## 1. Základní pojmy

**1.1. Úvodní poznámky.** V mnoha problémech je výhodné vyzkoušet chování algoritmů na reálných příkladech. K tomu lze využít SW nainstalovaný na počítačích Ústavu matematiky a statistiky. Doporučujeme zejména:

- PARI-GP : specializovaný SW na teorii čísel, při výpočtech s většími čísly obvykle výrazně efektivnější než obecně orientované balíky. Spouští se příkazem `gp`. Nejdůležitější příkazy: `\q` – ukončení, `?` – help, `??` – kompletní uživatelský manuál, `?? tutorial` – tutoriál pro úvodní seznámení. Viz také `pari.math.u-bordeaux.fr`.
- SAGE: obecně koncipovaný open-source systém, který mj. zahrnuje interface do Pari-GP a díky jeho prostředí je tak výrazně usnadněna práce. Protože jeho vývoj řídí William Stein, odborník na teorii čísel, je tato část balíku jednoznačně nejpropracovanější. Existuje rovněž mnoho výukových *worksheetů*. Spustit lze např. na `http://sage.math.muni.cz`
- Maple: vhodný zejména kvůli existenci mnoha výukových pracovních listů (worksheets, i pro teorii čísel), např. na `www.mapleapps.com`.

**1.2. Dělitelnost.**

Definice. Řekneme, že celé číslo $a$ *dělí* celé číslo $b$ (neboli číslo $b$ je *dělitelné* číslem $a$, též $b$ je *násobek* $a$), právě když existuje celé číslo $c$ tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$.

Přímo z definice plyne několik jednoduchých tvrzení, jejichž důkaz přenecháváme čtenáři jako cvičení s návodem v [**2**, §12]: Číslo nula je dělitelné každým celým číslem; jediné celé číslo, které je dělitelné nulou, je nula; pro libovolné číslo $a$ platí $a \mid a$; pro libovolná čísla $a, b, c$ platí tyto čtyři implikace:

$$a \mid b \ \wedge \ b \mid c \implies a \mid c \tag{1}$$

$$a \mid b \ \wedge \ a \mid c \implies a \mid b + c \ \wedge \ a \mid b - c \tag{2}$$

$$c \neq 0 \implies (a \mid b \iff ac \mid bc) \tag{3}$$

$$a \mid b \ \wedge \ b > 0 \implies a \leq b \tag{4}$$

Příklad. Zjistěte, pro která přirozená čísla $n$ je číslo $n^2+1$ dělitelné číslem $n + 1$.

Řešení. Platí $n^2 - 1 = (n + 1)(n - 1)$, a tedy číslo $n + 1$ dělí číslo $n^2 - 1$. Předpokládejme, že $n + 1$ dělí i číslo $n^2 + 1$. Pak ovšem musí dělit i rozdíl $(n^2 + 1) - (n^2 - 1) = 2$. Protože $n \in \mathbb{N}$, platí $n + 1 \geq 2$, a tedy z $n + 1 \mid 2$ plyne $n + 1 = 2$, proto $n = 1$. Uvedenou vlastnost má tedy jediné přirozené číslo 1. □

Věta 1. *(Věta o dělení celých čísel se zbytkem) Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ tak, že $a = qm + r$.*

Důkaz. Dokažme nejprve existenci čísel $q, r$. Předpokládejme, že přirozené číslo $m$ je dáno pevně a dokažme úlohu pro libovolné $a \in \mathbb{Z}$. Nejprve budeme předpokládat, že $a \in \mathbb{N}_0$ a existenci čísel $q, r$ dokážeme indukcí:

Je-li $0 \le a < m$, stačí volit $q = 0$, $r = a$ a rovnost $a = qm + r$ platí.

Předpokládejme nyní, že $a \ge m$ a že jsme existenci čísel $q, r$ dokázali pro všechna $a' \in \{0, 1, 2, \ldots, a-1\}$. Speciálně pro $a' = a - m$ tedy existují $q', r'$ tak, že $a' = q'm + r'$ a přitom $r' \in \{0, 1, \ldots, m-1\}$. Zvolíme-li $q = q' + 1$, $r = r'$, platí $a = a' + m = (q' + 1)m + r' = qm + r$, což jsme chtěli dokázat.

