



## Literatura

[1] J. Herman, R. Kučera a J. Šimša. *Metody řešení matematických úloh I*. MU Brno, druhé vydání, 2001.

### 1. Základní pojmy

#### 1.1. 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 [1, §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:

$$a \mid b \wedge b \mid c \implies a \mid c \quad (1)$$

$$a \mid b \wedge a \mid c \implies a \mid b + c \wedge a \mid b - c \quad (2)$$

$$c \neq 0 \implies (a \mid b \iff ac \mid bc) \quad (3)$$

$$a \mid b \wedge b > 0 \implies a \leq b \quad (4)$$



**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.  $\square$

**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  $q \in \mathbb{Z}$ ,  $r \in \{0, 1, \dots, m - 1\}$  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  $a' \in \{0, 1, 2, \dots, a - 1\}$ . Speciálně pro  $a' = a - m$  tedy existují  $q', r'$  tak, že  $a' = q'm + r'$  a přitom  $r' \in \{0, 1, \dots, m - 1\}$ . 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  $a \geq 0$ . Je-li naopak  $a < 0$ , pak ke kladnému číslu  $-a$  podle výše dokázaného existují  $q' \in \mathbb{Z}$ ,  $r' \in \{0, 1, \dots, m - 1\}$  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  $q_1, q_2 \in \mathbb{Z}$ ;  $r_1, r_2 \in \{0, 1, \dots, m - 1\}$  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 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.  $\square$

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

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

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.  $\square$

## 1.2. 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  $a_3 = a_1 - q_1 a_2$ , 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 dělitel čísel  $a_1, a_2$ .  $\square$

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.

**VĚTA 3.** (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  $a_3 = a_1 - q_1 a_2$ ,  $a_4 = a_2 - q_2 a_3$ ,  $\dots$ ,  $a_{k-1} = a_{k-3} - q_{k-3} a_{k-2}$ , což je ovšem  $(a_1, a_2)$ .  $\square$

**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 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.  $\square$

### 1.3. Dělitelé a násobky mnoha čísel.

DEFINICE. Největší společný dělitel a nejmenší společný násobek  $n$  čísel  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  definujeme analogicky jako v 1.2. Libovolné  $m \in \mathbb{Z}$  takové, že  $m \mid a_1, m \mid a_2, \dots, m \mid a_n$  (resp.  $a_1 \mid m, a_2 \mid m, \dots, a_n \mid m$ ) se nazývá *společný dělitel* (resp. *společný násobek*) čísel  $a_1, a_2, \dots, a_n$ . Společný dělitel (resp. násobek)  $m \geq 0$  čísel  $a_1, a_2, \dots, a_n$ , který je dělitelný libovolným společným dělitelem (resp. dělí libovolný společný násobek) těchto čísel, se nazývá *největší společný dělitel* (resp. *nejmenší společný násobek*) čísel  $a_1, a_2, \dots, a_n$  a značí se  $(a_1, a_2, \dots, a_n)$  (resp.  $[a_1, a_2, \dots, a_n]$ ).



Snadno se přesvědčíme, že platí

$$(a_1, \dots, a_{n-1}, a_n) = ((a_1, \dots, a_{n-1}), a_n), \quad (6)$$

$$[a_1, \dots, a_{n-1}, a_n] = [[a_1, \dots, a_{n-1}], a_n]. \quad (7)$$

Největší společný dělitel  $(a_1, \dots, a_n)$  totiž dělí všechna čísla  $a_1, \dots, a_n$ , a tedy je společným dělitelem čísel  $a_1, \dots, a_{n-1}$ , a proto dělí i největšího společného dělitele  $(a_1, \dots, a_{n-1})$ , tj.  $(a_1, \dots, a_n) \mid ((a_1, \dots, a_{n-1}), a_n)$ . Naopak největší společný dělitel čísel  $(a_1, \dots, a_{n-1}), a_n$  musí kromě čísla  $a_n$  dělit i všechna čísla  $a_1, \dots, a_{n-1}$ , protože dělí jejich největšího společného dělitele, a proto  $((a_1, \dots, a_{n-1}), a_n) \mid (a_1, \dots, a_n)$ . 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 nejmenší společný násobek libovolných  $n - 1$  čísel, podle (6) a (7) existuje i pro libovolných  $n$  čísel.

