MB141 – 10. přednáška
Celá čísla a dělitelnost

Martin Čadek
s využitím přednášek pro předmět MB104

Jarní semestr 2021

Doporučené zdroje k teorii čísel

- 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/podzim2019/M6520/um/main-print.pdf`
- 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/ATC2014.pdf`
- Adam Spencer, **Why I fell in love with monster prime numbers**, video, 17 minut, `https://www.ted.com/talks/adam_spencer_why_i_fell_in_love_with_monster_prime_numbers`

Osnova 10. přednášky

- Dělitelnost a dělení se zbytkem
- Největší společný dělitel, Eukleidův algoritmus
- Bezoutova věta
- Nesoudělnost
- Prvočísla, rozklad čísel na prvočísla

Problémy teorie čísel

Přirozená a celá čísla jsou nejjednodušší matematickou strukturou, zkoumání jejich vlastností však postavilo před generace matematiků celou řadu velice obtížných problémů.

Často jsou to problémy, které je možno snadno formulovat, přesto však dodnes neznáme jejich řešení.

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.

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

Příklady problémů teorie čísel

- *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
- *Goldbachova hypotéza* (rozhodnout, zda každé sudé číslo větší než 2 je možno psát jako součet dvou prvočísel),
- *velká Fermatova věta* (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.

Diofantické rovnice

V kouzelném měšci máme neomezené množství dvoukorun a pětikorun. Jaké částky můžeme zaplatit tak, aby nebylo potřeba vracet?

Ptáme se tedy, pro která přirozená čísla n existují přirozená k, ℓ tak, aby

$$2k + 5\ell = n.$$

Asi se dá vcelku snadno uvěřit, že libovolnou vyšší částku takto zaplatíme, po pravdě jakoukoliv častku s výjimkou 1 Kč a 3 Kč. S vracením pak zvládneme zaplatit libovolnou částku, tj. každé n lze vyjádřit jako

$$2k + 5\ell = n$$

pro nějaká celá k, ℓ.
Umíme to pro jakékoliv hodnoty mincí? Jak by to dopadlo třeba pro $7k + 11\ell = n$? A jak pro $2k + 4\ell = n$?

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 : 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:

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

Příklady

Příklad

Zjistěte, pro která přirozená čísla n je číslo $n^2 + 1$ dělitelné číslem 3.

Uvidí se, že záleží pouze na zbytku n po dělení třemi.

Příklad

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

$n = 3k + z \qquad z = 0, 1, 2$

$n^2 + 1 = (3k + z)^2 + 1 = \underbrace{8k^2 + 6kz}_{\text{si divide per } 3} + z^2 + 1$

$3 \mid n^2 + 1 \iff 3 \mid z^2 + 1$

$z = 0 \qquad z^2 + 1 = 1$

$z = 1 \qquad z^2 + 1 = 2$

$z = 2 \qquad z^2 + 1 = 4 + 1 = 5$

$3 \nmid 1, 2$ ami $5 \qquad 3 \nmid n^2 + 1$

Pro které n $\quad n-1 \mid n^2+1$.

$$(n-1)(n+1) = n^2 - 1$$

$$n^2+1 = (n-1)(n+1) + 2$$

$$n-1 \mid n^2+1 \iff n-1 \mid 2$$

dělitele 2 $\quad$ 1 $\quad$ 2

$n-1 = 1$ nebo 2

$n = 2$ nebo 3

Dělení se zbytkem

$\mathbb{Z}$ celá čísla

$\mathbb{N}$ přirozená čísla

$\mathbb{N} = \{1, 2, 3, \dots\}$

Věta (o dělení celých čísel se zbytkem)

Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \dots, m-1\}$ tak, že $a = qm + r$.

Důkaz indukcí: pro $a < m$ zřejmé, pro $a \geq m$ pak rekurzivně s využitím výsledku pro $a - m$ (podíl je potřeba zvětšit o 1, zbytek zůstane stejný).

$a \geq 0$

$a = 0 \cdot m + a$

a

$a - m < a$

$a - m = q_1 m + r$

$a = (q_1 + 1) m + r$

Dělení se zbytkem – pokračování

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

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

$a = mq + r \,/ : m$

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.

