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

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

Důkaz: α) $a = 0 \Rightarrow \gcd(a,b) = |b| = 0 \cdot a \pm b$

β) $b = 0 \Rightarrow \gcd(a,b) = |a| = \pm a + 0 \cdot b$

γ) $a, b \in \mathbb{Z} - \{0\} \Rightarrow |a|, |b| \in \mathbb{N} \Rightarrow$

$$\gcd(a,b) = \gcd(|a|,|b|) = \min M(|a|,|b|) = \min\left(\{x|a| + y|b| \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}\right)$$

$$\Rightarrow \exists x_0^*, y_0^* \in \mathbb{Z}: \quad \gcd(a,b) = x_0^*|a| + y_0^*|b| = \underbrace{x_0^* \cdot sig(a)}_{x_0 \in \mathbb{Z}} \cdot a + \underbrace{y_0^* \, sig(b)}_{y_0 \in \mathbb{Z}} b =$$
$$= x_0 a + y_0 b$$

$\square$

(Funkce signum: $sig(a) = 1$ pro $a > 0$; $sig(a) = -1$ pro $a < 0$; $sig(0) = 0$
$\Rightarrow |a| = sig(a) \cdot a$)

Věta (Euklidovo lema): Nechť $k, a, b \in \mathbb{Z}$. Potom platí:

$$(k \mid a \cdot b \ \wedge \ \gcd(k,a) = 1) \Rightarrow k \mid b$$

Důkaz: $\gcd(k,a) = 1 \Rightarrow \exists x_0, y_0 \in \mathbb{Z}:$

$$x_0 k + y_0 a = 1 \quad / \cdot b$$
$$x_0 bk + y_0 ab = b \quad / \ k \mid ab \Rightarrow \exists k_1 \in \mathbb{Z}: ab = k_1 k$$
$$x_0 bk + y_0 k_1 k = b$$
$$\underbrace{(x_0 b + y_0 k_1)}_{\in \mathbb{Z}} k = b$$
$$k \mid b$$

$\square$

Euklidův algoritmus

Uvažujme $a, b \in \mathbb{N}$, $a < b$.

$d | b$ $\quad b = q_1 a + r_1$ $\quad | \; 0 \le r_1 < a$

$d | a \Leftarrow$ $\quad a = q_2 r_1 + r_2$ $\quad | \; 0 \le r_2 < r_1$

$d | r_1 \Leftarrow$ $\quad r_1 = q_3 r_2 + r_3$ $\quad | \; 0 \le r_3 < r_2$

$d | r_2 \Leftarrow$ $\quad r_2 = q_4 r_3 + r_4$ $\quad | \; 0 \le r_4 < r_3 < r_2 < r_1 < a < b$

$d | r_3 \Leftarrow$ $\quad \vdots$

$\Rightarrow r_i$ je klesající posloupnost nezáporných celých čísel

$\Rightarrow$ po konečném počtu kroků musí nastat $r_m = 0$

$d | r_{m-3} \Leftarrow$ $\quad r_{m-3} = q_{m-1} r_{m-2} + r_{m-1}$

$d | r_{m-2} \Leftarrow$ $\quad r_{m-2} = q_m \underbrace{r_{m-1}}_{= d \ge 0} + 0$

$\Rightarrow$ 1.) $d = r_{m-1} \ge 0$

2.) $d | a \wedge d | b$

3.) Z výše uvedených rovnic je možno vyjádřit $r_{m-1} = d$ jako lineární kombinaci čísel a, b:

$$d = r_{m-1} = r_{m-3} - q_{m-1} \overset{\text{vyjádříme}}{r_{m-2}} = \dots = x_0 a + y_0 b$$

$\Rightarrow$ Jestliže $d^* | a \wedge d^* | b \Rightarrow d^* | d$

$\Rightarrow$ $\underline{\underline{d = r_{m-1} = \gcd(a, b)}}$

7.) Pomocí Euklidova algoritmu nalezněte největšího společného dělitele čísel a, b:

a) $a = 360$; $b = 420$

$$420 = 1 \cdot 360 + 60$$
$$360 = 6 \cdot 60 + 0$$
$$\Rightarrow \gcd(420, 360) = 60$$

b) $a = 431$; $b = 210$

$$431 = 2 \cdot 210 + 11$$
$$210 = \underbrace{19 \cdot 11}_{209} + 1 \quad \Rightarrow \gcd(431, 210) = 1$$
$$11 = 11 \cdot 1 + 0$$

