ДИСКРЕТНЕ СТРУКТУРЕ 1

предавање 11 (12.12.2022.)
Тема: **Конгруенције**

Александра Костић

Катедра за алгебру и математичку логику
Математички факултет, Београд

Дефиниција

Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod{m}$ или $a \equiv_m b$ ако $m \mid (a - b)$.

Дефиниција

Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod{m}$ или $a \equiv_m b$ ако $m \mid (a - b)$.

Тврђење

Релација $\equiv_m$ је релација еквиваленције.

Доказ: на часу.

Дефиниција

Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod{m}$ или $a \equiv_m b$ ако $m \mid (a - b)$.

Тврђење

Релација $\equiv_m$ је релација еквиваленције.

Доказ: на часу.

Тврђење

Ако је $a \equiv a_1 \pmod{m}$ и $b \equiv b_1 \pmod{m}$ онда је

$$\begin{aligned} a + b &\equiv a_1 + b_1 \pmod{m} \\ a \cdot b &\equiv a_1 \cdot b_1 \pmod{m} \\ a^n &\equiv a_1^n \pmod{m}, \text{ за све } n \geq 1. \end{aligned}$$

Доказ: на часу.

Дефиниција

Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod{m}$ или $a \equiv_m b$ ако $m \mid (a - b)$.

Тврђење

Релација $\equiv_m$ је релација еквиваленције.

Доказ: на часу.

Тврђење

Ако је $a \equiv a_1 \pmod{m}$ и $b \equiv b_1 \pmod{m}$ онда је

$$\begin{aligned} a + b &\equiv a_1 + b_1 \pmod{m} \\ a \cdot b &\equiv a_1 \cdot b_1 \pmod{m} \\ a^n &\equiv a_1^n \pmod{m}, \text{ за све } n \geq 1. \end{aligned}$$

Доказ: на часу.

Тврђење

Нека $d \mid a, b, m$ и нека је $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Тада је $a \equiv_m b$ акко $a' \equiv_{m'} b'$

Доказ: на часу.

Једначине са конгруенцијама

Када има решења и шта су решења једначине $ax \equiv b \pmod{m}$, где су $a, b \in \mathbb{Z}$?

Једначине са конгруенцијама

Када има решења и шта су решења једначине $ax \equiv b \pmod{m}$, где су $a, b \in \mathbb{Z}$?

Вилсонова теорема

Ако је p прост број тада је $(p-1)! \equiv -1 \pmod{p}$.

Доказ: на часу.

Једначине са конгруенцијама

Када има решења и шта су решења једначине $ax \equiv b \pmod{m}$, где су $a, b \in \mathbb{Z}$?

Вилсонова теорема

Ако је p прост број тада је $(p-1)! \equiv -1 \pmod{p}$.

Доказ: на часу.

Кинеска теорема о остацима

Систем конгруенција

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\dots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

има решење ако нзд$(m_i, m_j) \mid (a_i - a_j)$ за све $i \neq j$. Ако је $\overline{x}$ неко решење тог система, онда је опште решење облика $x = \overline{x} + \text{нзс}(m_1, \dots m_k) \cdot t$, где је $t \in \mathbb{Z}$.

Доказ: на часу.