

Říkáme, že celé číslo  $b$  dělí celé číslo  $a$  (nebo  $b$  je dělitelem  $a$  nebo  $a$  je dělitelné  $b$  nebo  $a$  je násobkem  $b$ ), právě když existuje celé číslo  $x$ , pro které platí  $a = b \cdot x$ . Zapisujeme  $b \mid a$ . Jestliže k číslům  $a, b \in \mathbb{C}$  neexistuje  $x \in \mathbb{Z}$  takové, že  $a = b \cdot x$ , říkáme, že  $b$  nedělí  $a$  a zapisujeme  $b \nmid a$ .

Platí-li, že  $a = b \cdot x$ , pak čísla  $b$  a  $x$  jsou dělitelé čísla  $a$  a nazývají se sdružení dělitelé čísla  $a$ . Dělitelé čísla  $a$  patřící do množiny přirozených čísel se nazývají přirození dělitelé čísla  $a$ .

1. Každé celé číslo  $a \neq 0, 1, -1$  má alespoň 4 celočíselné dělitele, a to čísla  $1, a, -1, -a$ . Tyto dělitele nazýváme samozřejmými (triviálními) děliteli čísla  $a$ . (Ostatní dělitele čísla  $a$ , pokud existují, nazýváme nesamozřejmými nebo netriviálními děliteli čísla  $a$ .)
2. Čísla  $1$  a  $-1$  mají právě dva dělitele v množině  $\mathbb{Z}$ , a to  $1, -1$ .
3. Číslo  $0$  má nekonečně mnoho dělitelů, a to každé celé číslo.
4. Číslo  $0$  není dělitelem žádného nenulového čísla  $a$ , protože neexistuje žádné celé číslo  $x$  tak, aby platilo  $0 \cdot x = a$ .
5. Číslo  $0$  je dělitelem sebe sama ( $0 \mid 0$ ), neboť pro libovolné celé číslo  $x$  platí  $0 \cdot x = 0$ .

Věta 1. Pro libovolná celá čísla  $a, b, c$  platí

- a)  $(b \mid a \wedge b \mid c) \Rightarrow (b \mid a+c \wedge b \mid a-c)$
- b)  $b \mid a \Rightarrow (-b) \mid a$
- c)  $b \mid a \Rightarrow b \mid (-a)$

Celé číslo, které je dělitelné dvěma se nazývá sudé číslo.

Celé číslo, které není dělitelné dvěma (tj. při dělení dvěma dává zbytek  $1$ ) se nazývá liché číslo.

Na základě části b) a c) uvedené věty 1. můžeme dále teorii dělitelnosti budovat jen v množině přirozených čísel. (Určíme-li přirozené dělitele přirozeného čísla  $a$ , umíme snadno určit všechny dělitele čísla  $a$  i čísla  $-a$ .)

## ZNAKY DĚLITELNOSTI

Znaky dělitelnosti jsou věty, které umožňují rozhodnout o dělitelnosti čísla jiným číslem bez provedení dělení, jen ze zápisu čísla.

Ve všech dalších úvahách máme na mysli přirozená čísla zapsaná v desítkové soustavě.

1. Přirozené číslo  $a$  je dělitelné dvěma (pěti, deseti) právě tehdy, když je dvěma (pěti, deseti) dělitelné číslo, zapsané jeho cifrou nultého řádu.
2. Přirozené číslo  $a$  je dělitelné čtyřmi, právě když je čtyřmi dělitelné číslo zapsané jeho posledním dvojčíslím.
3. Přirozené číslo  $a$  je dělitelné osmi, právě když je osmi dělitelné číslo zapsané jeho posledním trojčíslím.

4. Přirozené číslo  $a$  je dělitelné třemi (devíti), právě když je třemi (devíti) dělitelný jeho ciferný součet. (Ciferný součet je součet všech čísel zapsaných jednotlivými číslicemi v zápisu čísla  $a$ )
5. Přirozené číslo  $a$  je dělitelné jedenácti, právě když je jedenácti dělitelný součet čísel zapsaných jednotlivými ciframi sudého řádu zmenšený o součet čísel zapsaných jednotlivými ciframi lichého řádu v zápisu čísla  $a$ .

