Diskrétní matematika – 1. týden
Elementární teorie čísel – dělitelnost

Jan Slovák

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant **Matematika drsně a svižně**, *e*-text na `www.math.muni.cz/Matematika_drsne_svizne`.
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2012/M6520/um/main-print.pdf`
- Jiří Herman, Radan Kučera, Jaromír Šimša, **Metody řešení matematických úloh**. MU Brno, 2001.
- William Stein, **Elementary Number Theory: Primes, Congruences, and Secrets**, Springer, 2008. Dostupné na `http://wstein.org/ent/ent.pdf`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

V několika přednáškách se teď budeme zabývat úlohami o celých číslech. Převážně v nich půjde o dělitelnost celých čísel, popřípadě o řešení rovnic v oboru celých nebo přirozených čísel. Ačkoli jsou přirozená a konec konců i celá čísla v jistém smyslu nejjednodušší matematickou strukturou, zkoumání jejich vlastností postavilo před generace matematiků celou řadu velice obtížných problémů. Často jsou to problémy, které je možno snadno formulovat, přesto však dodnes neznáme jejich řešení.

God made integers, all else is the work of man. (L. Kronecker)

Notorické problémy teorie čísel

Uveďme některé z nejznámějších:

- *problém prvočíselných dvojčat* – rozhodnout, zda existuje nekonečně mnoho prvočísel p takových, že i $p + 2$ je prvočíslo,
- *problém existence lichého dokonalého čísla* – tj. čísla jehož součet dělitelů je roven dvojnásobku tohoto čísla
- *Goldbachovu hypotézu* (rozhodnout, zda každé sudé číslo větší než 2 je možno psát jako součet dvou prvočísel),
- nebo klenot mezi problémy teorie čísel *velkou Fermatovu větu* (Fermat's Last Theorem) – rozhodnout, zda existují přirozená čísla n, x, y, z tak, že $n > 2$ a platí $x^n + y^n = z^n$; Pierre de Fermat jej formuloval cca 1637, vyřešil Andrew Wiles v roce 1995.

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 : 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:

$$\begin{aligned} a \mid b \ \wedge \ b \mid c &\implies a \mid c \\ a \mid b \ \wedge \ a \mid c &\implies a \mid b + c \ \wedge \ a \mid b - c \\ c \neq 0 &\implies (a \mid b \iff ac \mid bc) \\ a \mid b \ \wedge \ b > 0 &\implies a \leq b \end{aligned}$$

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. □

Dělení se zbytkem

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 $0 \leq a < m$, stačí volit $q = 0$, $r = a$ a rovnost $a = qm + r$ platí. Předpokládejme nyní, že $a \geq m$ 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. □

Dokončení důkazu.

Existenci čísel q, r jsme tedy dokázali pro libovolné $a \geq 0$. 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 $0 \leq r_1 < m$, $0 \leq r_2 < m$ plyne $-m < r_1 - r_2 < m$, odkud dostáváme $r_1 - r_2 = 0$. 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. □

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

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

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 o dělení se zbytkem existují $s, t \in \mathbb{Z}$ tak, že $a = sm + 1$, $b = tm + 1$. Vynásobením dostaneme

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

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

Největší společný dělitel (gcd)

Jedním z nejdůležitějších nástrojů výpočetní teorie čísel je výpočet největšího společného dělitele. Protože jde, jak si ukážeme, o relativně rychlou proceduru, je i v moderních algoritmech velmi často využívána.

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 $(a, b) = (b, a)$, $[a, b] = [b, a]$, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, $[a, 0] = 0$.

Poznámka

Analogicky se definuje i největší společný dělitel a nejmenší společný násobek více než dvou celých čísel a snadno se následně dokáže, že platí

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

Euklidův algoritmus

Dosud jsme nijak nezdůvodnili, 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 definice 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) v následující větě, důkaz existence čísla $[a, b]$ pak dostaneme snadno ze vztahu mezi (a, b) a $[a, b]$.

Věta (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 o dělení se zbytkem 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

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

Z poslední rovnosti plyne, že $a_{k-1} \mid a_{k-2}$, dále $a_{k-1} \mid a_{k-3}$, atd., je tedy a_{k-1} společný dělitel čísel a_1, a_2. Naopak jejich libovolný společný dělitel dělí i číslo $a_3 = a_1 - q_1 a_2$, proto i $a_4 = a_2 - q_2 a_3, \dots$, a proto i $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$. Dokázali jsme, že a_{k-1} je největší společný dělitel čísel a_1, a_2. □

Vlastnosti gcd

Poznámka

Z definice, z předchozího tvrzení 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.

Věta (Bezoutova)

Pro libovolná celá čísla a_1, a_2 existuje jejich největší společný dělitel (a_1, a_2), přitom existují celá čísla k_1, k_2 tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$.

Důkaz.

Jistě stačí větu dokázat pro $a_1, a_2 \in \mathbb{N}$. Všimněme si, že jestliže je možné nějaká čísla $r, s \in \mathbb{Z}$ vyjádřit ve tvaru $r = r_1 a_1 + r_2 a_2$, $s = s_1 a_1 + s_2 a_2$, kde $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, můžeme tak vyjádřit i

$$r + s = (r_1 + s_1)a_1 + (r_2 + s_2)a_2$$

a také

$$c \cdot r = (c \cdot r_1)a_1 + (c \cdot r_2)a_2$$

pro libovolné $c \in \mathbb{Z}$. Protože $a_1 = 1 \cdot a_1 + 0 \cdot a_2$, $a_2 = 0 \cdot a_1 + 1 \cdot a_2$, plyne z (5), že takto můžeme vyjádřit i $a_3 = a_1 - q_1 a_2$, $a_4 = a_2 - q_2 a_3$, $\ldots$, $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$, což je ovšem (a_1, a_2). □

Příklad

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.
Příklad v systému SAGE je dostupný na
`https://sage.math.muni.cz/home/pub/6/`.

Poznámka

Euklidův algoritmus a Bezoutova věta jsou základními výsledky elementární teorie čísel a tvoří jeden z 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.

Nejmenší společný násobek

Věta

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. □

Dokončení.

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 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. □

Nesoudělnost

Definice

Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže 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: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

Věta

Pro libovolná přirozená čísla a, b, c *platí*

1. $(ac, bc) = (a, b) \cdot c$,
2. *jestliže* $a \mid bc$, $(a, b) = 1$, *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 Bezoutovy věty 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 rovnají.

ad 2. Předpokládejme, že $(a, b) = 1$ a $a \mid bc$. Podle Bezoutovy věty 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 1. části 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). □