O OŠKLIVÉM LEMÁTKU

PAVEL JAHODA

Prezentace pro přednášku v rámci ŠKOMAM 2014.

Dělitelnost na množině celých čísel

3 dělí 6

Dělitelnost na množině celých čísel

3 dělí 6 protože

Dělitelnost na množině celých čísel

$$3 \text{ dělí } 6 \text{ protože } \quad 6 = 2 \cdot 3$$

Dělitelnost na množině celých čísel

2 dělí 7 ?

Dělitelnost na množině celých čísel

2 dělí 7 ? $\quad 7 = 3,5 \cdot 2$

Dělitelnost na množině celých čísel

2 dělí 7 ? $\quad 7 = 3,5 \cdot 2$

ale $3,5 \notin \mathbb{Z}$

Dělitelnost na množině celých čísel

2 dělí 7 ? $7 = 3,5 \cdot 2$

ale $3,5 \notin \mathbb{Z}$, proto 2 nedělí 7

Dělitelnost na množině celých čísel

Definice

(a dělí b) Nechť $a, b \in \mathbb{Z}$. Říkáme, že a dělí b (nebo také a je dělitel b, nebo b je násobek a), právě tehdy, když existuje $k \in \mathbb{Z}$ tak, že

$$b = ka.$$

V případě, že a dělí b budeme psát $a \mid b$ a skutečnost, že a nedělí b symbolicky zapíšeme $a \nmid b$.

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :

značíme $\gcd(12, 16)$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :

značíme $\gcd(12, 16) = 4$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

2.) $4 \mid 12,\ 4 \mid 16$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

2.) $4 \mid 12$, $4 \mid 16$ (je to společný dělitel)

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

2.) $4 \mid 12,\ 4 \mid 16$

3.) $(d^* \mid 12,\ d^* \mid 16) \Rightarrow d^* \mid 4$

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

2.) $4 \mid 12,\ 4 \mid 16$

3.) $(d^* \mid 12,\ d^* \mid 16) \Rightarrow d^* \mid 4$ (je největší v absolutní hodnotě)

Největší společný dělitel

Největší společný dělitel čísel 12 a 16 :
$\gcd(12, 16) = 4$

1.) $4 \geq 0$ (je to největší společný dělitel)

2.) $4 \mid 12,\ 4 \mid 16$

3.) $(d^* \mid 12,\ d^* \mid 16) \Rightarrow d^* \mid 4$

Největší společný dělitel

Největší společný dělitel čísel a a b : $\gcd(a, b) = d$

Největší společný dělitel

Největší společný dělitel čísel a a b : $\gcd(a, b) = d$

$\Leftrightarrow$

1.) $d \geq 0$

Největší společný dělitel

Největší společný dělitel čísel a a b : $\gcd(a, b) = d$

$\Leftrightarrow$

1.) $d \geq 0$

2.) $d \mid a$, $d \mid b$

Největší společný dělitel

Největší společný dělitel čísel a a b : $\gcd(a, b) = d$

$\Leftrightarrow$

1.) $d \geq 0$

2.) $d \mid a,\ d \mid b$

3.) $(d^* \mid a,\ d^* \mid b) \Rightarrow d^* \mid d$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$816 = 2 \cdot 300 + 216$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$816 = 2 \cdot 300 + 216$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$

Euklidův algoritmus

Nalezněte největšího společného dělitele čísel 300 a 816.

$$\begin{aligned} 816 &= 2 \cdot 300 + 216 \\ 300 &= 1 \cdot 216 + 84 \\ 216 &= 2 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$

Největším společným dělitelem čísel 300 a 816 je poslední nenulový zbytek v Euklidově algoritmu. To jest,

$$\gcd(300, 816) = 12.$$

Euklidův algoritmus

Věta

(Euklidův algoritmus) Nechť $a, b \in \mathbb{N}$, $b \geq a$. *Jestliže* $a = b$, *potom* $\gcd(a, b) = a$. *Jestliže* $b > a$, *potom existje* $n \in \mathbb{N} \cup \{0\}$ *tak, že existují čísla* $r_{-1} = b$, $r_0 = a$, $q_j \in \mathbb{N}$, $r_j \in \mathbb{N} \cup \{0\}$ *pro* $j = 1, \ldots, n+1$ *takové, že pro každé* $i = -1, \ldots, n-1$ *platí*

$$r_i = q_{i+2}.r_{i+1} + r_{i+2}, \ 0 \leq r_{i+2} < r_{i+1},$$

$$a = r_0 > \cdots > r_{n+1} = 0.$$

Největším společným dělitelem čísel a a b je pak číslo r_n *(poslední nenulový zbytek, případně* $r_n = r_0 = a$*), tj.* $\gcd(a, b) = r_n$.