c) $a = 351$; $b = 762$

$$762 = \underbrace{2 \cdot 351}_{702} + 60$$
$$351 = \underbrace{5 \cdot 60}_{300} + 51$$
$$60 = 1 \cdot 51 + 9$$
$$51 = 5 \cdot 9 + 6$$
$$9 = 1 \cdot 6 + 3 \quad \Rightarrow \gcd(351, 762) = 3$$
$$6 = 2 \cdot 3 + 0$$

d) $a = 1705$; $b = 1650$

$$1705 = 1 \cdot 1650 + 55$$
$$1650 = 30 \cdot 55 + 0$$
$$\Rightarrow \gcd(1705, 1650) = 55$$

e) $a = 1694$, $b = 671$

$$1694 = \underbrace{2 \cdot 671}_{1342} + 352$$
$$671 = 1 \cdot 352 + 319$$
$$352 = 1 \cdot 319 + 33$$
$$319 = \underbrace{9 \cdot 33}_{297} + 22$$
$$33 = 1 \cdot 22 + 11 \Rightarrow$$
$$22 = 2 \cdot 11 + 0$$
$$\Rightarrow \gcd(1694, 671) = 11$$

Def ($\gcd(a_1, a_2, \dots, a_n)$). Nechť $a_1, \dots, a_n \in \mathbb{Z}$, $n \in \mathbb{N}$. Největším společným dělitelem čísel $a_1, a_2, \dots, a_n$ nazveme číslo d splňující podmínky:

1.) $d \geq 0$

2.) $d \mid a_1, \dots, d \mid a_n$

3.) $d^* \mid a_1, \dots, d^* \mid a_n \Rightarrow d^* \mid d$

Značíme $d = \gcd(a_1, \dots, a_n)$.

Poznámka Tato definice umožňuje i speciální případ $n = 1$.
Čemu je roven $\gcd(a_1)$?
Označme $d = \gcd(a_1)$.

1.) $d \geq 0$

2.) $d \mid a_1$

3.) $d^* \mid a_1 \Rightarrow d^* \mid d$

Víme, že $d^* = a_1$ je dělitelem a_1: $a_1 \mid a_1 \Rightarrow a_1 \mid d$ $\Big\} \Rightarrow$

$$\Rightarrow (d \mid a_1 \wedge a_1 \mid d) \Rightarrow |d| = |a_1| \qquad / \, d \geq 0$$

$$d = |a_1|$$

$$\boxed{\gcd(a_1) = |a_1|}$$

Věta: Nechť $a_1, \dots, a_n \in \mathbb{Z}$, $\forall n \in \mathbb{N}$. Potom $\gcd(a_1, \dots, a_n)$ existuje a je určen jednoznačně. Navíc platí (pro $n \geq 2$):

$$\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$$

Důkaz: α) $n = 1 \Rightarrow \gcd(a_1) = |a_1|$ viz. předchozí poznámka

β) $n \geq 2$ Důkaz provedeme indukcí

1.) $n = 2 \Rightarrow \gcd(a_1, a_2)$ existuje a je určen jednoznačně - dokázáno na předn.

$$\gcd(\gcd(a_1), a_2) = \gcd(|a_1|, a_2) = \gcd(a_1, a_2)$$

2.) Indukční krok. Předpokládejme, že $\gcd(a_1, \dots, a_{n-1})$ existuje a označme $d = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$ (takové číslo existuje a je určeno jednoznačně

I.) $d \geq 0$ (je to gcd)

II.) $d \mid \gcd(a_1, \dots, a_{n-1})$, $d \mid a_n \Rightarrow d \mid a_1, \dots, d \mid a_{n-1}, d \mid a_n$

III.) $d^* \mid a_1, \dots, d^* \mid a_{n-1}, d^* \mid a_n \Rightarrow d^* \mid \gcd(a_1, \dots, a_{n-1})$, $d^* \mid a_n \Rightarrow d^* \mid d$

$\Rightarrow d = \gcd(a_1, \dots, a_n) \Rightarrow \gcd(a_1, \dots, a_n)$ existuje a $= \gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$

Jednoznačnost plyne z 3.) podm. definice $\left.\begin{matrix} d_1 = \gcd(a_1, \dots, a_n) \\ d_2 = \gcd(a_1, \dots, a_n) \end{matrix}\right\} \Rightarrow d_1 \mid d_2 \wedge d_2 \mid d_1 \Rightarrow d_1 = d_2$ □