Uvedené znaky dělitelnosti plynou z obecnějších vět:

- I. Dělíme-li přirozené číslo  $a$  dvěma (pěti, deseti) dostaneme stejný zbytek, jako když dělíme dvěma (pěti, deseti) číslo zapsané cifrou nultého řádu v zápisu čísla  $a$ .
- II. Dělíme-li přirozené číslo  $a$  (aspoň trojciferné) čtyřmi, dostaneme stejný zbytek, jako když dělíme čtyřmi číslo zapsané jeho posledním dvojčíslem.
- III. Dělíme-li přirozené číslo  $a$  (aspoň čtyřciferné) osmi, dostaneme stejný zbytek, jako když dělíme osmi číslo zapsané jeho posledním trojčíslem.
- IV. Dělíme-li přirozené číslo  $a$  třemi (devíti), dostaneme stejný zbytek, jako když dělíme třemi (devíti) jeho ciferný součet.
- V. Dělíme-li přirozené číslo  $a$  jedenácti, dostaneme stejný zbytek, jako když dělíme jedenácti součet čísel zapsaných ciframi sudého řádu zmenšený o součet čísel zapsaných ciframi lichých řádů.

Důkazy vět I. – V. provedeme s využitím věty 2.

Věta 2. Je-li celé číslo  $a$  součtem dvou celých čísel, z nichž jedno je násobkem celého čísla  $b$ , pak druhé dává při dělení číslem  $b$  stejný zbytek jako číslo  $a$ .

Důkaz:

Nechť  $a = c_1 + c_2$  a  $b \mid c_1$ , (tj.  $c_1 = b \cdot x$ ,  $x \in \mathbb{C}$ ), pak  $a = b \cdot x + c_2$  (1)

Dále předpokládejme, že  $a$  dává při dělení číslem  $b$  zbytek  $z$ ,

tj.  $a = b \cdot q + z$ , kde  $0 \leq z < |b|$  (2)

Z (1) vyjádříme  $c_2$ :  $c_2 = a - b \cdot x$  a dosadíme za  $a$  z (2)

$$c_2 = b \cdot q + z - b \cdot x = b \cdot (q - x) + z.$$

Číslo  $c_2$  tedy dává při dělení číslem  $b$  zbytek  $z$  jako číslo  $a$  při dělení číslem  $b$ .

Věta: Je-li přirozené číslo dělitelné po dvou nesoudělnými čísly, je dělitelné i jejich součinem. Tuto větu lze také obrátit. Ukázky dělitelnosti 12, 15, 18, 24, 36.

Obecné kritérium dělitelnosti přirozeného čísla  $a = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \dots + 10^na_n$  přirozeným číslem  $n$ : Pro dané přirozené číslo  $a$  vypočteme jeho ciferný součet  $c$  s vahami jednotlivých cifer takto: Pro každé  $k = 0, \dots, n$  označíme  $\beta_k$  zbytek po dělení čísla  $10^k$  číslem  $n$  (platí tedy  $\beta_k \equiv 10^k \pmod{n}$ ). Potom  $c = a_0 \beta_0 + a_1 \beta_1 + a_2 \beta_2 + \dots + a_n \beta_n$ . Podle pravidel pro počítání s kongruencemi (bude uvedeno dále) dává číslo  $c$  při dělení číslem  $n$  stejný zbytek, jako číslo  $a$ . Odtud plyne tvrzení: Číslo  $a$  je dělitelné číslem  $n$ , právě když číslo  $c$  je dělitelné číslem  $n$ .

Poznamenejme, že posloupnost čísel  $\beta_k$  je vždy konečná a počet jejích prvků nemůže být větší než číslo  $n-1$  (počet možných nenulových zbytků při dělení číslem  $n$ ). V opačném případě, pokud by některá mocnina deseti byla dělitelná číslem  $n$ , nepoužili bychom toto obecné kritérium. Kritérium dělitelnosti číslem  $n$  by potom bylo analogické kritériu dělitelnosti číslem 4, 8, 25, ...).