Ošklivé lemátko

Lema

Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(a, b) = x_0 a + y_0 b.$$

Ošklivé lemátko

Lema

Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(a, b) = x_0 a + y_0 b.$$

Příklad: $\gcd(5, 3) = 1$

Ošklivé lemátko

Lema

Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(a, b) = x_0 a + y_0 b.$$

Příklad: $\gcd(5, 3) = 1$

$$\gcd(5, 3) = 1 \quad = \quad x_0 5 + y_0 3$$

Ošklivé lemátko

Lema

Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(a, b) = x_0 a + y_0 b.$$

Příklad: $\gcd(5, 3) = 1$

$$\gcd(5, 3) = 1 \quad = \quad x_0 5 + y_0 3$$

$$\gcd(5, 3) = 1 \quad = \quad 2 \cdot 5 + (-3) \cdot 3$$

Ošklivé lemátko

Lema

Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(a, b) = x_0 a + y_0 b.$$

Příklad: $\gcd(5, 3) = 1$

$$\begin{aligned} \gcd(5,3) = 1 &= x_0 5 + y_0 3 \\ \gcd(5,3) = 1 &= 2 \cdot 5 + (-3) \cdot 3 \\ \gcd(5,3) = 1 &= -4 \cdot 5 + 7 \cdot 3 \end{aligned}$$

Lema

Jestliže $k \mid ab$, $\gcd(k, a) = 1$, *potom* $k \mid b$

Lema

Jestliže $a, b, c \in \mathbb{Z}$, *potom* $\gcd(ca, cb) = |c| \cdot \gcd(a, b)$.

Věta

Nechť $a, b \in \mathbb{N}$. *Potom platí*

$$n(a,b) = \frac{ab}{\gcd(a,b)}.$$

Lema

Nechť p je prvočíslo, $s \in \mathbb{N}$. Jestliže $p \mid (a_1 . \cdots . a_s)$, potom p dělí alespoň jedno z čísel $a_1, \ldots, a_s$, tj. $p \mid a_1 \vee \cdots \vee p \mid a_s$.

Lema

Pro každé přirozené číslo k platí

$$\prod_{\substack{p\in\mathbb{P}\\ k+1<p\leq 2k+1}} p < 4^k.$$

Věta

Nechť $ac \equiv bc \pmod{m}$ *a* $\gcd(m, c) = 1$. *Potom* $a \equiv b \pmod{m}$.

Věta

(O jednoznačnosti kanonického rozkladu - Základní věta aritmetiky)
Pro každé přirozené číslo $n \neq 1$ *existuje právě jeden kanonický rozklad na součin prvočísel. Tj. pokud* $p_1, \ldots, p_m, q_1, \ldots, q_s$ *jsou prvočísla (nemusí být navzájem různá) a platí*

$$n = p_1 . \cdots . p_m = q_1 . \cdots . q_s, \tag{1}$$

potom $m = s$ *a pro každé* $i \in \{1, \ldots, m\}$ *existuje* $j_i \in \{1, \ldots, s\}$ *takové, že* $p_i = q_{j_i}$.

Lema

Pro každé přirozené číslo $n \geq 2$ platí

$$\prod_{p \in \mathbb{P}, p \leq n} p < 4^n.$$

Věta

Nechť $\gcd(a, m) = 1$. *Potom lineární kongruence* $ax \equiv b \pmod{m}$ *má jediné řešení.*

Věta

(Fermatova - Eulerova) Nechť $\gcd(a, m) = 1$. *Potom*

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Věta

(První Čebyševova) Existují reálné konstanty $c_1, c_2 > 0$ takové, že pro každé $x \geq 2$ platí

$$c_1 \frac{x}{\ln x} < \pi(x) < c_2 \frac{x}{\ln x}.$$

RSA algoritmus šifrování + lema ověřující jeho korektnost:

Lema

Nechť p, q jsou dvě navzájem nesoudělná čísla potom pro každé $k \in \mathbb{N}$ platí

$$p^{k\varphi(pq)+1} \equiv p (\mathrm{mod}\, pq).$$