ДИСКРЕТНЕ СТРУКТУРЕ 1

предавање 9 (21.11.2022.)
Тема: **Дељивост**

Александра Костић

Катедра за алгебру и математичку логику
Математички факултет, Београд

Дефиниција

Нека су $a, b \in \mathbb{N}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{N}$ тако да је $b = a \cdot c$.

Теорема (о Еуклидском дељењу)

Нека су $a, b \in \mathbb{N}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{N}$ који су јединствено одређени тако да је

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Доказ: на часу.

Дефиниција

Нека су $a, b \in \mathbb{N}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{N}$ тако да је $b = a \cdot c$.

Теорема (о Еуклидском дељењу)

Нека су $a, b \in \mathbb{N}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{N}$ који су јединствено одређени тако да је

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Доказ: на часу.

Дефиниција

Нека су $a, b \in \mathbb{Z}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{Z}$ тако да је $b = a \cdot c$.

Теорема

Нека су $a, b \in \mathbb{Z}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{Z}$ који су јединствено одређени тако да је

$$a = q \cdot b + r, \quad 0 \leq r < |b|.$$

Доказ: на часу.

Дефиниција

Број $d \in \mathbb{N}$ је заједнички делилац природних бројева a и b ако $d \mid a$ и $d \mid b$. За такав број d кажемо да је **највећи заједнички делилац** бројева a и b ако $d' \mid d$ за сваки заједнички делилац d' тих бројева. У том случају пишемо $d = \text{нзд}(a, b)$.

Дефиниција

Број $d \in \mathbb{N}$ је заједнички делилац природних бројева a и b ако $d \mid a$ и $d \mid b$. За такав број d кажемо да је **највећи заједнички делилац** бројева a и b ако $d' \mid d$ за сваки заједнички делилац d' тих бројева. У том случају пишемо $d = \text{нзд}(a, b)$.

Дефиниција

Број $s \in \mathbb{N}$ је заједнички садржалац природних бројева a и b ако $a \mid s$ и $b \mid s$. За такав број s кажемо да је **најмањи заједнички садржалац** бројева a и b ако $s \mid s'$ за сваки заједнички садржалац s' тих бројева. У том случају пишемо $s = \text{нзс}(a, b)$.

Дефиниција

Број $d \in \mathbb{N}$ је заједнички делилац природних бројева a и b ако $d \mid a$ и $d \mid b$. За такав број d кажемо да је **највећи заједнички делилац** бројева a и b ако $d' \mid d$ за сваки заједнички делилац d' тих бројева. У том случају пишемо $d = \text{нзд}(a, b)$.

Дефиниција

Број $s \in \mathbb{N}$ је заједнички садржалац природних бројева a и b ако $a \mid s$ и $b \mid s$. За такав број s кажемо да је **најмањи заједнички садржалац** бројева a и b ако $s \mid s'$ за сваки заједнички садржалац s' тих бројева. У том случају пишемо $s = \text{нзс}(a, b)$.

Тврђење

Ако је $a = bq + r$ онда је $\text{нзд}(a, b) = \text{нзд}(b, r)$.

Доказ: на часу.

Еуклидов алгоритам

Еуклидов алгоритам представља поступак за одређивање највећег заједничког делиоца датих целих бројева a и $b \neq 0$. Састоји се од узастопног примењивања теореме о еуклидском дељењу за целе бројеве. Прво, број a при дељењу са b даје неки количник q_1 и остатак r_1. Ако је $r_1 \neq 0$, можемо поделити b са r_1. У том случају добијамо количник q_2 и остатак r_2. Ако је $r_2 \neq 0$ настављамо поступак са бројевима r_1 и r_2. Поступак се завршава када добијемо остатак који је једнак нули. Алгоритам можемо представити шемом

$$
\begin{array}{rcll}
a & = & bq_1 + r_1, & 0 \leq r_1 < |b| \\
b & = & r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 & = & r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\
\vdots & & & \\
r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} & = & r_n q_{n+1} + r_{n+1}, & 0 \leq r_{n+1} < r_n
\end{array}
$$

Еуклидов алгоритам

Еуклидов алгоритам представља поступак за одређивање највећег заједничког делиоца датих целих бројева a и $b \neq 0$. Састоји се од узастопног примењивања теореме о еуклидском дељењу за целе бројеве. Прво, број a при дељењу са b даје неки количник q_1 и остатак r_1. Ако је $r_1 \neq 0$, можемо поделити b са r_1. У том случају добијамо количник q_2 и остатак r_2. Ако је $r_2 \neq 0$ настављамо поступак са бројевима r_1 и r_2. Поступак се завршава када добијемо остатак који је једнак нули. Алгоритам можемо представити шемом

$$\begin{array}{rcll}
a & = & bq_1 + r_1, & 0 \leq r_1 < |b| \\
b & = & r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 & = & r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\
\vdots & & & \\
r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} & = & r_n q_{n+1} + r_{n+1}, & 0 \leq r_{n+1} < r_n
\end{array}$$

Тврђење (Безуова релација)

Ако је нзд$(a, b) = d$, онда постоје бројеви x и y тако да $ax + by = d$.

Доказ: на часу.

Еуклидов алгоритам

$a, b \in \mathbb{Z}$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Матрицу M_{n+1} добијамо од матрице M_n једном од следећих трансформација:

- T1: множење врсте целим бројем и додавање другој врсти;
- T2: множење врсте са -1;
- T3: замена места врстама.

Еуклидов алгоритам

$a, b \in \mathbb{Z}$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Матрицу M_{n+1} добијамо од матрице M_n једном од следећих трансформација:

- T1: множење врсте целим бројем и додавање другој врсти;
- T2: множење врсте са -1;
- T3: замена места врстама.

Тврђење

Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $x = ap + bq$ и $y = as + bt$.

Доказ: на часу.

Еуклидов алгоритам

$a, b \in \mathbb{Z}$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Матрицу M_{n+1} добијамо од матрице M_n једном од следећих трансформација:

- T1: множење врсте целим бројем и додавање другој врсти;
- T2: множење врсте са -1;
- T3: замена места врстама.

Тврђење

Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $x = ap + bq$ и $y = as + bt$.

Доказ: на часу.

Тврђење

Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $\text{нзд}(a, b) = \text{нзд}(x, y)$.

Доказ: на часу.

Дефиниција

Бројеви $a, b \in \mathbb{Z}$ су **узајамно прости** ако је нзд$(a, b) = 1$.

Дефиниција

Бројеви $a, b \in \mathbb{Z}$ су **узајамно прости** ако је нзд$(a, b) = 1$.

Тврђење

Ако $a \mid bc$ и нзд$(a, b) = 1$ онда $a \mid c$.

Доказ: на часу.

Дефиниција

Бројеви $a, b \in \mathbb{Z}$ су **узајамно прости** ако је нзд$(a, b) = 1$.

Тврђење

Ако $a \mid bc$ и нзд$(a, b) = 1$ онда $a \mid c$.

Доказ: на часу.

Тврђење

Нека је $d =$ нзд(a, b), тада је нзс$(a, b) = \dfrac{|ab|}{d}$.

Доказ: на часу.