Příklad: Dělitelnost čísla 5894 sedmi. Platí:  $1 \equiv 1 \pmod{7}$ ,  $10 \equiv 3 \pmod{7}$ ,  $100 \equiv 2^k \pmod{7}$ ,  $1000 \equiv 6 \pmod{7}$ ,  $10^4 \equiv 4 \pmod{7}$ ,  $10^5 \equiv 5 \pmod{7}$ ,  $10^6 \equiv 1 \pmod{7}$ ,  $10^7 \equiv 3 \pmod{7}$ ,  $10^8 \equiv 2 \pmod{7}$  atd. Induktivním postupem jsme zjistili, že posloupnost zbytků 1, 3, 2, 6, 4, 5 se neustále opakuje. Proto  $\beta_0 = 1$ ,  $\beta_1 = 3$ ,  $\beta_2 = 2$ ,  $\beta_3 = 6$ ,  $\beta_4 = 4$ ,  $\beta_5 = 5$ ,  $\beta_6 = 1$ ,  $\beta_7 = 3$ ,  $\beta_8 = 2$  atd. Nyní vypočteme  $c = 4 \cdot 1 + 9 \cdot 3 + 8 \cdot 2 + 5 \cdot 6 = 77$ , což je číslo dělitelné sedmi. Proto i číslo 5894 je dělitelné sedmi. Poznamenejme, že s ohledem na vlastnosti kongruencí lze v posloupnosti čísel  $\beta_k$  nahradit kterékoli z nich číslem kongruentním s  $n$ , tedy posloupnost 1, 3, 2, 6, 4, 5 lze nahradit posloupností 1, 3, 2, -1, -3, -2, která je lépe zapamatovatelná a při výpočtech vhodnější (vypočtená čísla  $c$  jsou menší než pro původní hodnoty). Např. pro číslo 5894 by bylo  $c = 4 \cdot 1 + 9 \cdot 3 + 8 \cdot 2 + 5 \cdot (-1) = 42$ .

Příklad: Dělitelnost čísla  $a = 548\ 893\ 672\ 185\ 729\ 643$  číslem 17. Vypočteme posloupnost zbytků  $\beta_k$  (podrobnosti si již odpustíme): 1, -7, -2, -3, 4, 6, -8, 5, -1, 7, 2, 3, -4, -6, 8, -5. Nyní určíme ciferný součet  $c$  čísla  $a$  s vahami cifer:  $c = 3 \cdot 1 - 4 \cdot 7 - 6 \cdot 2 - 9 \cdot 3 + 2 \cdot 4 + 7 \cdot 6 - 5 \cdot 8 + 8 \cdot 5 - 1 \cdot 1 + 2 \cdot 7 + 7 \cdot 2 + 6 \cdot 3 - 3 \cdot 4 - 9 \cdot 6 + 8 \cdot 8 - 8 \cdot 5 + 4 \cdot 1 - 5 \cdot 7 = -42$ . Číslo  $c$  dává po dělení číslem 17 zbytek 9, tj. také zadané číslo  $a$  dává při dělení sedmnácti zbytek 9, není tedy číslem 17 dělitelné.

### PRVOČÍSLA, SLOŽENÁ ČÍSLA

Přirozené číslo  $p > 1$  nazýváme prvočíslem, právě když má právě dva různé přirozené dělitele (tj. čísla 1 a  $p$ ).

Přirozené číslo  $a > 1$ , které není prvočíslem (tj. má více než dva přirozené dělitele), nazýváme složeným číslem.

*Poznámka:* Číslo 1 podle definice není prvočíslo ani číslo složené.

Věta 2. Každé přirozené číslo  $n > 1$  má aspoň jednoho prvočíselného dělitele, menšího než  $\sqrt{n}$ .

Věta 3. Jestliže přirozené číslo  $a$  není dělitelné žádným prvočíslem menším nebo rovným  $\sqrt{a}$ , pak  $a$  je prvočíslo.

Věta 4. Každé složené číslo  $a$  lze vyjádřit právě jedním způsobem ve tvaru součinu konečného počtu prvočísel

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k},$$

kde  $p_1, p_2, \dots, p_k$  jsou prvočísla,  $e_1, e_2, \dots, e_k$  jsou nenulová přirozená čísla.

Tento zápis  $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$  se nazývá prvočíselný rozklad přirozeného čísla  $a$  a  $p_1, p_2, \dots, p_k$  jsou tzv. prvočinitelé rozkladu.

### NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Společný dělitel přirozených čísel  $a, b$  je každé přirozené číslo  $d$ , pro které platí  $d \mid a$  a  $d \mid b$ . Největší společný dělitel přirozených čísel  $a, b$  je ten ze společných dělitelů, který je dělitelný všemi společnými děliteli. Označujeme  $NSD(a, b)$ .

*Poznámka.* V množině přirozených čísel lze též říci, že největší společný dělitel je největší (maximální) číslo ze společných dělitelů.

Největší společný dělitel čísel můžeme určit různými způsoby:

- a) využitím definice,
- b) pomocí tzv. Euklidova algoritmu,
- c) pomocí rozkladu daných čísel na součin prvočinitelů.

