Organizační záležitosti

Výuka: pouze distanční

- přednášky zatím neplánuji online (tj. s vaší účastí)
- cvičení v režii cvičících

Podmínka pro připuštění ke zkoušce:

alespoň 15b ze 40b ze semestru

20b: 13 x DÚ po 2b., nejhorší tři se nesčítají

20b: písemka v polovině semestru

→ dvě písemky po 10b lepší – email

Organizační záležitosti

Hodnocení: práce v semestru max 40b } max
závěrečná písemka max 60b } 100b

Známky:
F: [0, 50)
E: [50, 60)
D: [60, 68)
C: [68, 76)
B: [76, 84)
A: [84, 100]

bude obsahovat i nějakou teorii (cca 20b z 60b)

Diskrétní matematika – 1. týden
Elementární teorie čísel – dělitelnost

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

jaro 2020

Obsah přednášky

1. Problémy teorie čísel
2. Dělitelnost
3. Společní dělitelé a společné násobky
4. Prvočísla

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant **Matematika drsně a svižně**, *e*-text na `www.math.muni.cz/Matematika_drsne_svizne`.

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/podzim2019/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/ATC2014.pdf`

Plán přednášky

1. Problémy teorie čísel
2. Dělitelnost
3. Společní dělitelé a společné násobky
4. Prvočísla

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,

$3, 5 \quad 5, 7 \quad 11, 13 \quad 17, 19 \ldots$

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

$6 = 1+2+3$ $28 = 1+2+4+7+14$

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),

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.

$n = 2$: $3^2 + 4^2 = 5^2$

diofantické rovnice

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

diofantické rovnice

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

celé nezáporné

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.

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

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

$n \geq (2-1)(5-1)$
lze

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

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

$2 \cdot (-2) + 5 \cdot 1 = 1$

$\Rightarrow 2 \cdot (-2n) + 5 \cdot n = n$

pro nějaká celá k, ℓ.

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

vše ne, pouze sudé čísla

Plán přednášky

1 Problémy teorie čísel

2 Dělitelnost

3 Společní dělitelé a společné násobky

4 Prvočísla

Základní: existence rozkladu na součin prvočísel, jednoznačný (až na pořadí)

Důkaz???

existence - jasná

jednoznačnost: $2 \cdot 3 \neq 5 \cdot 7$

LHS dělitelná 2, tj. sudá

$\Rightarrow$ RHS součin $\Rightarrow$ alespoň 1 číslo sudé $\Rightarrow$ je to 2

$\Rightarrow$ celé vydělíme 2 a použijeme indukci / rekurzi

to samé s $p=3$

Vlastnost: prvočísel
$p \mid a \cdot b$
$\Rightarrow p \mid a$
nebo $p \mid b$

$3 \cdot 7 \neq a \cdot b$

LHS dělitelná 3

$\Rightarrow$ jedno z čísel ab napravo je 3

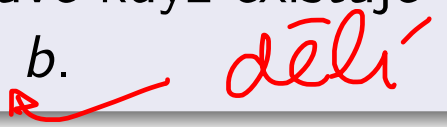
4 možnosti:

a dává zb.	1	po dělení 3
	1	3
b		
$\Rightarrow a \cdot b$	1	

kde $a \neq 3$, $b \neq 3$

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 $a \mid b$.



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 $a \mid b$.

$a \cdot 0 = 0$ $\quad 0 \cdot c = 0$ $\quad a \cdot 1 = a$

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 $a \mid a$;

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 $a \mid b$.