$a = k \cdot m + 1 \qquad b = l \cdot m + 1$

$a \cdot b = (k \cdot m + 1)(l \cdot m + 1) = klm^2 + (k+l)m + 1$

$= (klm + k + l)m + 1$

Největší společný dělitel (gcd)

gcd greatest common divisor

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 $m \mid a_1$, $m \mid a_2$ se nazývá *společný dělitel* čísel a_1, a_2. Společný dělitel $m \geq 0$ čísel a_1, a_2, který je dělitelný libovolným společným dělitelem čísel a_1, a_2, se nazývá *největší společný dělitel* čísel a_1, a_2 a značí se (a_1, a_2).

Například $(12, 64) = 4$.

dělitelé 12 1, 2, 3, 4, 6, 12

64 1, 2, 4, 8, 16, 32, 64

Společní dělitelé 1, 2, 4,

Největší společný dělitel je 4.

Rozklad na prvočísla

$12 = 2^2 \cdot 3$

$64 = 2^6$

$(12, 64) = 2^2$ ALE

Najít rozklad na prvočísla každého!

Nejmenší společný násobek

Definice

Mějme celá čísla a_1, a_2. Libovolné celé číslo m takové, že $a_1 \mid m$, $a_2 \mid m$ se nazývá *společný násobek* čísel a_1, a_2. Společný násobek $m \geq 0$ čísel a_1, a_2, který dělí libovolný společný násobek čísel a_1, a_2, se nazývá *nejmenší společný násobek* čísel a_1, a_2 a značí se $[a_1, a_2]$.

Poznámka

Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{Z}$ platí $(a, b) = (b, a)$, $[a, b] = [b, a]$, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, $[a, 0] = 0$. 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. To si lze hezky představit přes rozklad na prvočinitele, ale ten je výpočetně velmi náročný (RSA) a navíc k jeho odvození budeme existenci největšího společného dělitele využívat.
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.

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 $a_{k-1} = (a_1, a_2)$.

$$a_1 = q_1 a_2 + a_3 \qquad a_3 \in [0, a_2 - 1]$$

$$a_2 = q_2 a_3 + a_4 \qquad a_4 \in [0, a_3 - 1]$$

$$\vdots$$

$$a_{k-3} = q_{k-3} a_{k-2} + a_{k-1}$$

$$a_{k-2} = q_{k-2} a_{k-1} + a_k \qquad \boxed{a_k = 0}$$

a_{k-1} je Největší spol. dělitel čísel (a_1, a_2)

$$a_{k-1} = (a_1, a_2)$$

a_{k-1} dělí obě čísla a_1, a_2

$$a_{k-2} = q_{k-2}\, a_{k-1}$$

$$\Rightarrow a_{k-1} \mid a_{k-2}$$

$$a_{k-3} = \underbrace{q_{k-3}\, a_{k-2}}_{\text{je dělitelné } a_{k-1}} + a_{k-1}$$

$$\Rightarrow a_{k-1} \mid a_{k-3} \Rightarrow \text{atd. } a_{k-1} \mid a_2,\ a_{k-1} \mid a_1.$$

(1) a_{k-1} je společný dělitel čísel a_1, a_2.

(2) Jestliže $d \mid a_1$, $d \mid a_2 \Rightarrow d \mid a_{k-1}$

$$a_1 = q_1 a_2 + a_3 \Rightarrow d \mid a_3$$

$a_1 = 10\,175$, $a_2 = 2277$

$$10175 = 4 \cdot 2277 + 1067$$
$$2277 = 2 \cdot 1067 + 143$$
$$1067 = 7 \cdot 143 + 66$$
$$143 = 2 \cdot 66 + \boxed{11}$$
$$66 = 6 \cdot 11 + 0$$

nejsedí vpd. dělitel

$$a_2 = q_2 a_3 + a_4$$

$d \mid a_2, \; d \mid a_3 \Rightarrow d \mid a_4$

$d \mid a \;\; d \mid a_{k-1}$

$\Rightarrow \quad a_{k-1} = (a_1, a_2)$

Da'le

$$a_{k-1} = (a_{k-2}, a_{k-1}) = (a_{k-3}, a_{k-2})$$

$$= \cdots = (a_1, a_2)$$

Euklidův algoritmus – příklad

Algoritmus a důkaz jeho korektnosti demonstrujeme na příkladu:

Příklad

Určete největšího společného dělitele čísel 10175 a 2277.

