2$. Pokud jsou obě čísla nulová, platí

$$\mathrm{NSD}(nm_1, nm_2) = \mathrm{NSD}(0,0) = 0 = n \cdot \mathrm{NSD}(0,0) = n \cdot \mathrm{NSD}(m_1, m_2).$$

Poznamenejme, že $\mathrm{NSD}(0,0) = 0$ vyhovuje definici, neboť nula je společným dělitelem nuly s nulou a zároveň pro všechny další společné dělitele triviálně platí, že jsou děliteli nuly. Podobně vidíme, že je-li právě jedno z čísel nulové, BÚNO $m_1 \neq 0$ a $m_2 = 0$, obdržíme

$$\mathrm{NSD}(nm_1, 0) = nm_1 = n \cdot \mathrm{NSD}(m_1, 0).$$

Nadále předpokládejme, že $m_1$ a $m_2$ jsou obě nenulová. Všechny kroky Eukleidova algoritmu pro čísla $m_1$ a $m_2$ vynásobíme číslem $n$ a upravíme, čímž získáme

$$\begin{aligned} nm_1 &= q_1(nm_2) + nr_1, \\ nm_2 &= q_2(nr_1) + nr_2, \\ nr_1 &= q_3(nr_2) + nr_3, \\ &\vdots \\ nr_i &= q_{i+2}(nr_{i+1}), \end{aligned}$$

kde $r_{i+2} = 0$ je první zbytek rovný nule, tedy $r_{i+1} = d$. Ukážeme, že toto je průběh Eukleidova algoritmu pro čísla $nm_1$ a $nm_2$. Díky tomu, že $n$ je přirozené, platí $nr_1 < nm_2$ a $nr_{j+1} < nr_j$ pro každé $j > 0$. Z jednoznačnosti dělicího algoritmu v každém kroku pak plyne, že se vskutku jedná o Eukleidův algoritmus pro $nm_1$ a $nm_2$. Z toho už nutně

$$\mathrm{NSD}(nm_1, nm_2) = nr_{i+1} = nd,$$

jak jsme chtěli ukázat.

Poznámky:
S úlohou si vesměs všichni řešitelé poradili velmi dobře. Někteří zapomněli zmínit jednoznačnost dělicího algoritmu a nerovnosti pro zbytky. *(Kateřina Panešová)*

## Úloha 2.

*Ukažte, že pro kladná celá čísla a, b platí rovnost*

$$\mathrm{NSD}\left(2^a-1,\ 2^b-1\right)=2^{\mathrm{NSD}(a,b)}-1,$$

*kde* $\mathrm{NSD}(x,y)$ *je největší společný dělitel čísel* $x$, $y$. *(Kateřina Panešová)*

Řešení:
BÚNO nechť $a \geq b$, pak v Eukleidově algoritmu nalezneme čísla $q$ a $r$ taková, že $a = qb + r$ a $r < b$. V exponentech provedeme analogii Eukleidova algoritmu:

$$\begin{aligned}2^a-1&=2^{qb+r}-1\\&=2^{qb+r}-2^r+2^r-1\\&=2^r\left(2^{qb}-1\right)+2^r-1\\&=2^r\tilde{q}\left(2^b-1\right)+2^r-1,\end{aligned}$$

kde $\tilde{q}=\sum_{k=0}^{q-1}2^{bk}$. Protože $2^r-1<2^b-1$, je $2^r-1$ zbytek po dělení $2^a-1$ číslem $2^b-1$.

Pokud do Eukleidova algoritmu vložíme $2^a-1$ a $2^b-1$, příslušné zbytky $\tilde{r}_i$ jsou rovny $2^{r_i}-1$, kde $r_i$ je zbytek v $i$-tém kroku v Eukleidově algoritmu při vstupu $a$ a $b$. Oba algoritmy se také zastaví ve stejném kroku, neboť $\tilde{r}_{i+2}=0=2^{r_{i+2}}-1$, tedy $r_{i+2}=0$, ale zároveň pokud $r_{i+2}=0$, pak i $\tilde{r}_{i+2}=2^0-1=0$. Předchozí zbytek

$$\tilde{r}_{i+1}=\mathrm{NSD}\left(2^a-1,\ 2^b-1\right),$$

zároveň ale

$$\tilde{r}_{i+1}=2^{r_{i+1}}-1=2^{\mathrm{NSD}(a,b)}-1.$$

Spojením obou rovností je tvrzení dokázáno.

Poznámky:
Většina řešitelů se odvolala na Eukleidův algoritmus nebo si vystačila s dělitelností a definicí NSD. Oba přístupy jsou v pořádku. *(Hedvika Ranošová)*

## Úloha 3.

*Nechť a a b jsou kladná celá čísla. Definujme tento algoritmus.*

*Začneme s dvojicí* $(a,b)$. *Dokud* $a>0$, *budeme provádět následující krok:*

(1) *Pokud* $a<b$, *pak dvojici* $(a,b)$ *nahradíme dvojicí* $(2a, b-a)$.
(2) *Pokud* $a \geq b$, *pak dvojici* $(a,b)$ *nahradíme dvojicí* $(a-b, 2b)$.

*Pro jaké vstupní hodnoty se algoritmus po nějakém čase zastaví?* *(Kateřina Panešová)*

Řešení:
Nechť $d=\mathrm{NSD}(a,b)$, $x=\frac{a}{d}$ a $y=\frac{b}{d}$. Ukážeme, že se náš algoritmus zastaví právě tehdy, je-li součet $x+y$ mocninou dvojky.