#### 1.4. Nesoudělnost.

DEFINICE. Čísla  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  se nazývají *nesoudělná*, jestliže platí  $(a_1, a_2, \dots, a_n) =$

1. Čísla  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  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

$$2^{91} - 1 = 2^{28}(2^{63} - 1) + 2^{28} - 1,$$

$$2^{63} - 1 = (2^{35} + 2^7)(2^{28} - 1) + 2^7 - 1,$$

$$2^{28} - 1 = (2^{21} + 2^{14} + 2^7 + 1)(2^7 - 1).$$

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  $(a, b) = 1$  a  $a \mid bc$ , 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  $a \mid c$ .

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).  $\square$

## 2. 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, . . . Prvočísel je, jak brzy dokážeme, nekonečně mnoho, máme ovšem poměrně limitované výpočetní prostředky na zjištění, zda je dané číslo prvočíslem (největší známé prvočíslo  $2^{30\,402\,457} - 1$  má pouze 9 152 052 cifer).

**VĚTA 6.** *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  $p \mid b$ .*

**DŮKAZ.** „ $\Rightarrow$ “ Předpokládejme, že  $p$  je prvočíslo a  $p \mid ab$ , kde  $a, b \in \mathbb{Z}$ . Protože  $(p, a)$  je kladný dělitel  $p$ , platí  $(p, a) = p$  nebo  $(p, a) = 1$ . V prvním případě  $p \mid a$ , ve druhém  $p \mid b$  podle věty 5.

„ $\Leftarrow$ “ Jestliže  $p$  není prvočíslo, musí existovat jeho kladný dělitel různý od 1 a  $p$ . Označíme jej  $a$ ; pak ovšem  $b = \frac{p}{a} \in \mathbb{N}$  a platí  $p = ab$ , odkud  $1 < a < p$ ,  $1 < b < p$ . Našli jsme tedy celá čísla  $a, b$  tak, že  $p \mid ab$  a přitom  $p$  nedělí ani  $a$ , ani  $b$ .  $\square$

**PŘÍKLAD.** Nalezněte všechna čísla  $k \in \mathbb{N}_0$ , pro která je mezi deseti po sobě jdoucími čísly  $k + 1, k + 2, \dots, k + 10$  nejvíce prvočísel.

**ŘEŠENÍ.** Pro  $k = 1$  je mezi našimi čísly pět prvočísel: 2, 3, 5, 7, 11. Pro  $k = 0$  a  $k = 2$  pouze čtyři prvočísla. Jestliže  $k \geq 3$ , není mezi zkoumanými čísly číslo 3. Mezi deseti po sobě jdoucími celými čísly pět sudých a pět lichých čísel, mezi kterými je zase aspoň jedno dělitelné třemi. Našli jsme tedy mezi čísly  $k + 1$ ,



$k + 2, \dots, k + 10$  aspoň šest složených, jsou tedy mezi nimi nejvýše čtyři prvočísla. Zadáni proto vyhovuje jediné číslo  $k = 1$ .  $\square$

**PŘÍKLAD.** Dokažte, že pro libovolné přirozené číslo  $n$  existuje  $n$  po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslu.

**ŘEŠENÍ.** Zkoumejme čísla  $(n + 1)! + 2, (n + 1)! + 3, \dots, (n + 1)! + (n + 1)$ . Mezi těmito  $n$  po sobě jdoucími čísly není žádné prvočíslu, protože pro libovolné  $k \in \{2, 3, \dots, n + 1\}$  platí  $k \mid (n + 1)!$ , a tedy  $k \mid (n + 1)! + k$ , a proto  $(n + 1)! + k$  nemůže být prvočíslu.  $\square$

**PŘÍKLAD.** Dokažte, že pro libovolné prvočíslu  $p$  a libovolné  $k \in \mathbb{N}$ ,  $k < p$ , je kombinační číslo  $\binom{p}{k}$  dělitelné  $p$ .

