Diskrétní matematika – 1. týden
Elementární teorie čísel – dělitelnost

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

podzim 2024

Obsah přednášky

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

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,

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

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.

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?

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

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

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 $4k + 6\ell = n$?

Plán přednášky

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

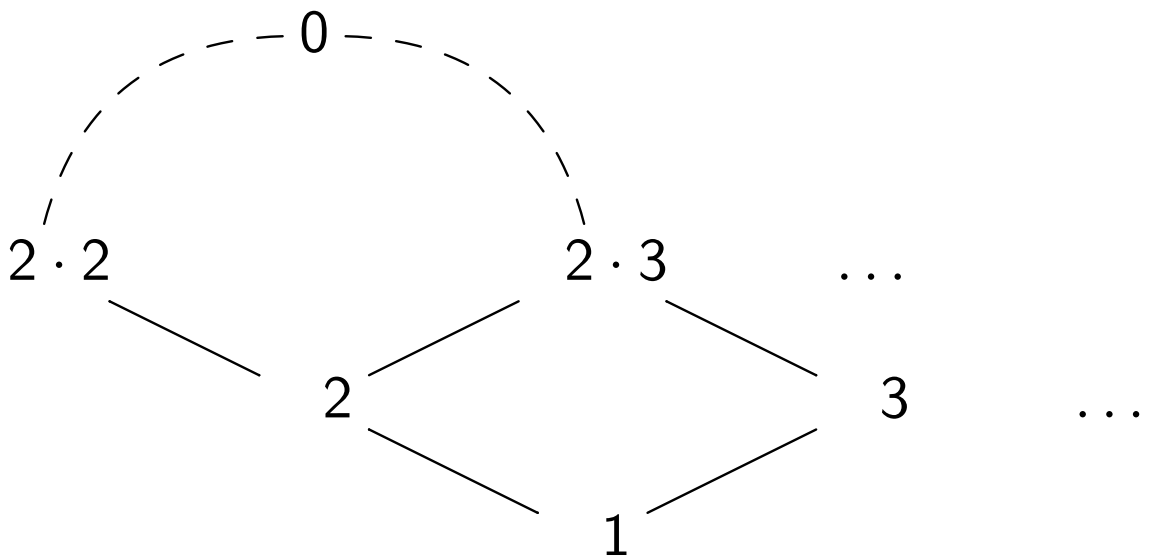
Řekneme, že celé číslo a *dělí* celé číslo b (neboli číslo b je *dělitelné* číslem a, též b je *násobek* a), právě když existuje celé číslo c tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$.

Snadno se vidí, že dělitelnost je uspořádání na přirozených (tedy nezáporných celých) číslech, tj. splňuje reflexivitu $a \mid a$, tranzitivitu $a \mid b \mid c \implies a \mid c$ a antisymetrii $a \mid b \mid a \implies a = b$:

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 $a \mid b$.

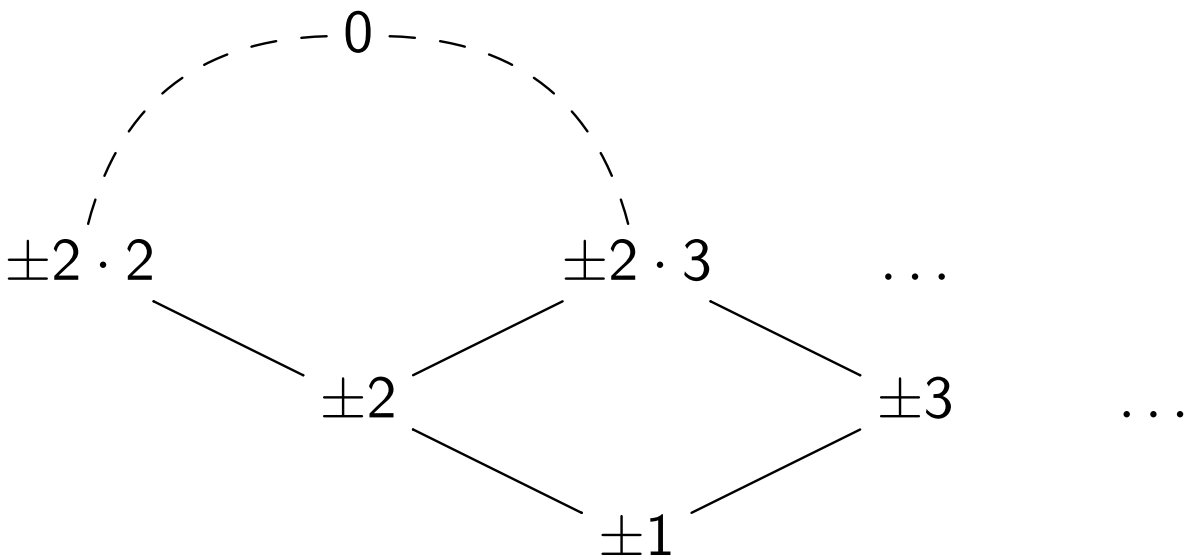
Snadno se vidí, že dělitelnost je uspořádání na přirozených (tedy nezáporných celých) číslech, tj. splňuje reflexivitu $a \mid a$, tranzitivitu $a \mid b \mid c \implies a \mid c$ a antisymetrii $a \mid b \mid a \implies a = b$:



