Místo "m dělí n" také někdy říkáme "n je <u>násobek</u> čísla m".

Pro dvě nenulová celá čísla m, n a čísla $\alpha, \beta \in \{1, -1\}$ platí:

$$m \mid n \iff \alpha m \mid \beta n$$

Speciálně:

$$m \mid n \iff |m| \mid |n|$$

Když m, n jsou celá čísla. Platí:

$$\boxed{m \mid n \wedge n \neq 0 \implies m \leq |n|}$$

[Př.: $m \mid n \wedge n \neq 0$ Ch.: $m \leq |n|$

$n = mq$, $q \in \mathbb{Z}$; $|n| = |m| \cdot |q|$

$n \neq 0$, tedy $|n| > 0$, $|m| \geq 0$, $|q| > 0$

$1 \leq |q| \mid \cdot |m|$

$|m| \leq |m| \cdot |q|$

$|m| \leq |n|$

$\underline{m \leq |n|}$ (je $m \leq |m|$)]

Když m, n jsou celá čísla, $m \neq 0$ nebo $n \neq 0$. Největší <u>společný dělitel</u> čísel m, n (značíme: $GCD(m, n)$) definujeme takto:

$$\boxed{GCD(m,n) = \max \{d \in \mathbb{Z} \mid d|m \wedge d|n\}}$$

Kontrola definice: Nechť $M = \{d \in \mathbb{Z} \mid d|m \wedge d|n\}$.
$M \neq \emptyset$, protože $1 \in M$
M je shora omezená: ~~Nechť $d \in M$, pak $d|$~~
Je $m \neq 0$ nebo $n \neq 0$, nechť například $m \neq 0$. Nechť $d \in M$. Pak $d|m$ a tedy $d \leq |m|$.

Nechť m, n jsou nenulová celá čísla. Pak nejmenší společný násobek čísel m, n (označení: $LCM(m,n)$) definujeme takto:

$$\boxed{LCM(m,n) = \min \{k \in \mathbb{Z} \mid k > 0 \wedge m|k \wedge n|k\}}$$

Kontrola definice: Je $M \subseteq \mathbb{Z}^+$. Stačí ukázat, že $M \neq \emptyset$.
Ukážeme, že $|m \cdot n| \in M$.
Je $|m \cdot n| \in \mathbb{Z}$, $|m \cdot n| > 0$, protože $m \neq 0$, $n \neq 0$.
Jsou 2 možnosti: $mn > 0$, $mn < 0$
$m \cdot n > 0$: $|m \cdot n| = m \cdot n$, $m | m \cdot n$, $n | m \cdot n$
$m \cdot n < 0$: $|m \cdot n| = (-1) \cdot m \cdot n$ ~~$m | m \cdot n$~~,
$m | (-1) \cdot m \cdot n$, $n | (-1) \cdot m \cdot n$
Tedy: $m \mid |m \cdot n|$, $n \mid |m \cdot n|$.

K výpočtu $GCD(m,n)$ pro celá čísla m, n, $0 \leq n < m$, můžeme použít následující, více než 2300 let starý rekurzivní algoritmus.

ALGORITHMUS 4.1.1. (EUKLIDŮV ALGORITHMUS)

Pro celá čísla m, n, $0 \leq m < n$, máme:

$$GCD(0, n) = n$$

$$GCD(m, n) = GCD(n \bmod m, m) \quad \text{pro } m > 0$$

Korektnost Euklidova algoritmu:

(I) $GCD(0, n) = n$:
Jistě $n \mid 0$, $n \mid n$.
Nechť d je také číslo, $d \mid 0$, $d \mid n$. Chceme: $d \leq n$.
Víme $n \neq 0$ (je $0 < n$), a $d \mid n$ tedy $d \leq |n|$.
Dáno $|n| = n$, tedy $d \leq n$.

(II) Nechť $m > 0$. Chceme, že $GCD(m, n) = GCD(n \bmod m, m)$.
Buď $d \in \mathbb{Z}$, chceme ukázat, že
$d \mid m \wedge d \mid n \iff$ ~~$d \mid GCD(a$~~
$d \mid n \bmod m \wedge d \mid m$

$\Rightarrow$: PČ: $d \mid n \wedge d \mid m$
CH: $d \mid n \bmod m \wedge d \mid m$
Jistě $d \mid m$.
$n \bmod m = n - m \cdot \left\lfloor \frac{n}{m} \right\rfloor$

Víme $d \mid n$ a $d \mid m$, dokázali $d \mid n \bmod m$.