Vlastnosti největšího společného dělitele

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 $(a_1, a_2) = k_1 a_1 + k_2 a_2$.

Důsledek

Pro libovolná celá čísla a_1, a_2 lze jako celočíselné kombinace $n = k_1 a_1 + k_2 a_2$ vyjádřit právě násobky největšího společného dělitele (a_1, a_2).

Ukázat praktický výpočet pro $a_1 = 10175$, $a_2 = 2277$.

$$\{ k a_1 + \ell a_2, \quad k, \ell \in \mathbb{Z} \}$$

$$= \{ p \cdot d, \ p \in \mathbb{Z} \}$$

$$d = (a_1, a_2) \qquad (7, 11) = 1$$

$d \mid a_1, a_2 \Rightarrow d \mid k a_1 + \ell a_2$

$\subseteq$ $\{7k + 11\ell\} = \mathbb{Z}$

$d = k_1 a_1 + \ell_1 a_2 \Rightarrow$

$d \in \{ k a_1 + \ell a_2, \ k, \ell \in \mathbb{Z} \}$

$\Rightarrow pd \in \{ \quad \} \supseteq$

Dělání Ber. věty

$a_1 = q_1 a_2 + a_3$

$a_2 = q_2 a_3 + a_4$

$a_{k-4} = q_{k-4} a_{k-3} + a_{k-2}$

$a_{k-3} = q_{k-3} a_{k-2} + a_{k-1}$

$a_{k-2} = q_{k-2} a_{k-1} + 0$

$a_{k-1} = a_{k-3} - q_{k-3} a_{k-2} =$

$= a_{k-3} - q_{k-3} (a_{k-4} - q_{k-4} a_{k-3})$

$= (1 + q_{k-4}) a_{k-3} - q_{k-3} a_{k-4}$

$\text{add} = k a_2 + l a_1 .$

Praktický způsob NSD čísel k, l

$k \cdot 10175$	$l \cdot 2277$	$k \cdot a_1 + l a_2$
1	0	10175
0	1	2277
1	−4	$1 \cdot 10175 - 4 \cdot 2277 = 1067$ •
−2	9	143 ••
15	−67	66 •
w	−32	143	11 •
$\log_2 w$			

$$(-32) \cdot 10175 + (143) \cdot 2277 = 11$$

Příklad

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` lze vyzkoušet na `https://cocalc.com/`.

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

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.

Nejlépe se vidí přes rozklad na součin prvočísel. □

$a_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$

$a_2 = p_1^{\beta_1} p_2^{\beta_2}$

$(a_1, a_2) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots$

$$[a_1, a_2] = p_1^{\max(\alpha_1, \beta_1)} \; p_2^{\max(\alpha_2, \beta_2)} \cdots .$$

$$(a_1, a_2)\,[a_1, a_2] = p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2}$$

$$= a_1 \cdot a_2$$

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 $(a_i, a_j) = 1$.

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: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

$(6,10) = 2 \quad (6,15) = 3, \quad (10,15) = 5$

$(6,10,15) = 1$

Nesoudělnost – důležité vlastnosti

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* $(q_1, q_2) = 1$.

$a \mid bc \;\wedge\; (a, b) = 1 \Rightarrow a \mid c$

$a \mid bc \wedge (a,b) = 1$

$1 = ak + bl \qquad / \cdot c$

$c = akc + blc$

$a \mid akc \wedge a \mid bcl$

$\Rightarrow \quad a \mid akc + bcl = c.$

Prvočísla

Prvočíslo je jeden z nejdůležitějších pojmů elementární teorie čísel. Jeho důležitost je dána především větou o jednoznačném rozkladu libovolného přirozeného čísla na součin prvočísel, která je silným a účinným nástrojem při řešení celé řady úloh z teorie čísel.

