ДИСКРЕТНЕ СТРУКТУРЕ 1

предавање 10 (5.12.2022.)
Тема: **Диофантове једначине. Прости бројеви.**

Александра Костић

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.

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.