$\Leftarrow$: PČ: $d \mid n \bmod m \wedge d \mid m$
CH: $d \mid m \wedge d \mid n$
Jistě $d \mid m$.
$n \bmod m = n - m \cdot \left\lfloor \frac{n}{m} \right\rfloor$, $n = n \bmod m + m \cdot \left\lfloor \frac{n}{m} \right\rfloor$

Tedy $d \mid n \bmod m$ a $d \mid m$, máme $d \mid n$.

(III) Když $m > 0$, je $0 \leq n \bmod m < m$, tedy během výpočtu nedostaneme žádné volání, neboť $(n \bmod m, m)$ je přípustná vstupní dvojice.
Důkaz: Výpočet skončí po konečně mnoha krocích, jelikož první složka dvojice se v každém kroku zmenší (m, n).

PŘÍKLAD 4.1.2.

$GCD(27, 36) = GCD(9, 27) = GCD(0, 9) = \underline{\underline{9}}$

$GCD(214, 352) = GCD(138, 214) = GCD(76, 138)$
$= GCD(62, 76) = GCD(14, 62) = GCD(6, 14)$
$= GCD(2, 6) = GCD(0, 2) = \underline{\underline{2}}$

— 29.3.2022

Jsou-li m, n celá čísla, $0 \leq m < n$, pak tzv. rozšířený Euklidův algoritmus vypočítá taková celá čísla m' a n' splňující

$$m' \cdot m + n' \cdot n = GCD(m, n)$$

To je jedna z nejdůležitějších aplikací Euklidova algoritmu.

Pro $m = 0$ je $GCD(m, n) = n$ a můžeme vzít $m' = 0$, $n' = 1$.

Když $m > 0$ a m'', n'' jsou nějaká vhodná celá čísla taková, že

$$m''(n \bmod m) + n'' \cdot m = GCD(n \bmod m, m)$$

pak

$$GCD(m, n) = GCD(n \bmod m, m)$$
$$= m''(n \bmod m) + n'' \cdot m$$
$$= m'' \cdot \left(n - m \cdot \left\lfloor \frac{n}{m} \right\rfloor\right) + n'' \cdot m$$

$$= m'' \cdot m - m' \cdot m \cdot \left\lfloor \frac{n}{m} \right\rfloor + n'' \cdot m$$

$$= \left(n'' - m' \cdot \left\lfloor \frac{n}{m} \right\rfloor \right) \cdot m + m' \cdot n$$

Vememe $m' = n'' - m' \cdot \left\lfloor \frac{n}{m} \right\rfloor$, $n' = m''$

a máme

$$m' \cdot m + n' \cdot n = GCD(m,n).$$

Podle Eukleidův algoritmus umíme k nalezení $GCD(m,n)$ a také najít čísla m' a n' splňující $m' \cdot m + n' \cdot n = GCD(m,n)$, ale nikoho, že jde říci ROZŠÍŘENÝ EUKLIDŮV ALGORITMUS.

PŘÍKLAD 4.1.3.

$GCD(57,237) = GCD(9,57) = GCD(3,9) = GCD(0,3) = 3$

$$237 = 4 \cdot 57 + 9$$
$$57 = 6 \cdot 9 + \underline{3}$$
$$9 = 3 \cdot 3 + 0$$

$$3 = (-6) \cdot 9 + 1 \cdot 57$$
$$= (-6) \cdot ((-4) \cdot 57 + 1 \cdot 237) + 1 \cdot 57 = 24 \cdot 57 + (-6) \cdot 237$$
$$+ 1 \cdot 57 = 25 \cdot 57 + (-6) \cdot 237$$

$$\underline{3 = 25 \cdot 57 + (-6) \cdot 237}$$

Všimněme si, že Eukleidův algoritmus lze užít $GCD(m,n)$ v libovolné dvě celá čísla m a n, $m \neq 0$ nebo $n \neq 0$.

Je $|m| = |n|$ tedy algoritmus nepředpokládá, neboť $GCD(m,n) = |m|$.