Definice

Každé přirozené číslo $n \geq 2$ má aspoň dva kladné dělitele: 1 a n. Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se *prvočíslo*. V opačném případě hovoříme o *složeném čísle*.

V dalším textu budeme zpravidla prvočíslo značit písmenem p. Nejmenší prvočísla jsou 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... (zejména číslo 1 za prvočíslo ani za číslo složené nepovažujeme). Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem (největší známé prvočíslo $2^{82\,589\,933} - 1$ má pouze 24 862 048 cifer).

Dk Euklidovy věty

p prvočíslo $\Leftrightarrow$ $p \mid ab \Rightarrow p \mid a$ nebo $p \mid b$

$\Rightarrow$ Nechť p je prvočíslo

$p \mid ab$ a p nedělí a

$$(p, a) = 1$$

$$kp + la = 1 \qquad / \cdot b$$

$$kpb + lab = b$$

$$p \mid kpb \wedge p \mid lab \Rightarrow p \mid b$$

$\Leftarrow$ Chceme dk že p je prvočíslo

Poichè $p = ab$ dicemo che, o è

$a = 1$ e $b = p$

oppure

$a = p$ e $b = 1$

$p = ab \Rightarrow p \mid ab \Rightarrow$

$1 \le a \le p$

$1 \le b \le p$

$p \mid a$

$\Downarrow$

$p = a$

$b = 1$

oppure

$p \mid b$

$\Downarrow$

$p = b$

$a = 1$

Prvočísel je nekonečně mnoho.

Nejdříve je potřeba rozklad na prvočísla.

$p = 2 \cdot 3 = 6$ není prvočíslo

$p \mid 2^2 \cdot 3^2 = 36$

~~$\Rightarrow$~~ $p \mid 2^2$ nebo $p \mid 3^2$

$\overline{p}$ je prvočíslo

$p \mid ab \Rightarrow p \mid a$ nebo $p \mid b$

Základní věta aritmetiky

Uveďme nyní větu, která udává ekvivalentní podmínku prvočíselnosti a je základní ingrediencí při důkazu jednoznačnosti rozkladu na prvočísla.

Věta (Eukleidova o prvočíslech)

Přirozené číslo $p \geq 2$ je prvočíslo, právě když platí: pro každá celá čísla a, b z $p \mid ab$ plyne $p \mid a$ nebo $p \mid b$.

Věta

Libovolné přirozené číslo $n \geq 2$ je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li n prvočíslo, pak jde o „součin“ jednoho prvočísla.)

Indukcí Každé n je součin prvočísel.

Pro $n = 2$ platí.

Nechť platí pro čísla $\leq n-1$.

n dělitele 1) $1, n$ n je prvočíslo

2) $\exists$ dělitel $1 < a < n$

$n = a \cdot b$, a i b lze psát jako součin prvočísel, tedy i n je součin prvočísel.

Jednoznačnost

$\alpha_i + \beta_i > 0$

$\alpha_i \geq 0$

$\beta_i \geq 0$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$= p_1^{\beta_1} p_2^{\beta_2} \cdots .$$

Kdyby $\beta^1 > \alpha_1$

$$a = \frac{n}{p_1^{\alpha_1}} = \frac{p_2^{\alpha_2} \cdots}{} \qquad \beta_1 - \alpha_1 > 0$$

$$= \frac{p_1^{\beta_1 - \alpha_1} p_2^{\alpha_2} \cdots}{}$$

$p_1 / a \Rightarrow p_1 / p_2^{\alpha_2}$ nebo $p_1 / p_3^{\alpha_3} \cdots$ spor.

Prvočísel je nekonečně mnoho.

Sepišme všechna prvočísla jsou

$p_1, p_2, \ldots, p_N$

$a = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$

a není prvočíslo $\neq p_1, p_2, \ldots, p_N$

ale a má rozklad na prvočísla

$\exists p_i \quad p_i \mid a$, ale p_1 to není, p_2 to není, atd., spor.