Existenci čísel $q, r$ jsme tedy dokázali pro libovolné $a \ge 0$. Je-li naopak $a < 0$, pak ke kladnému číslu $-a$ podle výše dokázaného existují $q' \in \mathbb{Z}$, $r' \in \{0, 1, \ldots, m-1\}$ tak, že $-a = q'm + r'$, tedy $a = -q'm - r'$. Je-li $r' = 0$, položíme $r = 0$, $q = -q'$; je-li $r > 0$, položíme $r = m - r'$, $q = -q' - 1$. V obou případech $a = q \cdot m + r$, a tedy čísla $q, r$ s požadovanými vlastnostmi existují pro každé $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

Nyní dokážeme jednoznačnost. Předpokládejme, že pro některá čísla $q_1, q_2 \in \mathbb{Z}$; $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ platí $a = q_1 m + r_1 = q_2 m + r_2$. Úpravou dostaneme $r_1 - r_2 = (q_2 - q_1)m$, a tedy $m \mid r_1 - r_2$. Ovšem z $0 \le r_1 < m$, $0 \le r_2 < m$ plyne $-m < r_1 - r_2 < m$, odkud podle (4) platí $r_1 - r_2 = 0$. Pak ale i $(q_2 - q_1)m = 0$, a proto $q_1 = q_2$, $r_1 = r_2$. Čísla $q, r$ jsou tedy určena jednoznačně. Tím je důkaz ukončen. □

Číslo $q$, resp. $r$ z věty se nazývá *(neúplný) podíl*, resp. *zbytek* při dělení čísla $a$ číslem $m$ se zbytkem. Vhodnost obou názvů je zřejmá, přepíšeme-li rovnost $a = mq + r$ do tvaru

$$\frac{a}{m} = q + \frac{r}{m}, \quad \text{přitom} \quad 0 \le \frac{r}{m} < 1.$$

Je vhodné též si uvědomit, že z věty 1 plyne, že číslo $m$ dělí číslo $a$, právě když zbytek $r$ je roven nule.

Příklad. Dokažte, že jsou-li zbytky po dělení čísel $a, b \in \mathbb{Z}$ číslem $m \in \mathbb{N}$ jedna, je jedna i zbytek po dělení čísla $ab$ číslem $m$.

Řešení. Podle věty 1 existují $s, t \in \mathbb{Z}$ tak, že $a = sm+1$, $b = tm+1$. Vynásobením dostaneme vyjádření

$$ab = (sm+1)(tm+1) = (stm + s + t)m + 1 = qm + r,$$

kde $q = stm + s + t$, $r = 1$, které je podle věty 1 jednoznačné, a tedy zbytek po dělení čísla $ab$ číslem $m$ je jedna. □

SW ukázka. Vydělením čísla 1234567890 číslem 321 se zbytkem dostáváme 3846005, zbytek 285 - jak vidíme v PARI:

```
? divrem(1234567890,321)
%2 = [3846005, 285]~
```

nebo i jinak:

```
? 1234567890\321
%3 = 3846005
? 1234567890%321
%4 = 285
```

### 1.3. Největší společný dělitel a nejmenší společný násobek.

Definice. Mějme celá čísla $a_1, a_2$. Libovolné celé číslo $m$ takové, že $m \mid a_1$, $m \mid a_2$ (resp. $a_1 \mid m$, $a_2 \mid m$) se nazývá *společný dělitel* (resp. *společný násobek*) čísel $a_1, a_2$. Společný dělitel (resp. násobek) $m \geq 0$ čísel $a_1, a_2$, který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) čísel $a_1, a_2$, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel $a_1, a_2$ a značí se $(a_1, a_2)$ (resp. $[a_1, a_2]$).

Poznámka. Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{Z}$ platí $(a, b) = (b, a)$, $[a, b] = [b, a]$, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, $[a, 0] = 0$. Ještě však není jasné, zda pro každou dvojici $a, b \in \mathbb{Z}$ čísla $(a, b)$ a $[a, b]$ vůbec existují. Pokud však existují, jsou určena jednoznačně: Pro každá dvě čísla $m_1, m_2 \in \mathbb{N}_0$ totiž podle (4) platí, že pokud $m_1 \mid m_2$ a zároveň $m_2 \mid m_1$, je nutně $m_1 = m_2$. Důkaz existence čísla $(a, b)$ podáme (spolu s algoritmem jeho nalezení) ve větě 2, důkaz existence čísla $[a, b]$ a způsob jeho určení pak popíšeme ve větě 4.