Př: Určete gcd(1305, 555, 235)

$\gcd(1305, 555) = ?$

$$1305 = \underbrace{2\cdot 555}_{1110} + 195$$

$$555 = \underbrace{2\cdot 195}_{390} + 165$$

$$195 = 1\cdot 165 + 30$$

$$165 = 5\cdot 30 + 15 = \gcd(1305, 555)$$

$$30 = 2\cdot 15 + 0$$

$\Rightarrow \gcd(1305, 555, 235) = \gcd(15, 235)$

$$235 = \underbrace{15\cdot 15}_{225} + 10$$

$$15 = 1\cdot 10 + 5 \Rightarrow \underline{\underline{\gcd(1305, 555, 235) = 5}}$$

$$10 = 2\cdot 5 + 0$$

$\boxed{\text{Př. 1. Nechť } a, b \in \mathbb{Z}. \text{ Potom } \gcd(a-b, b) = \gcd(a,b)}$

Důkaz: Označme $d = \gcd(a,b)$ a $d_1 = \gcd(a-b, b)$.

a) $d = \gcd(a,b) \Rightarrow$ 1.) $d \geq 0$
2.) $(d \mid a \wedge d \mid b) \Rightarrow (d \mid a \wedge d \mid -b) \Rightarrow (d \mid (a-b) \wedge d \mid b) \Rightarrow$
$\Rightarrow d \mid d_1$ (protože $d_1 = \gcd(a-b, b)$)

b) $d_1 = \gcd(a-b, b) \Rightarrow$ 1.) $d_1 \geq 0$
2.) $(d_1 \mid (a-b) \wedge d_1 \mid b) \Rightarrow (d_1 \mid \overbrace{(a-b)+b}^{=a} \wedge d_1 \mid b) \Rightarrow$
$\Rightarrow d_1 \mid d$ (protože $d = \gcd(a,b)$)

$\Rightarrow$ Z a) a b) plyne, že $|d_1| = |d|$ a protože $d_1, d \geq 0 \Rightarrow d = d_1$.

$\boxed{\text{Př. 2. Nechť } a, b \in \mathbb{Z}. \text{ Potom } \gcd(a+b, b) = \gcd(a,b).}$

Důkaz:

a) $d = \gcd(a,b) \Rightarrow$ 1.) $d \geq 0$
2.) $(d \mid a \wedge d \mid b) \Rightarrow (d \mid (a+b) \wedge d \mid b) \Rightarrow$
$\Rightarrow d \mid d_1 = \gcd(a+b, b)$

b) $d_1 = \gcd(a+b, b) \Rightarrow$ 1.) $d_1 \geq 0$
2.) $(d_1 \mid (a+b) \wedge d_1 \mid b) \Rightarrow$
$\Rightarrow (d_1 \mid \underbrace{(a+b)-b}_{a} \wedge d_1 \mid b) \Rightarrow$
$\Rightarrow d_1 \mid d$

$\Rightarrow$ Z a) a b) plyne, že $|d_1| = |d|$ a protože $d_1, d \geq 0 \Rightarrow d_1 = d$.

Př.3: Nechť $a, b \in \mathbb{Z}$. Potom $\gcd(a,b) = \gcd(a-b, a) = \gcd(a+b, a)$.

Důkaz: Podle předchozího:

$$\gcd(a,b) = \gcd(b,a) = \gcd(b-a, a) = \gcd(a-b, a)$$

$$\gcd(a,b) = \gcd(b,a) = \gcd(b+a, a) = \gcd(a+b, a)$$

Př.4: Nechť $a, b, k_1, k_2 \in \mathbb{Z}$. Potom $\gcd(a,b) = \gcd(k_1 a + k_2 b, a)$.

D: $$\gcd(a,b) \underset{\substack{\uparrow \\ \text{Př.3.}}}{=} \gcd(a \pm b, a) \underset{\substack{\uparrow \\ \text{Př.3.}}}{=} \gcd(a \pm 2b, a) = \dots \underset{\substack{\uparrow \\ \text{Př.3.}}}{=} \gcd(a + k_2 b, a) \underset{\substack{\uparrow \\ \text{Př.1 a 2.}}}{=}$$

$$= \gcd(a \pm a + k_2 b, a) = \gcd(a \pm 2a + k_2 b, a) =$$

$$= \gcd(k_1 a + k_2 b, a)$$