**ŘEŠENÍ.** Podle definice kombinačního čísla

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{1 \cdot 2 \cdot \dots \cdot k} \in \mathbb{N},$$

a tedy  $k! \mid p \cdot a$ , kde jsme označili  $a = (p-1) \cdot \dots \cdot (p-k+1)$ . Protože  $k < p$ , není žádné z čísel  $1, 2, \dots, k$  dělitelné prvočíslem  $p$ , a tedy podle věty 6 není ani  $k!$  dělitelné prvočíslem  $p$ , odkud  $(k!, p) = 1$ . Podle věty 5 platí  $k! \mid a$ , a tedy  $b = \frac{a}{k!}$  je celé číslo. Protože  $\binom{p}{k} = \frac{pa}{k!} = pb$ , je číslo  $\binom{p}{k}$  dělitelné číslem  $p$ .  $\square$



VĚTA 7. *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.)*

POZNÁMKA. Dělitelnost je možné obdobným způsobem jako v 1.1 definovat v libovolném oboru integrity (zkuste si rozmyslet, proč se omezujeme na obory integrity). V některých oborech integrity přitom žádné prvky s vlastností prvočísla (říkáme jim *ireducibilní*) neexistují (např.  $\mathbb{Q}$ ), v jiných sice ireducibilní prvky existují, ale zase tam neplatí věta o jednoznačném rozkladu (např. v  $\mathbb{Z}(\sqrt{-5})$  máme následující rozklady:  $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ ; zkuste si rozmyslet, že všichni uvedení činitelé jsou skutečně v  $\mathbb{Z}(\sqrt{-5})$  ireducibilní).

DŮKAZ. Nejprve dokážeme indukcí, že každé  $n \geq 2$  je možné vyjádřit jako součin prvočísel.

Je-li  $n = 2$ , je  $n$  součin jediného prvočísla 2.

Předpokládejme nyní, že  $n > 2$  a že jsme již dokázali, že libovolné  $n'$ ,  $2 \leq n' < n$ , je možné rozložit na součin prvočísel. Jestliže  $n$  je prvočíslo, je součinem jediného prvočísla. Jestliže  $n$  prvočíslo není, pak existuje jeho dělitel  $d$ ,  $1 < d < n$ . Označíme-li  $c = \frac{n}{d}$ , platí také  $1 < c < n$ . Z indukčního předpokladu plyne, že  $c$  i  $d$  je možné vyjádřit jako součin prvočísel, a proto je takto možné vyjádřit i jejich součin  $c \cdot d = n$ .



Nyní dokážeme jednoznačnost. Předpokládejme, že platí rovnost součinů  $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$ , kde  $p_1, \dots, p_m, q_1, \dots, q_s$  jsou prvočísla a navíc platí  $p_1 \leq p_2 \leq \dots \leq p_m, q_1 \leq q_2 \leq \dots \leq q_s$  a  $1 \leq m \leq s$ . Indukcí vzhledem k  $m$  dokážeme, že  $m = s, p_1 = q_1, \dots, p_m = q_m$ .

Je-li  $m = 1$ , je  $p_1 = q_1 \cdot \dots \cdot q_s$  prvočíslo. Kdyby  $s > 1$ , mělo by číslo  $p_1$  dělitele  $q_1$  takového, že  $1 < q_1 < p_1$  (neboť  $q_2 q_3 \dots q_s > 1$ ), což není možné. Je tedy  $s = 1$  a platí  $p_1 = q_1$ .