Věta 5.

Jestliže přirozené číslo  $a$  dává při dělení nenulovým přirozeným číslem  $b$  nenulový zbytek  $z$ , tzn.  $a = b \cdot q + z$  a  $z < b$ , pak platí, že množina všech společných dělitelů čísel  $a, b$  je množinou všech společných dělitelů čísel  $b, z$ . Také největší společný dělitel čísel  $a, b$  je roven největšímu společnému děliteli čísel  $b, z$ , tj.  $NSD(a, b) = NSD(b, z)$ .

Tím převádíme problém určení  $NSD(a, b)$  na určení  $NSD(b, z)$ . Číslo  $b$  a  $z$  jsou menší než číslo  $a$ .

Na větě 5. je založen postup výpočtu největšího společného dělitele dvou přirozených čísel nazývaný Euklidův algoritmus. Použití Euklidova algoritmu ukážeme na příkladě:

Příklad:

Určete  $NSD(600, 252)$  pomocí Euklidova algoritmu.

*Řešení:*

$$\begin{array}{l} 600 : 252 = 2 \\ 96 \end{array} \quad \text{neboli} \quad 600 = 252 \cdot 2 + 96$$

$$\begin{array}{l} 252 : 96 = 2 \\ 60 \end{array} \quad 252 = 96 \cdot 2 + 60$$

$$\begin{array}{l} 96 : 60 = 1 \\ 36 \end{array} \quad 96 = 60 \cdot 1 + 36$$

$$\begin{array}{l} 60 : 36 = 1 \\ 24 \end{array} \quad 60 = 36 \cdot 1 + 24$$

$$\begin{array}{l} 36 : 24 = 1 \\ 12 \end{array} \quad 36 = 24 \cdot 1 + 12$$

$$\begin{array}{l} 24 : 12 = 2 \\ 0 \end{array} \quad 24 = 12 \cdot 2$$

Největší společný dělitel čísel  $600$  a  $252$  je číslo  $12$ , tj. poslední nenulový zbytek při postupném dělení.

Definice 5.

Přirozená čísla  $a, b$  se nazývají nesoudělná, právě když je jejich největší společný dělitel roven  $1$ , tedy  $NSD(a, b) = 1$

Definice 6.

Přirozená čísla  $a, b$  se nazývají soudělná, právě když je jejich největší společný dělitel větší než  $1$ , tedy  $NSD(a, b) > 1$ .

Definice 5. a 6. lze rozšířit na libovolný konečný počet přirozených čísel. Číslo po dvou nesoudělná.

## NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Definice 7.

Společný násobek přirozených čísel  $a, b$  je každé přirozené číslo  $m$ , které je dělitelné oběma čísly  $a, b$ , tj.  $a \mid m$  a  $b \mid m$ .

Definice 8.

Nejmenší společný násobek přirozených čísel  $a, b$  je ten ze společných násobků, který je dělitelem všech společných násobků čísel  $a, b$ . Zapisujeme  $NSN(a, b)$ .

Poznámka:

1. V množině přirozených čísel lze těž říci, že  $NSN(a, b)$  je nejmenší číslo z kladných společných násobků čísel  $a, b$ .
2. Definice 7. a 8. lze rozšířit na libovolný konečný počet přirozených čísel  $a_1, \dots, a_n$ .

Nejmenší společný násobek čísel  $a, b$  můžeme určit různými způsoby:

- d) využitím definice,
- e) pomocí vztahu mezi  $NSN(a, b)$  a  $NSD(a, b)$
- f) pomocí rozkladu daných čísel na součin prvočinitelů

Věta 5.

Pro každá dvě přirozená čísla  $a, b$  platí  $a \cdot b = NSN(a, b) \cdot NSD(a, b)$ .

Poznámka: Větu 5. nelze rozšířit na více než dvě přirozená čísla.

## ROZKLAD PŘIROZENÉHO ČÍSLA NA SOUČIN PRVOČIITELŮ - UŽITÍ

Prvočíselný rozklad přirozeného čísla využíváme především

- a) k výpočtu největšího společného dělitele a nejmenšího společného násobku daných čísel  $a, b$
- b) k určení počtu všech přirozených dělitelů daného přirozeného čísla.

ad a) Výpočet největšího společného dělitele a nejmenšího společného násobku z rozkladu daných čísel na součin prvočinitelů.