Nechť $|m| \neq |n|$. Nechť například $|m| < |n|$.
Pak $0 \leq |m| < |n|$ a Euklidův algoritmus lze užít
$GCD(|m|,|n|)$.
Pro každé celé číslo d a všechna $\alpha, \beta \in \{1,-1\}$ platí:

$$d|a \wedge d|b \iff d|\alpha a \wedge d|\beta b$$

Z toho ihned plyne, že $GCD(m,n) = GCD(\alpha m, \beta n)$,
speciálně $GCD(m,n) = GCD(|m|,|n|)$.

Ještě si všimněme, že Euklidův algoritmus lze pro libovolná celá čísla m,n, $m \neq 0$ nebo $n \neq 0$ najít celá čísla m', n' taková, že $m' \cdot m + n' \cdot n = GCD(m,n)$.
Pro $|m| = |n|$ žádný algoritmus nepotřebujeme, neboť
$GCD(m,n) = |n| = 0 \cdot m + \alpha \cdot n$, kde $\alpha \in \{1,-1\}$.

Nechť $|m| \neq |n|$. Euklidův algoritmus nám dá celá čísla m'', n'' taková, že $m'' \cdot |m| + n'' \cdot |n| = GCD(|m|,|n|)$.
Označme $GCD(m,n) = GCD(|m|,|n|)$, $|m| = \alpha \cdot m$, $|n| = \beta \cdot n$, $\alpha, \beta \in \{1,-1\}$. Pak

$$GCD(m,n) = \alpha \cdot m'' \cdot m + \beta \cdot n'' \cdot n$$

a označme $m' = \alpha \cdot m''$, $n' = \beta \cdot n''$.

Jsou-li m,n dvě celá čísla, $m \neq 0$ nebo $n \neq 0$, pak říkáme, že čísla m a n jsou <u>nesoudělná</u> (značení: $m \perp n$), jestliže $GCD(m,n) = 1$.

TVRZENÍ 4.1.4.
Nechť a,b,c jsou celá čísla. Nechť p je prvočíslo. Platí:

(I) $a|b \cdot c \wedge a \perp b \implies a|c$
(II) $a|c \wedge b|c \wedge a \perp b \implies ab|c$

(III) $p \mid b \cdot c \Rightarrow p \mid b \vee p \mid c$

Důkaz:

(I) PŘ: $a \mid b \cdot c \wedge a \perp b$ CH: $a \mid c$

$GCD(a,b) = a' \cdot a + b' \cdot b$ (a', b' jsou celá čísla)

$1 = a' \cdot a + b' \cdot b \quad | \cdot c$

$c = a' \cdot a \cdot c + b' \cdot bc$

$c = (a'c) \cdot a + b' \cdot (bc)$

Když $a \mid a$, $a \mid bc$, potom $a \mid c$.

(II) PŘ: $a \mid c \wedge b \mid c \wedge a \perp b$ CH: $ab \mid c$

$b \mid c$, tedy $c = bq$ pro nějaké celé číslo q

$a \mid bq$, $a \perp b$, tedy $a \mid q$, $q = a \cdot r$ pro nějaké celé číslo r

$c = bq = bar$, $c = (ab) \cdot r$, $\underline{ab \mid c}$

(III) PŘ: $p \mid b \cdot c$ CH: $p \mid b \vee p \mid c$

Jsou 2 možnosti:
$p \mid b$: jsme hotovi
$p \nmid b$: Buď d nějaké celé číslo, $d \mid p \wedge d \mid b$.
Ukážeme že $d = 1$. Z toho vyplývá, že $GCD(p,b) = 1$, $p \perp b$.
Když p je prvočíslo, je $d = p$ nebo $d = 1$.
Dosaďme $d = p$. Ale $p \mid b$, spor. Takže musí $d = 1$.

Když $p \mid bc \wedge p \perp b$, potom $p \mid c$ (viz část (I)).