Věta 2. *(Euklidův algoritmus) Nechť $a_1, a_2$ jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme $a_n$ zbytek po dělení čísla $a_{n-2}$ číslem $a_{n-1}$. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.*

Důkaz. Podle věty 1 platí $a_2 > a_3 > a_4 > \dots$. Protože jde o nezáporná celá čísla, je každé následující alespoň o 1 menší než předchozí, a proto po určitém konečném počtu kroků dostáváme $a_k = 0$, přičemž $a_{k-1} \neq 0$. Z definice čísel $a_n$ plyne, že existují celá čísla $q_1, q_2, \dots, q_{k-2}$ tak, že

$$\begin{aligned}
a_1 &= q_1 \cdot a_2 + a_3, \\
a_2 &= q_2 \cdot a_3 + a_4, \\
&\vdots \\
a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1} \\
a_{k-2} &= q_{k-2} \cdot a_{k-1}.
\end{aligned} \tag{5}$$

Z poslední rovnosti plyne, že $a_{k-1} \mid a_{k-2}$, z předposlední, že $a_{k-1} \mid a_{k-3}$, atd., až nakonec ze druhé $a_{k-1} \mid a_2$ a z první dostaneme $a_{k-1} \mid a_1$. Je tedy $a_{k-1}$ společný dělitel čísel $a_1, a_2$. Naopak jejich libovolný společný dělitel dělí i číslo $a_3 = a_1 - q_1a_2$, proto i $a_4 = a_2 - q_2a_3, \ldots,$ a proto i $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$. Dokázali jsme, že $a_{k-1}$ je největší dělitel čísel $a_1, a_2$. □

Poznámka. Z poznámky za definicí, z věty 2 a z toho, že pro libovolná $a, b \in \mathbb{Z}$ platí $(a, b) = (a, -b) = (-a, b) = (-a, -b)$ plyne, že existuje největší společný dělitel libovolných dvou celých čísel. Navíc dostáváme z Euklidova algoritmu i následující zajímavé a často využívané tvrzení.

Věta 3. *(Bezoutova) Pro libovolná celá čísla $a, b$ existují celá čísla $k, l$ tak, že $(a, b) = ka + lb$.*

Důkaz. Jistě stačí větu dokázat pro $a, b \in \mathbb{N}$. Všimněme si, že jestliže je možné nějaká čísla $r, s \in \mathbb{Z}$ vyjádřit ve tvaru $r = r_1a + r_2b$, $s = s_1a + s_2b$, kde $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, můžeme tak vyjádřit i

$$r + s = (r_1 + s_1)a + (r_2 + s_2)b$$

a také

$$c \cdot r = (c \cdot r_1)a + (c \cdot r_2)b$$

pro libovolné $c \in \mathbb{Z}$. Z Euklidova algoritmu (pro $a_1 = a, a_2 = b$) plyne, že takto můžeme vyjádřit i $a_3 = a_1 - q_1a_2$, $a_4 = a_2 - q_2a_3, \ldots,$ a tedy i číslo $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, což je ovšem $(a_1, a_2)$.

Zdůrazněme přitom, že hledaná čísla $k, l$ zdaleka nejsou určena jednoznačně. □

SW ukázka. Výpočet největšího společného dělitele pomocí Euklidova algoritmu je s využitím výpočetní techniky i pro relativně velká čísla poměrně rychlý. V našem příkladu to vyzkoušíme na 2 číslech A,B, z nichž každé je součinem dvou 101-ciferných prvočísel. Všimněme si, že výpočet největšího společného dělitele i takto velkých čísel trval zanedbatelný čas. Pozorovatelem zaznamenatelný čas zabere tento výpočet až ve druhé ukázce, v níž jsou vstupem dvě čísla mající více než milion cifer.

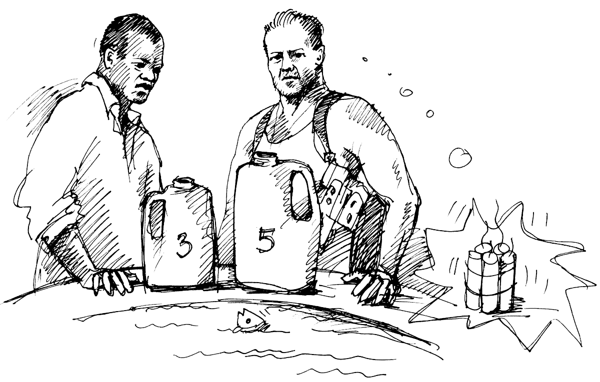
```
sage: p=next_prime(5*10^100)
sage: q=next_prime(3*10^100)
sage: r=next_prime(10^100)
sage: A=p*q;B=q*r;
sage: time G=gcd(A,B); print G

Time: CPU 0.00 s, Wall: 0.00 s
3000000000000000000000000000000000\
0000000000000000000000000000000000\
000000000000000000000000000223

time G=gcd(A^10000+1,B^10000+1);
Time: CPU 2.47 s, Wall: 2.48 s
```

Poznámka. Euklidův algoritmus a Bezoutova věta jsou jedny z nejdůležitějších výsledků elementární teorie čísel a tvoří jeden ze základních pilířů algoritmů algebry a teorie čísel.

