

## 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:  $a = bq + r, 0 \leq r < |b|$ , přičemž toto vyjádření je jednoznačné.

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

**Definice:** Necht'  $a, b \in \mathbf{C}, m \in \mathbf{N}, m \geq 2$ . Pak řekneme, že číslo  $a$  je kongruentní s číslem  $b$  podle modulu  $m$  (píšeme  $a \equiv b \pmod{m}$ ), právě když obě čísla  $a, b$  dávají při dělení modulem  $m$  stejný zbytek.

**Příklad:**  $9 \equiv 23 \pmod{7}, 19 \equiv 51 \pmod{8}, -26 \equiv 22 \pmod{8}$ , ale  $11 \not\equiv 19 \pmod{5}$ .

**Věta:** Relace kongruence je pro libovolný modul  $m$  relací ekvivalence na množině  $\mathbf{C}$  (je reflexivní, symetrická a tranzitivní).

**Definice:** Necht'  $m$  je pevné přirozené číslo větší než jedna. Označme

$$C_i = \{x \in \mathbf{C}; x \text{ dává po dělení číslem } m \text{ zbytek } i\}, \text{ pro } i = 0, 1, \dots, m-1.$$

Pak množina  $C_i$  se nazývá zbytková třída podle modulu  $m$ . Symbolem  $\mathbf{C}_m$  pak označíme množinu všech zbytkových tříd podle modulu  $m$ , tj.  $\mathbf{C}_m = \{C_0, C_1, \dots, C_{m-1}\}$ .

**Poznámka:** Protože při dělení číslem  $m$  jsou možné zbytky  $0, 1, \dots, m-1$ , je počet zbytkových tříd podle modulu  $m$  roven číslu  $m$ . Každá zbytková třída podle modulu  $m$  obsahuje nekonečně mnoho celých čísel, která dávají při dělení modulem  $m$  též zbytek (tzn. liší se o nějaký celočíselný násobek modulu  $m$ ).

**Příklad:** a)  $m = 4$

$$C_0 = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$C_1 = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$C_2 = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$C_3 = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

b)  $m = 5$

$$C_0 = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$C_1 = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$C_2 = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$C_3 = \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$C_4 = \{\dots, -6, -1, 4, 9, 14, \dots\}$$

**Věta:** Necht'  $m$  je pevné přirozené číslo větší než jedna. Pak množina  $\mathbf{C}_m$  všech zbytkových tříd podle modulu  $m$  tvoří rozklad množiny  $\mathbf{C}$  všech celých čísel.

**Poznámka:** Nyní se budeme zabývat binárními operacemi sčítání a násobení definovanými na množině  $\mathbf{C}_m$  pro různé moduly  $m$ . Obě operace na systému všech zbytkových tříd budeme chápat následujícím způsobem: Necht' např.  $m = 5$ . Zápis součtu  $C_3 + C_4 = C_2$  znamená, že sečtením libovolného celého čísla dávajícího při dělení pěti zbytek 3 s libovolným celým číslem dávajícím při dělení pěti zbytek 4 dostaneme vždy celé číslo, které při dělení pěti dává zbytek 2. Analogicky zápis spoje násobení  $C_2 \cdot C_4 = C_3$  znamená, že vynásobením libovolného celého čísla dávajícího při dělení pěti zbytek 2 s libovolným celým číslem dávajícím při dělení pěti zbytek 4 dostaneme vždy celé číslo, které při dělení pěti dává zbytek 3. Populárně řečeno,

výsledek sčítání či násobení zbytkových tříd podle modulu  $m$  získáme tak, že sečteme nebo vynásobíme indexy zbytkových tříd ze zadání úlohy, zjistíme zbytek součtu či součinu při dělení číslem  $m$  a tento zbytek je indexem zbytkové třídy hledaného součtu nebo součinu.

**Příklady:** a)  $m = 4 : C_1 + C_3 = C_0, C_2 + C_3 = C_1, C_2 \cdot C_3 = C_2, C_2 \cdot C_2 = C_0$ .  
 a)  $m = 3 : C_1 + C_2 = C_0, C_2 + C_2 = C_1, C_2 \cdot C_2 = C_1, C_0 \cdot C_2 = C_0$ .

**Poznámka:** V následujících tvrzeních uvedeme typy algebraických struktur definovaných na množinách zbytkových tříd. Tvrzení nebudeme dokazovat, vždy uvedeme jen ilustraci dané struktury pomocí tabulky. Kvůli zjednodušení zápisů rovněž budeme místo  $C_m$  uvádět pouze index  $m$  (zřejmě nebude moci dojít k nedorozumění). V předchozím příkladu a) tedy např.  $1 + 3 = 0, 2 + 3 = 1, 2 \cdot 3 = 2, 2 \cdot 2 = 0$ .