Předpokládejme, že  $m \geq 2$  a že tvrzení platí pro  $m - 1$ . Protože  $p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_s$ , dělí  $p_m$  součin  $q_1 \cdot \dots \cdot q_s$ , což je podle věty 6 možné jen tehdy, jestliže  $p_m$  dělí nějaké  $q_i$  pro vhodné  $i \in \{1, 2, \dots, s\}$ . Protože  $q_i$  je prvočíslo, plyne odtud  $p_m = q_i$  (neboť  $p_m > 1$ ). Zcela analogicky se dokáže, že  $q_s = p_j$  pro vhodné  $j \in \{1, 2, \dots, m\}$ . Odtud plyne

$$q_s = p_j \leq p_m = q_i \leq q_s,$$

takže  $p_m = q_s$ . Vydělením dostaneme  $p_1 \cdot p_2 \cdot \dots \cdot p_{m-1} = q_1 \cdot q_2 \cdot \dots \cdot q_{s-1}$ , a tedy z indukčního předpokladu  $m - 1 = s - 1, p_1 = q_1, \dots, p_{m-1} = q_{m-1}$ . Celkem tedy  $m = s$  a  $p_1 = q_1, \dots, p_{m-1} = q_{m-1}, p_m = q_m$ . Jednoznačnost, a proto i celá věta 7 je dokázána.  $\square$

**POZNÁMKA.** Již jsme se zmínili, že je složité o velkých číslech s jistotou rozhodnout, jde-li o prvočíslo (na druhou stranu je o naprosté většině složených



čísel snadné prokázat, že jsou skutečně složená). Přesto se v roce 2002 podařilo indickým matematikům (Agrawal, Saxena, Kayal: [http://www.cse.iitk.ac.in/users/manindra/primality\\_v6.pdf](http://www.cse.iitk.ac.in/users/manindra/primality_v6.pdf)) dokázat, že problém prvočíselnosti je možné rozhodnout algoritmem s časovou složitostí polynomiálně závislou na počtu cifer vstupního čísla. Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán).

Že je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i výzva učiněná firmou RSA Security (viz <http://www.rsasecurity.com/rsalabs/node.asp?id=2093>). Pokud se vám podaří rozložit čísla označená podle počtu cifer jako RSA-704, RSA-768, ..., RSA-2048, obdržíte 30 000, 50 000, ..., resp. 200 000 dolarů (čísla RSA-576 a RSA-640 již byla rozložena v roce 2003, resp. 2005; byla-li vyplacena slíbená odměna, mi není známo).

**DŮSLEDEK.** (1) *Jsou-li  $p_1, \dots, p_k$  navzájem různá prvočísla a  $n_1, \dots, n_k \in \mathbb{N}_0$ , je každý kladný dělitel čísla  $a = p_1^{n_1} \cdots p_k^{n_k}$  tvaru  $p_1^{m_1} \cdots p_k^{m_k}$ , kde  $m_1, \dots, m_k \in \mathbb{N}_0$  a  $m_1 \leq n_1, m_2 \leq n_2, \dots, m_k \leq n_k$ . Číslo  $a$  má tedy právě*

$$\tau(a) = (n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$$



kladných dělitelů, jejichž součet je

$$\sigma(a) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

- (2) Jsou-li  $p_1, \dots, p_k$  navzájem různá prvočísla a  $n_1, \dots, n_k, m_1, \dots, m_k \in \mathbb{N}_0$  a označíme-li  $r_i = \min\{n_i, m_i\}$ ,  $t_i = \max\{n_i, m_i\}$  pro každé  $i = 1, 2, \dots, k$ , platí

$$(p_1^{n_1} \cdots p_k^{n_k}, p_1^{m_1} \cdots p_k^{m_k}) = p_1^{r_1} \cdots p_k^{r_k},$$

$$[p_1^{n_1} \cdots p_k^{n_k}, p_1^{m_1} \cdots p_k^{m_k}] = p_1^{t_1} \cdots p_k^{t_k}.$$

POZNÁMKA. S pojmem *součet všech kladných dělitelů čísla a* souvisí pojem tzv. *dokonalého čísla a*, které splňuje podmínku  $\sigma(a) = 2a$ , resp. slovně: „součet všech kladných dělitelů čísla  $a$  menších než  $a$  samotné je roven číslu  $a$ “.

Takovými čísly jsou např.  $6 = 1 + 2 + 3$ ,  $28 = 1 + 2 + 4 + 7 + 14$ ,  $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$  a  $8128$  (jde o všechna dokonalá čísla menší než 10 000).

Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž: *a je sudé dokonalé číslo, právě když je tvaru  $a = 2^q - 1 \cdot (2^q - 1)$ , kde  $2^q - 1$  je prvočíslo*. Mersenneho prvočísla jsou právě prvočísla tvaru  $2^k - 1$ . Bez zajímavosti není ani to, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět“ – obecně je pro velká čísla, u kterých se nedaří nalézt netriviálního





dělitele, obtížné prokázat, že jsou prvočísla. Pro Mersenneho prvočísla existuje poměrně jednoduchý a rychlý postup. Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru  $2^k - 1$  (viz např. <http://www.utm.edu/research/primes/largest.html>).

Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje**

**PŘÍKLAD.** Dokažte, že pro každé celé  $n > 2$  existuje mezi čísly  $n$  a  $n!$  alespoň jedno prvočísl.

**ŘEŠENÍ.** Označme  $p$  libovolné prvočísl dělící číslo  $n! - 1$  (takové existuje podle věty 7, protože  $n! - 1 > 1$ ). Kdyby  $p \leq n$ , muselo by  $p$  dělit číslo  $n!$  a nedělilo by  $n! - 1$ . Je tedy  $n < p$ . Protože  $p \mid (n! - 1)$ , platí  $p \leq n! - 1$ , tedy  $p < n!$ . Prvočísl  $p$  splňuje podmínky úlohy.  $\square$

Nyní uvedeme několik důkazů toho, že existuje nekonečně mnoho prvočísel (i když tvrzení v podstatě vyplývá už z předchozího příkladu).

**VĚTA 8.** *Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

**DŮKAZ.** (Eukleides) Předpokládejme, že prvočísel je konečně mnoho a označme je  $p_1, p_2, \dots, p_n$ . Položme  $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ . Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od  $p_1, \dots, p_n$  (čísla  $p_1, \dots, p_n$  totiž dělí číslo  $N - 1$ ), což je spor.

(Kummer, 1878): Předpokládejme, že prvočísel je konečně mnoho a označme je  $p_1 < p_2 < \dots < p_n$ . Položme  $N = p_1 \cdot p_2 \cdot \dots \cdot p_n > 2$ . Číslo  $N - 1$  je podle věty 7 dělitelné některým prvočíslem  $p_i$ , které dělí zároveň číslo  $N$  a tedy i  $N - (N - 1) = 1$ . Spor.

(Fürstenberg, 1955):

*V této poznámce uvedeme elementární „topologický“ důkaz existence nekonečně mnoha prvočísel. Zavedeme topologii prostoru celých čísel pomocí báze tvořené aritmetickými posloupnostmi (od  $-\infty$  do  $+\infty$ ). Lze snadno ověřit, že jde skutečně o topologický prostor, navíc lze ukázat, že je normální a tedy metrizovatelný. Každá aritmetická posloupnost je uzavřená i otevřená množina (její komplement je sjednocení ostatních aritmetických posloupností se stejnou diferencí). Dostáváme, že sjednocení konečného počtu aritmetických posloupností je uzavřená množina. Uvažme množinu  $A = \cup A_p$ , kde  $A_p$  je tvořena všemi násobky  $p$  a  $p$  probíhá všechna prvočísla. Jediná celá čísla nepatřící do  $A$  jsou  $-1$  a  $1$  a protože množina  $\{-1, 1\}$  zřejmě není otevřená, množina  $A$  nemůže být uzavřená. A tedy není konečným sjednocením uzavřených množin, což znamená, že musí existovat nekonečně mnoho prvočísel.*





**PŘÍKLAD.** Dokažte, že existuje nekonečně mnoho prvočísel tvaru  $3k + 2$ , kde  $k \in \mathbb{N}_0$ .

**ŘEŠENÍ.** Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je  $p_1 = 2, p_2 = 5, p_3 = 11, \dots, p_n$ . Položme  $N = 3p_2 \cdot p_3 \cdot \dots \cdot p_n + 2$ . Rozložíme-li  $N$  na součin prvočísel podle věty 7, musí v tomto rozkladu vystupovat aspoň jedno prvočíslo  $p$  tvaru  $3k+2$ , neboť v opačném případě by bylo  $N$  součinem prvočísel tvaru  $3k + 1$  (uvažte, že  $N$  není dělitelné třemi), a tedy podle příkladu na str. 3 by bylo i  $N$  tvaru  $3k + 1$ , což neplatí. Prvočíslo  $p$  ovšem nemůže být žádné z prvočísel  $p_1, p_2, \dots, p_n$ , jak plyne z tvaru čísla  $N$ , a to je spor.  $\square$