*To, že znalost těchto základů je občas důležitá i v praktickém životě, dokazuje Bruce Willis a Samuel Jackson ve filmu Smrtonosná past 3, kde mají za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů. Zde stačí s využitím Euklidova algoritmu najít celá čísla $k, l$ tak, že bude platit $3k + 5l = 4$.*
*Netroufám si tvrdit, že zmínění herci ovládají uvedené základy teorie čísel (tuto konkrétní úlohu jistě snadno vyřešíte experimentálně), nicméně předchozí věty dávají návod, jak vyřešit úlohu tohoto typu s libovolnými zadanými parametry, což podrobně rozebereme v části o diofantických rovnicích.*




Věta 4. *Pro libovolná celá čísla $a_1, a_2$ existuje jejich nejmenší společný násobek $[a_1, a_2]$ a platí $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.*

Důkaz. Věta jistě platí, je-li některé z čísel $a_1, a_2$ rovno nule. Můžeme navíc předpokládat, že obě nenulová čísla $a_1, a_2$ jsou kladná, neboť jejich znaménka se v dokazovaném vzorci neprojeví. Budeme hotovi, ukážeme-li, že $q = a_1 \cdot a_2/(a_1, a_2)$ je nejmenší společný násobek čísel $a_1, a_2$. Protože $(a_1, a_2)$ je společný dělitel čísel $a_1, a_2$, jsou $a_1/(a_1, a_2)$ i $a_2/(a_1, a_2)$ celá čísla, a proto

$$q = \frac{a_1 a_2}{(a_1, a_2)} = \frac{a_1}{(a_1, a_2)} \cdot a_2 = \frac{a_2}{(a_1, a_2)} \cdot a_1$$

je společný násobek čísel $a_1, a_2$. Podle Bezoutovy věty 3 existují $k_1, k_2 \in \mathbb{Z}$ tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$. Předpokládejme, že $n \in \mathbb{Z}$ je libovolný společný násobek čísel $a_1, a_2$ a ukážeme, že je dělitelný číslem $q$. Je tedy $n/a_1, n/a_2 \in \mathbb{Z}$, a proto je i celé číslo

$$\frac{n}{a_2} \cdot k_1 + \frac{n}{a_1} \cdot k_2 = \frac{n(k_1 a_1 + k_2 a_2)}{a_1 a_2} = \frac{n(a_1, a_2)}{a_1 a_2} = \frac{n}{q}.$$

To ovšem znamená, že $q \mid n$, což jsme chtěli dokázat. □

### 1.4. Dělitelé a násobky mnoha čísel.

Definice. Největší společný dělitel a nejmenší společný násobek $n$ čísel
$a_1, a_2, \ldots, a_n \in \mathbb{Z}$ definujeme analogicky jako v 1.3. Libovolné $m \in \mathbb{Z}$ takové, že $m \mid a_1$, $m \mid a_2$, …, $m \mid a_n$ (resp. $a_1 \mid m$, $a_2 \mid m$, …, $a_n \mid m$) se nazývá *společný dělitel* (resp. *společný násobek*) čísel $a_1, a_2, \ldots, a_n$. Společný dělitel (resp. násobek) $m \geq 0$ čísel $a_1, a_2, \ldots, a_n$, který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) těchto čísel, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel $a_1, a_2, \ldots, a_n$ a značí se $(a_1, a_2, \ldots, a_n)$ (resp. $[a_1, a_2, \ldots, a_n]$).

