Kongruence, rozklad na zbytkové třídy

Věta: Nechť 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 $-26 = (-8).4 + 6.$

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

Příklad: $9 \equiv 23$ (mod 7), $19 \equiv 51$ (mod 8), $-26 \equiv 22$ (mod 8), ale $11 \not\equiv 19$ (mod 5).

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

Definice: Nechť m je pevné přirozené číslo větší než jedna. Označme

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

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

Poznámka: Protože při dělení číslem m jsou možné zbytky $0, 1, \ldots, m-1,$ 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 týž zbytek (tzn. liší se o nějaký celočíselný násobek modulu m).

Příklad: a) $m = 4$

$$C_0 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$C_1 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$C_2 = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$C_3 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

b) $m = 5$

$$C_0 = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$C_1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$C_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$C_3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$C_4 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$

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

Poznámka: Nyní se budeme zabývat binárními operacemi sčítání a násobení definovanými na množině $\boldsymbol{C}_m$ pro různé moduly m. Obě operace na systému všech zbytkových tříd budeme chápat následujícím způsobem: Nechť 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 dělené pěti dává zbytek $2.$ Analogicky zápis spoje násobení $C_2 . C_4 = C_3$ 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 dělené 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) $m = 4 : C_1 + C_3 = C_0, C_2 + C_3 = C_1, C_2 . C_3 = C_2, C_2 . C_2 = C_0.$
a) $m = 3 : C_1 + C_2 = C_0, C_2 + C_2 = C_1, C_2 . C_2 = C_1, C_0 . C_2 = C_0.$

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. $1 + 3 = 0, 2 + 3 = 1, 2 . 3 = 2, 2 . 2 = 0.$

Věta: Nechť *m* je pevné přirozené číslo větší než jedna. Pak algebraická struktura $(\boldsymbol{C}_m , +)$ je komutativní grupa s neutrálním prvkem C_0.

Ilustrace $(\boldsymbol{C}_4 , +)$:

+	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 $(\boldsymbol{C}_m , .)$ je komutativní pologrupa s neutrálním prvkem C_1 a agresivním prvkem C_0.

Ilustrace $(\boldsymbol{C}_4 , .)$:

.	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 $(\boldsymbol{C}_5 , .)$:

.	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 tabulek první řádek a první sloupec, odpovídající třídě C_0, dostáváme následující tabulky struktur $(\boldsymbol{C}_4 - \{C_0\} , .)$ a $(\boldsymbol{C}_5 - \{C_0\} , .)$:

Ilustrace $(\boldsymbol{C}_4 - \{C_0\} , .)$:

.	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Ilustrace ($\boldsymbol{C}_5 - \{C_0\}$, .):

.	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 ($\boldsymbol{C}_4 - \{C_0\}$, .) 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 ($\boldsymbol{C}_5 - \{C_0\}$, .) se ještě „zlepšila, nyní jde již o komutativní grupu. Který případ nastane, závisí na modulu.

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

Důsledek: Nechť modul m je prvočíslo. Pak algebraická struktura se dvěma operacemi ($\boldsymbol{C}_m - \{C_0\}$,+, .) je komutativní těleso.

Poznámka: Podle předchozího tvrzení není ($\boldsymbol{C}_m - \{C_0\}$, .) 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. ($\boldsymbol{C}_4 - \{C_0\}$, .)).

Definice: Nechť modul m je složené číslo, nechť pro dvě zbytkové třídy C_u, C_v podle modulu m platí $C_u \neq C_0$, $C_v \neq C_0$. Jestliže $C_u . C_v = C_0$, 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 ($\boldsymbol{C}_m - \{C_0\}$,+, .) pro složený modul m.

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

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