**Věta:** Nechť  $m$  je pevné přirozené číslo větší než jedna. Pak algebraická struktura  $(C_m, +)$  je komutativní grupa s neutrálním prvkem  $C_0$ .

Ilustrace  $(C_4, +)$ :

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

**Věta:** Nechť  $m$  je pevné přirozené číslo větší než jedna. Pak algebraická struktura  $(C_m, \cdot)$  je komutativní pologrupa s neutrálním prvkem  $C_1$  a agresivním prvkem  $C_0$ .

Ilustrace  $(C_4, \cdot)$ :

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Ilustrace  $(C_5, \cdot)$ :

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

**Poznámka:** Prohlédneme-li si pozorně obě tabulky v ilustraci předchozí věty, vidíme, že při operaci násobení zřejmě podstatně závisí na modulu. Odstraníme-li z obou těchto tabule první řádek a první sloupec, odpovídající třídě  $C_0$ , dostáváme následující tabulky struktur  $(C_4 - \{C_0\}, \cdot)$  a  $(C_5 - \{C_0\}, \cdot)$ :

Ilustrace  $(C_4 - \{C_0\}, \cdot)$ :

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Ilustrace  $(\mathbf{C}_5 - \{C_0\}, \cdot)$ :

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Struktura  $(\mathbf{C}_4 - \{C_0\}, \cdot)$  nyní již není ani grupoid, neboť obsahuje v tabulce prvek 0, který již nepatří do nosné množiny (není v záhlaví tabulky). Oproti tomu, algebraická struktura  $(\mathbf{C}_5 - \{C_0\}, \cdot)$  se ještě „zlepšila, nyní jde již o komutativní grupu. Který případ nastane, závisí na modulu.

**Věta:** Necht' modul  $m$  je prvočíslo. Pak algebraická struktura  $(\mathbf{C}_m - \{C_0\}, \cdot)$  je komutativní grupa. Je-li modul  $m$  číslo složené, pak  $(\mathbf{C}_m - \{C_0\}, \cdot)$  není ani grupoidem.

**Důsledek:** Necht' modul  $m$  je prvočíslo. Pak algebraická struktura se dvěma operacemi  $(\mathbf{C}_m - \{C_0\}, +, \cdot)$  je komutativní těleso.

**Poznámka:** Podle předchozího tvrzení není  $(\mathbf{C}_m - \{C_0\}, \cdot)$  pro složený modul ani grupoidem. Protože je však potřeba popsat i struktury zbytkových tříd se dvěma operacemi pro složený modul  $m$ , musíme nějak „popsat“ situaci nul vyskytujících se v tabulkách (např.  $(\mathbf{C}_4 - \{C_0\}, \cdot)$ ).

**Definice:** Necht' modul  $m$  je složené číslo, necht' pro dvě zbytkové třídy  $C_u, C_v$  podle modulu  $m$  platí  $C_u \neq C_0, C_v \neq C_0$ . Jestliže  $C_u \cdot C_v = C_0$ , pak obě třídy  $C_u, C_v$  se nazývají vlastní dělitelé nulového prvku  $C_0$ .

**Poznámka:** Definice vlastních dělitelů nulového prvku (stručně jen dělitelů nuly) je samozřejmě obecnější. Struktury zbytkových tříd však poskytují užitečnou ilustraci tohoto pojmu. Současně ve shodě s obecnou teorií algebraických struktur se dvěma operacemi umožňuje existence dělitelů nuly popsat i struktury  $(\mathbf{C}_m - \{C_0\}, +, \cdot)$  pro složený modul  $m$ .

**Věta:** Necht' modul  $m$  je složené číslo. Pak algebraická struktura se dvěma operacemi  $(\mathbf{C}_m - \{C_0\}, +, \cdot)$  je komutativní okruh, který nikdy není oborem integrity (obsahuje dělitele nuly).

**Příklad:** V okruhu  $(\mathbf{C}_4 - \{C_0\}, +, \cdot)$  je dělitelem nuly  $C_2$ ; v okruhu  $(\mathbf{C}_6 - \{C_0\}, +, \cdot)$  jsou dělitelé nuly  $C_2, C_3$ ; v okruhu  $(\mathbf{C}_8 - \{C_0\}, +, \cdot)$  jsou dělitelé nuly  $C_2, C_4, C_6$ .