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 $a \mid b$.

Snadno se vidí, že dělitelnost je uspořádání na přirozených (tedy nezáporných celých) číslech, tj. splňuje reflexivitu $a \mid a$, tranzitivitu $a \mid b \mid c \implies a \mid c$ a antisymetrii $a \mid b \mid a \implies a = b$:



Dále nás budou zajímat algebraické vlastnosti dělitelnosti:

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

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

Dále nás budou zajímat algebraické vlastnosti dělitelnosti:

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

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

Příklad

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

Dále nás budou zajímat algebraické vlastnosti dělitelnosti:

$$a \mid b \ \wedge \ a \mid c \implies a \mid b+c \ \wedge \ a \mid b-c$$
$$a \mid b \iff ac \mid bc \quad (c \neq 0)$$

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.

Dále nás budou zajímat algebraické vlastnosti dělitelnosti:

$$a \mid b \ \wedge \ a \mid c \implies a \mid b+c \ \wedge \ a \mid b-c$$
$$a \mid b \iff ac \mid bc \quad (c \neq 0)$$

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 $n+1$.

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 $a = qm + r$.

Důkaz.

Dokážeme pro $a \geq 0$ 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). □

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

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 přirozená čísla a, b. Libovolné přirozené číslo m takové, že $m \mid a$, $m \mid b$ se nazývá *společný dělitel* čísel a, b. Společný dělitel čísel a, b, který je dělitelný libovolným společným dělitelem těchto čísel, se nazývá *největší společný dělitel* čísel a, b a značí se (a, b). (Jedná se o infimum vzhledem k dělitelnosti.)

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 přirozená čísla a, b. Libovolné přirozené číslo m takové, že $m \mid a$, $m \mid b$ se nazývá *společný dělitel* čísel a, b. Společný dělitel čísel a, b, který je dělitelný libovolným společným dělitelem těchto čísel, se nazývá *největší společný dělitel* čísel a, b a značí se (a, b). (Jedná se o infimum vzhledem k dělitelnosti.)

Například $(12, 16) = 4$.

Poznámka

Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{N}$ platí $(a, b) = (b, a)$, $(a, 1) = 1$, $(a, 0) = a$.

Poznámka

Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{N}$ platí $(a, b) = (b, a)$, $(a, 1) = 1$, $(a, 0) = a$.

Definice

Mějme přirozená čísla a, b. Libovolné přirozené číslo m takové, že $a \mid m$, $b \mid m$ se nazývá *společný násobek* čísel a, b. Společný násobek čísel a, b, který dělí libovolný společný násobek těchto čísel, se nazývá *nejmenší společný násobek* čísel a, b a značí se $[a, b]$.

Poznámka

Přímo z definice plyne, že pro libovolné $a, b \in \mathbb{N}$ platí $(a, b) = (b, a)$, $(a, 1) = 1$, $(a, 0) = a$.