Největší společný dělitel daných přirozených čísel je součinem všech prvočinitelů, kteří se současně vyskytují v prvočíselných rozkladech všech daných čísel, a to s nejmenším s vyskytujícími se exponentů.

Nejmenší společný násobek daných čísel je součinem všech různých prvočinitelů, kteří se vyskytují v rozkladech daných čísel, a to v největší mocnině.

Příklad:

Zjistěte  $NSD(108, 90)$  a  $NSN(108, 90)$ .

Řešení:  $108 = 2^2 \cdot 3^3$       $90 = 2 \cdot 3^2 \cdot 5$

$$NSD(108, 90) = 2 \cdot 3^2 = 18$$

$$NSN(108, 90) = 2^2 \cdot 3^3 \cdot 5 = 540$$

ad b) Určení počtu všech přirozených dělitelů daného přirozeného čísla:

Věta 6: Je-li  $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$  prvočíselný rozklad přirozeného čísla  $a > 1$ , pak počet všech přirozených dělitelů čísla  $a$  (ozn.  $\mathcal{D}(a)$ ) je určen takto:

$$\mathcal{D}(a) = (e_1 + 1) \cdot (e_2 + 1) \cdot \dots \cdot (e_k + 1)$$

Všechny přirozené dělitele čísla  $a$  určíme jako všechny možné součiny prvočinitelů, přičemž každý prvočinitel, probíhá všechny mocniny od 0 po tu, ve které se vyskytují v rozkladu.

Příklad:

Zjistěte počet všech přirozených dělitelů čísla 648 a napište všechny přirozené dělitele čísla 648. Dále určete všechny dvojice sdružených dělitelů čísla 648.

Řešení:

	$3^0$	$3^1$	$3^2$	$3^3$	$3^4$
$2^0$	1	3	9	27	81
$2^1$	2	6	18	54	162
$2^2$	4	12	36	108	324
$2^3$	8	24	72	216	648

$$648 = 2^3 \cdot 3^4$$

$$\mathcal{D}(648) = (3+1) \cdot (4+1) = 20$$

Číslo 648 má 20 přirozených dělitelů.

Sdružené dvojice dělitelů: 1 . 648, 2 . 324, 3 . 216, 4 . 162, 6 . 108, 8 . 81, 9 . 72, 12 . 54, 18 . 36, 24 . 27.

## NEURČITÉ ROVNICE

Neurčité rovnice jsou rovnice se dvěma nebo více neznámými, které se řeší v oboru všech celých čísel.

### Definice 9

Lineární neurčitá rovnice o dvou neznámých  $x, y$  je rovnice

$$a \cdot x + b \cdot y = c, \quad a \neq 0, \quad b \neq 0.$$

*Poznámka.*

- Jsou-li koeficienty  $a, b, c$  racionální necelá čísla, vynásobíme rovnici vhodným číslem tak, aby nabyly celočíselných hodnot.
- Neurčité rovnice se nazývají též *diofantické*, podle řeckého matematika Diofanta z Alexandrie, 3. století př.n.l., který se zabýval řešením těchto rovnic.

Řešitelnost lineární neurčité rovnice.

Neurčitá rovnice  $a \cdot x + b \cdot y = c$  má řešení v případě, že největší společný dělitel koeficientů  $a, b$  je také dělitelem čísla  $c$ . Pak řešením je nekonečně mnoho dvojic celých čísel  $x, y$ .

V případě, že největší společný dělitel čísel  $a$ ,  $b$  není dělitelem koeficientu  $c$ , pak rovnice nemá řešení.

Řešení neurčité rovnice:

I. Necht'  $x_0, y_0$  je jedno pevné řešení neurčité rovnice. Potom obecné řešení je dáno vztahy

$$x = x_0 + \frac{b}{NSD(a,b)}t, \quad y = y_0 - \frac{a}{NSD(a,b)}t, \quad t \in \mathbf{Z}.$$

Výchozí dvojice  $x_0, y_0$  se určí buďto úsudkem nebo se vypočte z podílů Eukleidova algoritmu při hledání  $NSD(a, b)$ .

II. Redukční metoda.

### Kongruence, rozklad na zbytkové třídy.

**Věta:** Necht'  $a, b$  jsou celá čísla taková, že  $b \neq 0$ . Potom existují celá čísla  $q, r$  splňující vztah:

$$a = bq + r, \quad 0 \leq r < |b|, \quad \text{přičemž toto vyjádření je jednoznačné.}$$

*Poznámka:* Je nutno si uvědomit, že zbytek  $r$  při dělení je vždy nezáporný, a to i při dělení záporným číslem. Např.  $a = -26, b = 8, q = -4, r = 6$ , protože  $-26 = 8 \cdot (-4) + 6$ .