Snadno se přesvědčíme, že platí

$$(a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n), \tag{6}$$
$$[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]. \tag{7}$$

Největší společný dělitel $(a_1, \ldots, a_n)$ totiž dělí všechna čísla $a_1, \ldots, a_n$, a tedy je společným dělitelem čísel $a_1, \ldots, a_{n-1}$, a proto dělí i největšího společného dělitele $(a_1, \ldots, a_{n-1})$, tj. $(a_1, \ldots, a_n) \mid ((a_1, \ldots, a_{n-1}), a_n)$. Naopak největší společný dělitel čísel $(a_1, \ldots, a_{n-1}), a_n$ musí kromě čísla $a_n$ dělit i všechna čísla $a_1, \ldots, a_{n-1}$, protože dělí jejich největšího společného dělitele, a proto $((a_1, \ldots, a_{n-1}), a_n) \mid (a_1, \ldots, a_n)$. Dohromady dostáváme rovnost (6) a zcela analogicky se dokáže (7).

Pomocí (6) a (7) snadno dokážeme existenci největšího společného dělitele i nejmenšího společného násobku libovolných $n$ čísel indukcí vzhledem k $n$: pro $n = 2$ je jejich existence dána větami 2 a 4, jestliže pro některé $n > 2$ víme, že existuje největší společný dělitel i nejměnší společný násobek libovolných $n - 1$ čísel, podle (6) a (7) existuje i pro libovolných $n$ čísel.

### 1.5. Nesoudělnost.

Definice. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže pro ně platí $(a_1, a_2, \ldots, a_n) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé $i, j$ takové, že $1 \leq i < j \leq n$, platí $(a_i, a_j) = 1$.

Poznámka. V případě $n = 2$ oba pojmy splývají, pro $n > 2$ plyne z nesoudělnosti po dvou nesoudělnost, ne však naopak: například čísla 6, 10, 15 jsou nesoudělná, ale nejsou nesoudělná po dvou, neboť dokonce žádná dvojice z nich vybraná nesoudělná není: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

Příklad. Nalezněte největší společný dělitel čísel $2^{63} - 1$ a $2^{91} - 1$.

Řešení. Užijeme Euklidův algoritmus. Platí

$$\begin{aligned} 2^{91}-1 &= 2^{28}(2^{63}-1)+2^{28}-1,\\ 2^{63}-1 &= (2^{35}+2^{7})(2^{28}-1)+2^{7}-1,\\ 2^{28}-1 &= (2^{21}+2^{14}+2^{7}+1)(2^{7}-1). \end{aligned}$$

Hledaný největší společný dělitel je tedy $2^7-1=127$. □

Věta 5. *Pro libovolná přirozená čísla $a, b, c$ platí*

*(1)* $(ac, bc) = (a, b)\cdot c$,
*(2) jestliže* $a \mid bc$ *a* $(a, b) = 1$, *pak* $a \mid c$,
*(3)* $d = (a, b)$ *právě tehdy, když existují* $q_1, q_2 \in \mathbb{N}$ *tak, že* $a = dq_1$, $b = dq_2$ *a* $(q_1, q_2) = 1$.

Důkaz. ad 1. Protože $(a, b)$ je společný dělitel čísel $a, b$, je $(a, b)\cdot c$ společný dělitel čísel $ac$, $bc$, proto $(a, b)\cdot c \mid (ac, bc)$. Podle věty 3 existují $k, l \in \mathbb{Z}$ tak, že $(a, b) = ka + lb$. Protože $(ac, bc)$ je společný dělitel čísel $ac$, $bc$, dělí i číslo $kac + lbc = (a, b)\cdot c$. Dokázali jsme, že $(a, b)\cdot c$ a $(ac, bc)$ jsou dvě přirozená čísla, která dělí jedno druhé, proto se podle (4) rovnají.

ad 2. Předpokládejme, že $(a, b) = 1$ a $a \mid bc$. Podle Bezoutovy věty (věta 3) existují $k, l \in \mathbb{Z}$ tak, že $ka + lb = 1$, odkud plyne, že $c = c(ka + lb) = kca + lbc$. Protože $a \mid bc$, plyne odsud, že i $a \mid c$.

ad 3. Nechť $d = (a, b)$, pak existují $q_1, q_2 \in \mathbb{N}$ tak, že $a = dq_1$, $b = dq_2$. Pak podle části (1) platí $d = (a, b) = (dq_1, dq_2) = d\cdot(q_1, q_2)$, a tedy $(q_1, q_2) = 1$. Naopak, je-li $a = dq_1$, $b = dq_2$ a $(q_1, q_2) = 1$, pak $(a, b) = (dq_1, dq_2) = d(q_1, q_2) = d\cdot 1 = d$ (opět užitím 1. části tohoto tvrzení). □