Základní pojmy

Řešené příklady

Příklad. Dokažte: $\forall n \in \mathbb{N} : 64 | 3^{2n+3} + 40n - 27$.

Řešení. Důkaz povedeme matematickou indukcí:

1. $n = 1$: $3^{2n+3} + 40n - 27 = 3^{2+3} + 40 - 27 = 243 + 40 - 27 = 256 = 4 \cdot 64$
2. Nechť $64 | 3^{2n+3} + 40n - 27$ pro $n \in \{1, 2, \ldots, k\}$.
3. $k = n + 1$. Pak $3^{2k+3} + 40k - 27 = 3^{2(n+1)+3} + 40(n+1) - 27 =$
   $= 3^{2n+3+2} + 40n + 40 - 27 = 3^2 \cdot 3^{2n+3} + 40n - 27 + 40 =$
   $= 9 \cdot (3^{2n+3} + 40n - 27) - 8 \cdot (40n - 27) + 40 =$
   $= 9 \cdot (3^{2n+3} + 40n - 27) - 64 \cdot 5n + 256 = 9 \cdot (3^{2n+3} + 40n - 27) + 64(4 - 5n)$

□

Příklad. Nechť $(u, v) = 1$. Dokažte, že $(u + v, u - v)$ je rovno buď 1 nebo 2.

Řešení. Jak u, tak v může být buď sudé, nebo liché.

1. u - sudé, v - sudé
   Není splněn předpoklad $(u, v) = 1$.
2. u - liché, v - liché, tj. $u = 2k + 1$, $v = 2l + 1$, $k, l \in \mathbb{Z}$
   Předpokládejme, že existuje prvočíslo $p \neq 2 : p|(u + v) \wedge p|(u - v)$., tj. platí
   $$\begin{aligned} u + v &= pm, \; m \in \mathbb{Z} \\ u - v &= pn, \; n \in \mathbb{Z} \end{aligned}$$
   Ze součtu těchto dvou rovnic plyne, že $p|u$, z jejich rozdílu plyne $p|v$, což je spor se zadáním.
   Tedy platí: $(u + v, u - v) = (2k + 1 + 2l + 1, 2k + 1 - 2l - 1) = 2$.
3. u - liché, v - sudé
   Součet i rozdíl čísel u, v v tomto případě je vždy liché číslo, jejich společným dělitelem tedy nemůže být číslo 2. Pokud by čísla u, v byla soudělná a jejich největším společným dělitelem bylo číslo k, pak by součet i rozdíl byl dělitelný tímto k, a to by také bylo největším společným dělitelem součtu a rozdílu u, v. Protože $k = 1$, je i $(u + v, u - v) = k = 1$.

4. v - liché, u - sudé
   Analogicky jako předchozí případ.

$\square$

Příklad. Pomocí Euklidova algoritmu určete největšího společného dělitele čísel $3^{45}-1$ a $3^{65}-1$.

Řešení.

$$\begin{aligned} 3^{65}-1 &= (3^{45}-1)\cdot 3^{20} + (3^{20}-1) \\ 3^{45}-1 &= (3^{20}-1)\cdot(3^{25}+3^{5}) + (3^{5}-1) \\ 3^{20}-1 &= (3^{5}-1)\cdot(3^{15}+3^{10}+3^{5}+1) + 0 \end{aligned}$$

$(3^{45}-1, 3^{65}-1) = 3^{5}-1$ $\square$

Příklad. Pomocí předchozího příkladu určete Bezoutovu rovnost pro čísla $3^{45}-1$ a $3^{65}-1$.

Řešení.

$$\begin{aligned} 3^{5}-1 &= (3^{45}-1)-(3^{20}-1)(3^{25}+3^{5}) = \\ &= (3^{45}-1)-[(3^{65}-1)-(3^{45}-1)3^{20}](3^{25}+3^{5}) = \\ &= (3^{45}-1)-(3^{25}+3^{5})(3^{65}-1)+(3^{45}-1)(3^{45}+3^{25}) = \\ &= (3^{45}-1)(3^{45}+3^{25}+1)-(3^{65}-1)(3^{25}+3^{5}) \end{aligned}$$

$\square$

Příklad. Určete, zda jsou daná čísla nesoudělná, popř. po dvou nesoudělná:

1. $6, 10, 15$
2. $3, 7, 16$
3. $21, 31, 41, 51$

Řešení.

1. $(6,10,15)=1$, $(6,10)=2$, $(6,15)=3$, $(10,15)=5$. Čísla $6,10,15$ jsou nesoudělná, ale nejsou po dvou nesoudělná.
2. $(3,7,16)=1$, $(3,7)=1$, $(7,16)=1$, $(3,16)=1$. Čísla $3,7,16$ jsou nesoudělná i po dvou nesoudělná.
3. $(21,31,41,51)=1$, $(21,31)=1$, $(21,41)=1$, $(21,51)=3$, $(31,41)=1$, $(31,51)=1$, $(41,51)=1$. Čísla $21,31,41,51$ jsou nesoudělná, ale nejsou po dvou nesoudělná.

$\square$

Příklad. Nalezněte $\forall a \in \mathbb{Z}$, pro která $(a-3)|(a-3)$

Řešení.

$$\begin{array}{rl}
(a^3 \qquad\qquad - 3) : (a-3) = a^2 + 3a + 9 \\
\underline{-\, a^3 + 3a^2 \qquad\qquad} \\
-\, 3a^2 \qquad - 3 \\
\underline{-\, 3a^2 + 9a \qquad} \\
9a - 3 \\
\underline{-\, 9a + 27} \\
24
\end{array}$$

$(a-3)|(a^3-3) \wedge (a-3)|(a-3)(a^2+3a+9) \Rightarrow (a-3)|24 \Rightarrow \exists k \in \mathbb{Z} : 24 = k \cdot (x-3)$
dělitelé čísla 24: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$
$a \in \{4, 5, 6, 7, 9, 11, 15, 27, 2, 1, 0, -1, -3, -5, -9, -21\}$ □

Příklad. Nalezněte největího společného dělitele $(319, 754) = d$ a určete Bezoutovu rovnost.

Řešení.

$$\begin{aligned}
754 &= 319 \cdot 2 + 116 \\
319 &= 116 \cdot 2 + \ \ 87 \\
116 &= \ \ 87 \cdot 1 + \ \ \underline{29} \\
87 &= \ \ 29 \cdot 3 + \ \ \ \ 0
\end{aligned}$$

$$\underline{(319, 754) = 29}$$

$$\begin{aligned}
29 &= 116 - 87 \cdot 1 = \\
&= 116 - (319 - 116 \cdot 2) = \\
&= (754 - 319 \cdot 2) - (319 - (754 - 319 \cdot 2) \cdot 2) = \\
&= 754 - 319 \cdot 2 - 319 + 754 \cdot 2 - 319 \cdot 4 = \\
&= 754 \cdot 3 + 319 \cdot (-7)
\end{aligned}$$

□