Nejprve si rozmyslíme, že se algoritmus zastaví pro dvojici $(a,b)$, právě když se zastaví pro $(x,y)$: snadnou indukcí ukážeme, že pokud po $k$ krocích algoritmu z dvojice $(a,b)=(a_0,b_0)$ dostaneme čísla $(a_k,b_k)$, tak po $k$ krocích z $(x,y)=(x_0,y_0)$ dostaneme dvojici $(x_k,y_k)=\left(\frac{a_k}{d},\frac{b_k}{d}\right)$, přičemž obě tato čísla jsou celá. Z toho vidíme, že je $a_k=0$ ekvivalentní $x_k=0$ pro libovolné $k\in\mathbb{N}$, takže se oba algoritmy zastaví po stejném počtu kroků.

Zkoumejme tedy, kdy se algoritmus zastaví pro dvojici nesoudělných čísel $(x, y)$. Zároveň si můžeme všimnout, že náš algoritmus zachovává součet $x + y$, takže je jeho zastavení ekvivalentní tomu, že po čase dospějeme do dvojice $(0, x + y)$.

Nyní indukcí dle počtu kroků ukážeme, že pro výstup algoritmu po $k$ krocích $(x_k, y_k)$ platí, že $\mathrm{NSD}(x_k, y_k)$ dělí $2^k$: pro $k = 0$ tvrzení platí díky výše zmíněné nesoudělnosti $x$ a $y$.

Pro indukční krok nám stačí ukázat, že $\mathrm{NSD}(x_k, y_k)$ dělí $2\,\mathrm{NSD}(x_{k-1}, y_{k-1})$. BÚNO předpokládejme, že platí $(x_k, y_k) = (2x_{k-1}, y_{k-1} - x_{k-1})$, symetrický případ se vyřeší analogicky. Z Eukleidova algoritmu máme $\mathrm{NSD}(x_{k-1}, y_{k-1}) = \mathrm{NSD}(x_{k-1}, y_{k-1} - x_{k-1})$, zároveň pro libovolná přirozená čísla $m$, $n$ zjevně platí $\mathrm{NSD}(m, 2n) \mid 2\,\mathrm{NSD}(m, n)$, takže

$$\mathrm{NSD}(x_k, y_k) = \mathrm{NSD}(2x_{k-1}, y_{k-1} - x_{k-1}) \mid 2\,\mathrm{NSD}(x_{k-1}, y_{k-1} - x_{k-1}) = 2\,\mathrm{NSD}(x_{k-1}, y_{k-1}).$$

Tímto jsme tedy dokázali, že $\mathrm{NSD}(x_k, y_k)$ dělí $2^k$.

Předpokládáme-li, že se algoritmus zastaví po $n$ krocích, pak musí platit $(x_n, y_n) = (0, x + y)$ a $\mathrm{NSD}(x_n, y_n) = x + y$ musí být dělitelem mocniny dvojky neboli mocninou dvojky, takže uvedená podmínka je nutná.

Nyní předpokládejme, že začínáme ze dvojice nesoudělných čísel $(x, y)$, která splňují $x + y = 2^n$ pro přirozené číslo $n$. Indukcí na $n$ ukážeme, že se algoritmus po $n$ krocích zastaví, takže je výše uvedená podmínka zároveň i postačující: pro $n = 1$ je jedinou vyhovující dvojicí $(1, 1)$, ze které algoritmus půjde do $(0, 2)$ a zastaví se.

Pro indukční krok si všimněme, že z nesoudělnosti musí pro $n > 1$ být $x$, $y$ různá lichá čísla. Zároveň díky různosti můžeme ze symetrie BÚNO předpokládat $x < y$. Po prvním kroku se tedy algoritmus dostane do dvojice $(x_1, y_1) = (2x, y - x)$. Protože mají $x$ a $y$ stejnou paritu, je rozdíl $y - x$ sudý, takže $\left(\frac{x_1}{2}, \frac{y_1}{2}\right) = \left(x, \frac{y-x}{2}\right)$ je dvojicí přirozených čísel se součtem $x + \frac{y-x}{2} = 2^{n-1}$. Zároveň z výše odvozeného vztahu můžeme odvodit, že tato čísla budou nesoudělná, neboť

$$2\,\mathrm{NSD}\left(x, \frac{y - x}{2}\right) = \mathrm{NSD}(x_1, y_1) \mid 2\,\mathrm{NSD}(x, y) = 2.$$

Z indukčního předpokladu se tedy algoritmus z dvojice $\left(x, \frac{y-x}{2}\right)$ zastaví po $n - 1$ krocích, takže z původní dvojice $(x, y)$ bude k zastavení zapotřebí $(n - 1) + 1 = n$ kroků, čímž je indukční krok dokončen a máme hotovo.

Poznámky:

Většina úspěšných řešení se vydala podobným směrem jako vzorové řešení. Několikrát se ale objevila i řešení, která přímo indukcí dle $n$ dokázala, pro které dvojice se algoritmus zastaví po $n$ krocích. Taková řešení jsou možná o trochu přímočařejší, ale obsahovala několik ne moc pěkných výpočtů. Nejčastější chybou bylo, že nebylo ukázáno, že podmínka $x + y = 2^n$ je nutná, nýbrž pouze že se pro takové dvojice čísel algoritmus zastaví. Podle toho, jak jednoduché bylo z uvedeného postupu důkaz dokončit, jsem za to strhával dva až tři body. *(Danil Koževnikov)*