**POZNÁMKA.** Předchozí příklady je možné značně zobecnit. Platí totiž tvrzení: „Pro libovolné přirozené číslo  $n > 5$  existují mezi čísly  $n$  a  $2n$  alespoň dvě prvočísla“, které zobecňuje *Čebyševovu větu*: „Pro každé číslo  $n > 3$  existuje mezi čísly  $n$  a  $2n - 2$  alespoň jedno prvočíslo“. Důkaz lze provést elementárními prostředky, je však poměrně dlouhý.

Předchozí příklad zobecňuje *Dirichletova věta o aritmetické posloupnosti*: „Jsou-li  $a, m$  nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel  $k$  tak, že  $mk + a$  je prvočíslo“. Jde o hlubokou větu teorie čísel, k jejímuž důkazu je zapotřebí aparát značně přesahující její elementární část.



**OZNAČENÍ.** Pro libovolné prvočíslo  $p$  a libovolné přirozené číslo  $n$  je podle věty 7 jednoznačně určen exponent, se kterým vystupuje  $p$  v rozkladu čísla  $n$  na prvočinitele (pokud  $p$  nedělí číslo  $n$ , považujeme tento exponent za nulový). Budeme jej označovat symbolem  $v_p(n)$ . Pro záporné celé číslo  $n$  klademe  $v_p(n) = v_p(-n)$ .

Podle důsledku 2 můžeme právě zavedené označení  $v_p(n)$  charakterizovat tím, že  $p^{v_p(n)}$  je nejvyšší mocninou prvočísla  $p$ , která dělí číslo  $n$ , nebo tím, že  $n = p^{v_p(n)} \cdot m$ , kde  $m$  je celé číslo, které není dělitelné číslem  $p$ . Odtud snadno plyne, že pro libovolná nenulová celá čísla  $a, b$  platí

$$v_p(ab) = v_p(a) + v_p(b) \quad (8)$$

$$v_p(a) \leq v_p(b) \wedge a + b \neq 0 \implies v_p(a + b) \geq v_p(a) \quad (9)$$

$$v_p(a) < v_p(b) \implies v_p(a + b) = v_p(a) \quad (10)$$

$$v_p(a) \leq v_p(b) \implies v_p((a, b)) = v_p(a) \wedge v_p([a, b]) = v_p(b) \quad (11)$$

Na následujícím příkladu demonstrujme užitečnost zavedeného označení.

**PŘÍKLAD.** Dokažte, že pro libovolná přirozená čísla  $a, b, c$  platí

$$([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$$

**ŘEŠENÍ.** Podle věty 7 budeme hotovi, ukážeme-li, že  $v_p(L) = v_p(P)$  pro libovolné prvočíslo  $p$ , kde  $L$ , resp.  $P$  značí výraz na levé, resp. pravé straně. Nechť

je tedy  $p$  libovolné prvočíslo. Vzhledem k symetrii obou výrazů můžeme bez újmy na obecnosti předpokládat, že  $v_p(a) \leq v_p(b) \leq v_p(c)$ . Podle (11) platí  $v_p([a, b]) = v_p(b)$ ,  $v_p([a, c]) = v_p([b, c]) = v_p(c)$ ;  $v_p((a, b)) = v_p((a, c)) = v_p(a)$ ,  $v_p((b, c)) = v_p(b)$ , odkud  $v_p(L) = v_p(b) = v_p(P)$ , což jsme měli dokázat.  $\square$

[Home Page](#)

[Title Page](#)

[Contents](#)



Page 21 of 21

[Go Back](#)

[Full Screen](#)

[Close](#)

[Quit](#)