Jestliže m a n jsou celá čísla, $n > 0$, $m \perp n$, pak rozšířený Euklidův algoritmus najde celá čísla m', n' taková, že $m' \cdot m + n' \cdot n = 1$. Platí

$$m^{-1} \bmod n = m' \bmod n$$

Dále:

$m^{-1} \bmod n \in \mathbb{Z}$, $0 \le m^{-1} \bmod n < n$,

$n \mid 1 - (m^{-1} \bmod n) \cdot m$.

$$m^{-1} \bmod n = m' \bmod n = m' - n \left\lfloor \frac{m'}{n} \right\rfloor,$$

$$\begin{aligned}(m^{-1} \bmod n) \cdot m &= \left(m' - n \cdot \left\lfloor \frac{m'}{n} \right\rfloor\right) \cdot m \\ &= m'm - n \cdot \left\lfloor \frac{m'}{n} \right\rfloor \cdot m \\ &= 1 - n' \cdot n - n \cdot \left\lfloor \frac{m'}{n} \right\rfloor \cdot m\end{aligned}$$

$$n'n + n \cdot \left\lfloor \frac{m'}{n} \right\rfloor \cdot m = 1 - (m^{-1} \bmod n) \cdot m$$

$$n \cdot \left(n' + \left\lfloor \frac{m'}{n} \right\rfloor \cdot m\right) = 1 - (m^{-1} \bmod n) \cdot m$$

$$n \mid 1 - (m^{-1} \bmod n) \cdot m$$

Poznámka: V jazyku kongruencí (vysvětlení je později), lze místo

$$n \mid 1 - (m^{-1} \bmod m) \cdot m$$

psát $(m^{-1} \bmod n) \cdot m \equiv 1 \pmod n$

Číslo m modulo n se nyní nazývá multiplikativní inverze čísla m modulo n.

V této kapitole budeme analýzu složitosti Euklidova algoritmu.

POMOCNÉ TVRZENÍ

Nechť a, b jsou celá čísla, $0 < a < b$. Pak $b \bmod a < \frac{b}{2}$.

Důkaz: Nastane 2 případy: (I) $a \leq \frac{b}{2}$

(II) $a > \frac{b}{2}$

ad (I): $b \bmod a < a$.

ad (II): Víme: $b - a \cdot \left\lfloor \frac{b}{a} \right\rfloor < \frac{b}{2}$

$$\frac{b}{2} < a \cdot \left\lfloor \frac{b}{a} \right\rfloor$$

Víme: $a \leq a \cdot \left\lfloor \frac{b}{a} \right\rfloor$, tj. $1 \leq \left\lfloor \frac{b}{a} \right\rfloor$.

Víme-li $a < b$, pak $1 < \frac{b}{a}$, $1 \leq \left\lfloor \frac{b}{a} \right\rfloor$.

Na následující větě.

Nechť m, n jsou celá čísla, $0 < m < n$.
Pro běh Euklidova algoritmu zmenší přechod od dvojice (m, n) ke dvojici (m_1, m), kde $m_1 = n \bmod m$.

Důkaz: Platí $m_1 < \frac{n}{2}$.

Předpokládejme $0 < m_1$. Pak $0 < m_1 < m$. Dále platí

Eukleidův algoritmus provede přechod od dvojice (n_1, m) ke dvojici (m_1, n_1), kde $m_1 = m \bmod n_1$.

Dle 1. tvrzení je $m_1 < \frac{m}{2}$.

Zjistili jsme tedy: Eukleidův algoritmus po 2 krocích přejde od dvojice (m,n) ke dvojici (m_1, n_1), kde

$m_1 < \frac{m}{2}$, $n_1 < \frac{n}{2}$.

Předpokládejme nyní, že m, n jsou celá čísla, $0<m<n$.

Předpokládejme navíc, že ~~$m = 2^k$~~. $n = 2^k$.

Výpočet Eukleidova algoritmu pro vstup (m,n) skončí tedy nejpozději po k dvojkrocích (neboť $2^{k-k} = 2^0 = 1$).

Počet rekurzivních volání Eukleidova algoritmu pro vstup (m,n) označme $T(n)$. Je tedy $T(n) \leq 2k = 2 \cdot \lg n$.

Odvodili jsme tedy:

Jestliže $T(n)$ je počet rekurzivních volání Eukleidova algoritmu pro vstup (m,n), pak

$$T(n) \leq O(\lg n).$$

4.2. PRVOČÍSLA

Celé číslo p, $p>1$, se nazývá prvočíslo, jestliže má pouze dva kladné dělitele, 1 a p; v opačném případě