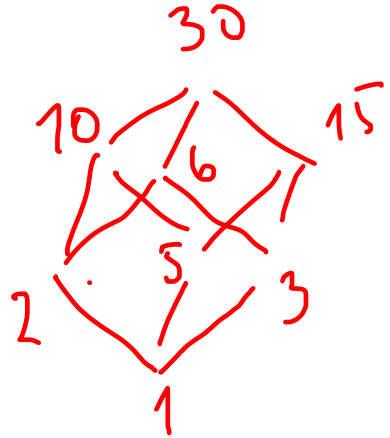
Přímo z definice plyne několik jednoduchých tvrzení : Číslo nula je dělitelné každým celým číslem; jediné celé číslo, které je dělitelné nulou, je nula; pro libovolné číslo a platí $a \mid a$; pro libovolná čísla a, b, c platí tyto čtyři implikace:

$$a \mid b \ \wedge \ b \mid c \implies a \mid c$$

$$a \mid b \ \wedge \ a \mid c \implies a \mid b + c \ \wedge \ a \mid b - c$$

$$c \neq 0 \implies (a \mid b \iff ac \mid bc)$$

$$a \mid b \ \wedge \ b > 0 \implies a \leq b$$



Příklad

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

Kdy $3 \mid n^2+1$?

zbytek n^2+1 po dělení 3 závisí pouze na zb. n

rozdělíme podle zb. n po dělení 3

$n = 3k$

$\Rightarrow n^2+1 = (3k)^2+1 = 9k^2+1 = 3\cdot(3k^2)+1$ → zb. 1

$n = 3k+1$

$\Rightarrow n^2+1 = (3k+1)^2+1 = 9k^2+6k+2 = 3(3k^2+2)+2$ → zb. 2

$n = 3k+2$

$\Rightarrow n^2+1 = (3k+2)^2+1 = 9k^2+12k+5 = 3(3k^2+6k+1)+2$ → zb. 2

Příklad

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

Řešení

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 3.

Řešení

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 $n+1$.

vždy $n+1 \mid n^2-1$ protože $n^2-1=(n-1)(n+1)$

$\Rightarrow$ $\dfrac{n+1 \mid n^2+1}{n+1 \mid (n^2+1)-(n^2-1)=2}$ $\Rightarrow$ $n+1 \in \{-2,-1,1,2\}$

$n \in \{-3,-2,0,1\}$

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 $a = qm + r$.

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 $a = qm + r$.

zbytek

Důkaz. uvažme $a \geq 0$

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). □

Pro $a < 0$ potřeba řešit zvlášť, v C++ není specifikováno

$(-2) \bmod 5$

$2 \bmod 5$

$-2 = (-1) \cdot 5 + 3$

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

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

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.

Plán přednášky

1 Problémy teorie čísel

2 Dělitelnost

3 Společní dělitelé a společné násobky

4 Prvočísla

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.

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 $m \mid a_1$, $m \mid a_2$ 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).

největ. nebo dělitelný ostatní

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 $m \mid a_1$, $m \mid a_2$ 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).