Definice

Mějme přirozená čísla a, b. Libovolné přirozené číslo m takové, že $a \mid m$, $b \mid m$ se nazývá *společný násobek* čísel a, b. Společný násobek čísel a, b, který dělí libovolný společný násobek těchto čísel, se nazývá *nejmenší společný násobek* čísel a, b a značí se $[a, b]$.

Poznámka

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

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.

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

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).

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/`.

Poznámka

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

Nesoudělnost

Definice

Čísla $a, b \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a, b) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé $i \neq j$ platí $(a_i, a_j) = 1$.

Nesoudělnost

Definice

Čísla $a, b \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a, b) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé $i \neq j$ platí $(a_i, a_j) = 1$.

Věta

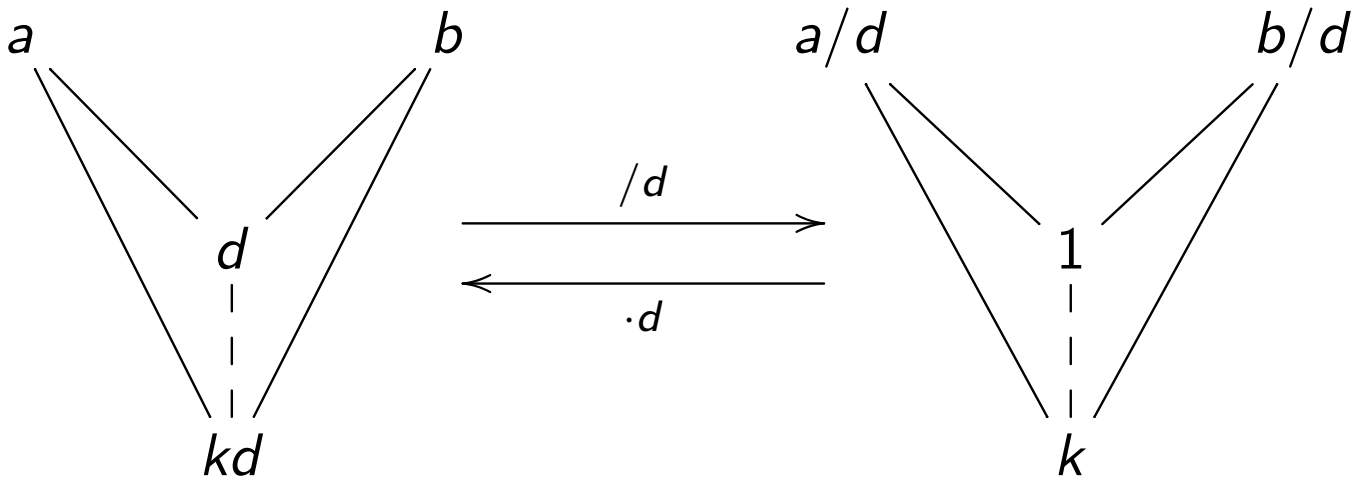
Pro libovolná přirozená čísla a, b a jejich největšího společného dělitele $(a, b) = d$ jsou čísla a/d, b/d nesoudělná.

Důkaz.

Číslo k je společný dělitel čísel a/d, b/d, právě když

$$k \mid a/d,\ k \mid b/d \Leftrightarrow kd \mid a,\ kd \mid b \Leftrightarrow kd \mid (a,b) = d \Leftrightarrow k \mid 1$$

a jediné takové k je tedy 1. □



Věta

Pro libovolná přirozená čísla a, b, c platí: jestliže $c \mid ab$, $(c, a) = 1$, pak $c \mid b$.

Důkaz.

Zjevně $c \mid cb$ a podle předpokladu také $c \mid ab$, musí tedy c dělit i jakoukoliv jejich celočíselnou kombinaci; přitom podle Bezoutova lemmatu $kc + la = 1$, takže

$$c \mid (k \cdot cb + l \cdot ab) = (kc + la)b = b. \qquad \square$$

Nejmenší společný násobek

Věta

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

Důkaz.

Nejlépe se vidí přes rozklad na součin prvočísel. □

Plán přednášky

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*.

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 $p \mid b$.

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.)