*Poznámka:* Celá čísla  $a, b$  jsou nesoudělná, je-li jejich největší společný dělitel roven jedné. V opačném případě se nazývají soudělná. Největší společný dělitel čísel  $a, b$  budeme označovat  $NSD(a, b)$ , nejmenší kladný společný násobek  $NSN(a, b)$ .

**Eulerova funkce**  $\varphi(n)$  vyjadřuje počet přirozených čísel menších nebo rovných číslu  $n$ , nesoudělných s  $n$ . Necht'  $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ , pak platí  $\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$ . Je-li  $n$  prvočíslo, pak  $\varphi(n) = n - 1$ .

**Kongruence:**  $a, b \in \mathbf{Z}, m \in \mathbf{N}, m \geq 2$ . Platí  $a \equiv b \Leftrightarrow m \mid (a - b)$ . Čteme: Číslo  $a$  je kongruentní s číslem  $b$  podle modulu  $m$ . Dvě čísla kongruentní podle nějakého modulu  $m$  dávají při dělení tímto modulem  $m$  týž zbytek. Relace kongruence je ekvivalence na množině všech celých čísel (je reflexivní, symetrická a tranzitivní).

*Vlastnosti kongruencí:*

1)  $p$  prvočíslo, pak  $a \equiv b \pmod{p^n} \Rightarrow a \equiv b \pmod{p}$

Platí-li kongruence podle modulu, který je mocninou prvočísla, platí i podle modulu rovného tomuto prvočíslu.

2)  $a \equiv b \pmod{m_i}, i = 1, 2, \dots, k \Rightarrow a \equiv b \pmod{NSN(m_1, \dots, m_k)}$

Platí-li kongruence podle několika modulů, platí i podle modulu rovného nejmenšímu společnému násobku těchto modulů.

$$3) a_i \equiv b_i \pmod{m}, i = 1, \dots, k \Rightarrow \sum_{i=1}^k a_i \equiv \sum_{i=1}^k b_i \pmod{m}, \prod_{i=1}^k a_i \equiv \prod_{i=1}^k b_i \pmod{m}.$$

Kongruence podle téhož modulu lze sčítat i násobit.

Nechť v dalším platí  $a \equiv b \pmod{m}$ :

$$4) a + x \equiv b + x \pmod{m}, a \cdot y \equiv b \cdot y \pmod{m}$$

K oběma stranám kongruence lze přičíst stejné celé číslo a obě strany kongruence lze vynásobit týmž celým číslem. Obecně ale nelze obě strany kongruence dělit týmž celým číslem, např.  $24 \equiv 40 \pmod{8}$ , ale po vydělení čtyřmi  $6 \not\equiv 10 \pmod{8}$ .

$$5) m \mid z \Rightarrow a + z \equiv b \pmod{m}$$

Celé číslo, které je násobkem modulu, lze přičíst pouze k jedné straně kongruence.

$$6) a^n \equiv b^n \pmod{m}$$

Obě strany kongruence lze umocnit na libovolný přirozený exponent.

$$7) d \mid a \wedge d \mid b \wedge \text{NSD}(d, m) = 1 \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$$

Obě strany kongruence lze vydělit celým číslem nesoudělným s modulem.

$$8) ac \equiv bc \pmod{mc}$$

Obě strany kongruence i modul lze vynásobit týmž celým kladným číslem.

$$9) e \mid a \wedge e \mid b \wedge e \mid c \Rightarrow \frac{a}{e} \equiv \frac{b}{e} \pmod{\frac{m}{e}}$$

Obě strany kongruence i modul lze vydělit týmž celým kladným číslem různým od nuly.

$$10) a \equiv b \pmod{m} \wedge d \mid m \Rightarrow a \equiv b \pmod{d}$$

Platí-li kongruence podle modulu  $m$ , platí i podle modulu rovného libovolnému kladnému děliteli čísla  $m$ , většímu než jedna.

Eulerova věta:  $m \in \mathbb{N}, m > 1, a \in \mathbb{Z}, \text{NSD}(a, m) = 1$ , pak  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

Je-li speciálně  $p$  prvočíslo, které není dělitelem čísla  $a$ , pak platí  $a^{p-1} \equiv 1 \pmod{p}$  (tzv. malá Fermatova věta).