jiná

$NSD(a_1, a_2)$

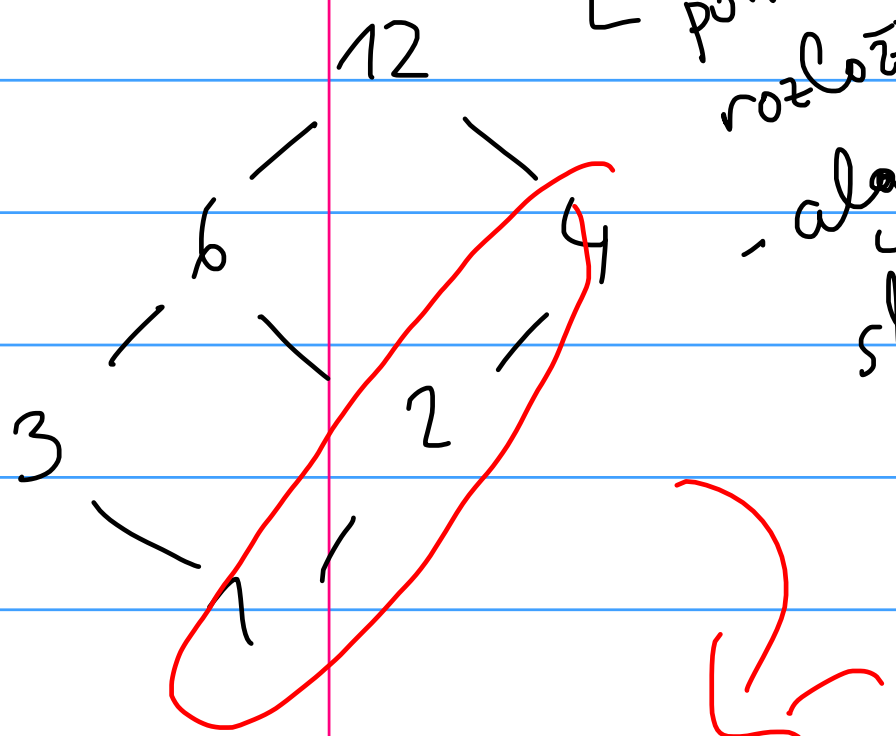
$GCD(a_1, a_2$

Například $(12, 64) = 4$.

$(12,64) = ?$

$12 = 2^2 \cdot 3$

↳ potřeba rozložit - algoritmus složíte



$(12,64) = 4$

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

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 $[a_1, a_2]$.

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

1 je dělitelné pouze 1

0 je dělitelná vším

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 roklad na prvočinitele, ale ten je výpočetně velmi náročný (RSA) a navíc k jeho odvození budeme existenci největšího společného dělitele využívat.

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 roklad 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.

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

Euklidův algoritmus

Algoritmus a důkaz jeho korektnosti demonstrujeme na příkladu:

Příklad

Určete největšího společného dělitele čísel 10175 a 2277.

$(10175, 2277) = ?$

$$(a, b) = (a - b, b) = (a - k \cdot b, b)$$

$10175 = 4 \cdot 2277 + 1067$

$2277 = 2 \cdot 1067 + 143$

$1067 = 7 \cdot 143 + 66$

$143 = 2 \cdot 66 + 11$

$66 = 6 \cdot 11 + 0$

$11 = 1 \cdot 143 - 2 \cdot 66$

$= 1 \cdot 143 - 2 \cdot (1067 - 7 \cdot 143)$

$= -2 \cdot 1067 + 15 \cdot 143$

$= -2 \cdot 1067 + 15 \cdot (2277 - 2 \cdot 1067)$

$= 15 \cdot 2277 - 32 \cdot 1067$

$= 15 \cdot 2277 - 32 \cdot (10175 - 4 \cdot 2277)$

$= -32 \cdot 10175 + 143 \cdot 2277$

$(10175, 2277) = (1067, 2277) = (2277, 1067)$

$4 \cdot 2277 + 1067$

$= (1067, 143) = (143, 66)$

$= (66, 11) = (11, 0) = 11$

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.

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

$3 = 2 - 1 \cdot 5$

$1 = 2 \cdot 2 + 1 \cdot 5$

$1 = (2, 5) = k_1 \cdot 2 + k_2 \cdot 5$

vejsou jednoznačně

$1 = (7, 11) = k_1 \cdot 7 + k_2 \cdot 11$

$2 = (2, 4) = k_1 \cdot 2 + k_2 \cdot 4$

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

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).

Jiná organizace výpočtu:

$(10175, 2277) = ?$

	10175	2277		
	1	0	10175	$\leftarrow 1 \cdot 10175 + 0 \cdot 2277 = 10175$
-4x	0	1	2277	$\leftarrow 0 \cdot 10175 + 1 \cdot 2277 = 2277$
-2x	1	-4	1067	
-7x	-2	9	143	
-2x	15	-67	66	
-6x	-32	143	11	$\leftarrow -32 \cdot 10175 + 143 \cdot 2277 = 11$
	*	*	0	

výsledek

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.

počet kroků lin. v délce A,B
⇒ složitost kvadratická

Příklad v systému SAGE lze vyzkoušet na https://cocalc.com/.

Poznámka

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 $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.

