Дискретне структуре 1

предавање 7 (23.12.2025.)

Тема: ДИОФАНТОВЕ ЈЕДНАЧИНЕ.
ПРОСТИ БРОЈЕВИ. КОНГРУЕНЦИЈЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Диофантове једначине

дефиниција: Диофантова једначина је једначина са целобројним коефицијентима код које тражимо решења у скупу $\mathbb{Z}$.

Пример: Једначина $ax = b$, где су $a, b \in \mathbb{Z}$ и $a \neq 0$ је Диофантова једначина. Има решење у $\mathbb{Z}$ ако и само ако $a \mid b$.

Диофантове једначине

дефиниција: Диофантова једначина је једначина са целобројним коефицијентима код које тражимо решења у скупу $\mathbb{Z}$.

Пример: Једначина $ax = b$, где су $a, b \in \mathbb{Z}$ и $a \neq 0$ је Диофантова једначина. Има решење у $\mathbb{Z}$ ако и само ако $a \mid b$.

У наставку ћемо посматрати Диофантову једначину облика

$$ax + by = c.$$

теорема: Једначина $ax + by = c$, где је $a, b \neq 0$ има целобројна решења ако и само ако $\text{нзд}(a, b) \mid c$. У том случају опште решење ове једначине је

$$\begin{aligned} x &= p\frac{c}{\text{нзд}(a,b)} + \frac{b}{\text{нзд}(a,b)} \cdot t \\ y &= q\frac{c}{\text{нзд}(a,b)} - \frac{a}{\text{нзд}(a,b)} \cdot t, \qquad t \in \mathbb{Z}, \end{aligned}$$

где су p и q добијени помоћу (обрнутог) Еуклидовог алгоритма такви да важи $ap + bq = \text{нзд}(a, b)$.

Доказ: на часу.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

тврђење: Постоји бесконачно много простих бројева.
Доказ: на часу.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

тврђење: Постоји бесконачно много простих бројева.
Доказ: на часу.

тврђење: Ако је p прост број и $p \mid ab$, онда је $p \mid a$ или $p \mid b$.
Доказ: на часу.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

тврђење: Постоји бесконачно много простих бројева.
Доказ: на часу.

тврђење: Ако је p прост број и $p \mid ab$, онда је $p \mid a$ или $p \mid b$.
Доказ: на часу.

тврђење: Сваки природан број већи од 1 је прост или се може представити као производ простих бројева.
Доказ: на часу.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

тврђење: Постоји бесконачно много простих бројева.
Доказ: на часу.

тврђење: Ако је p прост број и $p \mid ab$, онда је $p \mid a$ или $p \mid b$.
Доказ: на часу.

тврђење: Сваки природан број већи од 1 је прост или се може представити као производ простих бројева.
Доказ: на часу.

теорема: (Основна теорема аритметике) Сваки природни број већи од 1 може се представити у облику производа простих бројева на јединствен начин (до на редослед простих фактора).
Доказ: на часу.

Конгруенције

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 $m \mid (a - b)$.

Конгруенције

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 $m \mid (a - b)$.

Релација $\equiv_m$ је релација еквиваленције.

Конгруенције

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 $m \mid (a - b)$.

Релација $\equiv_m$ је релација еквиваленције.

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.

Конгруенције

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 $m \mid (a - b)$.

Релација $\equiv_m$ је релација еквиваленције.

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.

Конгруенције

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 $m \mid (a - b)$.

Релација $\equiv_m$ је релација еквиваленције.

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.

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

Конгруенције

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 $m \mid (a-b)$.

Релација $\equiv_m$ је релација еквиваленције.

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.

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

теорема: (Вилсонова теорема) Ако је p прост број тада је

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказ: на часу.