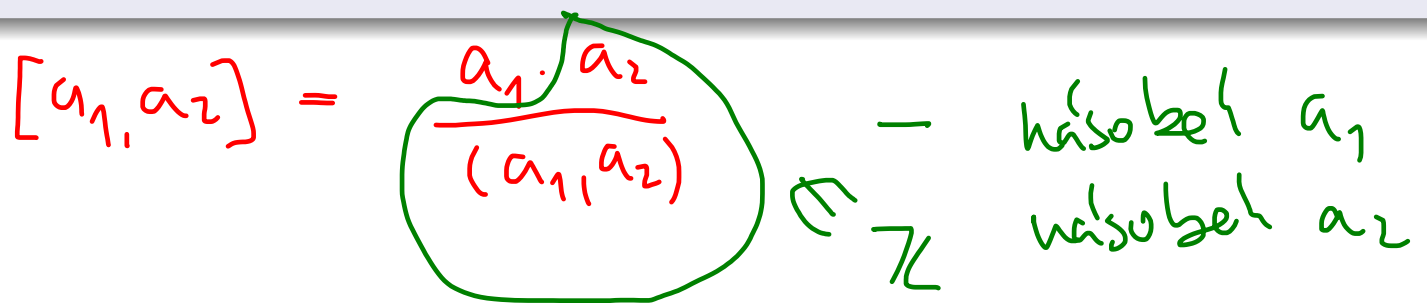
Nejmenší společný násobek

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. □



Nesoudělnost

$1 = (7, 11)$ ... $7, 11$ jsou nesoudělná

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

používá při Eukleidově algoritmu

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* $(q_1, q_2) = 1$.

$(a + k \cdot b, b) = (a, b)$

(2) $c \cdot b \cdot c$ dělitelné a

$k \cdot a \cdot c$ dělitelné a

$(k \cdot a + l \cdot b) \cdot c$ dělitelné a

můžeme vhodnou volbou k, l dostat 1

Plán přednášky

1 Problémy teorie čísel

2 Dělitelnost

3 Společní dělitelé a společné násobky

4 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*.

Pozn. 1 není prvočíslo

$6 = 2 \cdot 3 = 3 \cdot 2 = \cancel{1 \cdot 2 \cdot 3 \text{ atd.}}$

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, je totiž invertibilní, neboli tzv. jednotkou okruhu celých čísel). 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).

Základní věta aritmetiky

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

Věta (Euklidova 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 $p \mid b$.

plyne z $p \mid a \cdot b$ a $(p, a) = 1 \Rightarrow p \mid b$

$(p, a) = 1 \Leftrightarrow p \nmid a$

Základní věta aritmetiky

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

Věta (Euklidova 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.)

existence rozkladu: rozděl a panuj

$\underline{n}$ – prvočíslo $n = n$ rozklad

– složené / alg. složité $\Rightarrow$ $n = a \cdot b$

menší, rekurze

jednoznačnost:

$$p_1 \cdots p_r = n = q_1 \cdots q_s$$

$$p_1 \mid p_1 \cdots p_r = q_1 \cdots q_s$$

$\overset{V}{\Rightarrow}$ $\exists i : p_1 \mid q_i$ můžeme předp. $p_1 \mid q_1$

$\xrightarrow{q_1 \text{ prvočíslo}, \; p_1 \neq 1}$ $p_1 = q_1$

vydělíme p_1 a aplikujeme indukci

na $\underline{p_2 \cdots p_r} = \frac{n}{p_1} = \underline{q_2 \cdots q_s}$

V. Prvočísel je nekonečně mnoho

D. Předp. že $p_1, \dots, p_r$ jsou

všechna prvočísla a uvažme

$$p_1 \cdots p_r + 1$$ a rozložme na

součin prvočísel

Ale to nelze, protože jediné přir. číslo které nen

$$p_i \nmid p_1 \cdots p_r + 1 \neq 1$$ dil. prvočís

neboť $$(p_i, \underbrace{p_1 \cdots p_r}_{\text{násobek } p_i} + 1) = (p_i, 1) = 1$$

V. Mezi čísly tvaru $3k+1$ je ∞ prvočísel.