Алгебра 1 семестр ПИ,
Лекция, 09/17/21

Собрано 27 сентября 2021 г. в 19:09

Содержание

1.1. Делимость

Def. 1.1.1. $a \vdots b$ *или* $b|a \Leftrightarrow \exists q : a = b \cdot q, b \neq 0$

Свойства:

1. Рефлексивность. $a \vdots a, a \neq 0$
2. Антисимметричность на $\mathbb{N}$. $a \vdots b, b \vdots a \Rightarrow a = b$
3. Транзитивность. $a \vdots b, \vdots c \Rightarrow a \vdots c$
4. $a|b, a|c \Rightarrow a|(b \pm c)$.

   Доказательство. $b = a \cdot q_1, c = aq_2 \Rightarrow b \pm c = aq_1 \pm aq_2 = a(q_1 \pm q_2)$ ■
5. $a|b \Rightarrow \forall c \to a|bc$
6. Пусть $a|b_i, i = 1, ..., n, a|(b_1 + ... + b_n + c) \Rightarrow a|c$

   Доказательство. $b_1 + ... + b_n + c = aq, aq_1 + aq_2 + ... + aq_n + c = aq \Rightarrow c = a(q - q_1 - ... - q_n)$ $\Rightarrow a|c$ ■
7. $a|b \Rightarrow \forall k \neq 0 \to ka|kb$
8. $ka|kb \Rightarrow a|b$

Теорема 1.1.2 (О делении с остатком)**.**

$$\forall a \wedge \forall b > 0 \ \exists! q, r, 0 \leqslant r < b : a = bq + r$$

Def. 1.1.3. *a - делимое, b - делитель, q - частное (неполное частное), r - остаток*

Доказательство. $\exists$-ние. Рассмотрим $a - bq$. Выберем q так, чтобы $a - bq > 0$ было наименьшим. Положим $r = a - bq \geqslant 0 \Rightarrow a = bq + r$. По выбору $q \to a - b(q + 1) < 0 \Rightarrow a < b(q + 1) \Rightarrow$ $r = a - bq < b(q + 1) - bq = b$.
Единственность. Преположим, что $a = bq_1 + r_1 = bq_2 + r_2, 0 \leqslant r_1, r_2 < b$

$$|r_1 - r_2| < b, bq_1 + r_1 = bq_2 + r_2 \Rightarrow b(q_1 - q_2) = r_2 - r_1 \Rightarrow |b(q_1 - q_2)| \geqslant b$$

Но $|r_1 - r_2| < b$ - противоречие. ■

1.2. Наибольший общий делитель

Def. 1.2.1. *Общим делителем* $a_1, a_2, ..., a_n$ *называется* $d : d|a_i, i = 1, ..., n$.

Def. 1.2.2. *Наибольший общий делитель* $a_1, a_2, ..., a_n$ *называется* d *такое, что*

1. $d > 0$
2. $d|a_i, i = 1, ..., n$
3. *если* $d'|a_i, i = 1, ..., n$, *то* $d'|d$

Обозначается $\gcd(a_1, a_2, ..., a_n) = (a_1, a_2, ..., a_n)$

Замечание 1.2.3. По определению $\gcd(0, 0) = 0$. $a \neq 0$, то $\gcd(a, 0) = 0$

Свойства:

1. $b|a \Rightarrow (a, b) = b$

   Доказательство. Докажем, что множество делителей (a, b) совпадает с множество делителей b.

$$d|(a, b) \Rightarrow d|b$$

$$d|b \Rightarrow d|a(\text{по транзитивности}) \Rightarrow d|(a, b)$$

■

2. $a = bq + c \Rightarrow (a, b) = (b, c)$
3.

   Алгоритм 1.2.4 (Алгоритм Евклида).

$$a = bq_1 + r_1, 0 \leqslant r_1 < b$$

$$b = r_1q_1 + r_2, 0 \leqslant r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, 0 \leqslant r_3 < r_2$$

$$...$$

$$r_{n-2} = r_{n-1}q_n + r_n, 0 \leqslant r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}$$

   Теорема 1.2.5. $r_n = \gcd(a, b)$

   Доказательство. $r_1 > r_2 > r_3 > ... \geqslant 0 \Rightarrow \exists r_{n+1} = 0$. $r_n|r_{n-1}$.

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = ... = (r_2, r_1) = (b, r_1) = (a, b)$$

■

4. $(ma, mb) = m \cdot (a, b)$
5. $d|a, d|b \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$

   Доказательство. $(a, b) = \left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot \left(\frac{a}{d}, \frac{b}{d}\right)$ ■
6. $(a, b) = 1 \Rightarrow (a, bc) = (a, c)$

   Доказательство. Докажем, что $(a, bc)|(a, c)$

   $$(a, bc)|a, (a, bc)|ac, (a, bc)|bc \Rightarrow (a, bc)|(ac, bc) \Rightarrow (a, bc)|(a, b) \cdot c = c \Rightarrow (a, bc)|(a, c)$$

   Теперь докажем, что $(a, c)|(a, bc)$

   $$(a, c)|a, (a, c)|c \Rightarrow (a, c)|bc \Rightarrow (a, c)|(a, bc) \Rightarrow (a, bc) = (a, c)$$

   ■
7. $(a, b) = 1, b|ac \Rightarrow b|c$

   Доказательство.

   $$b|bc, b|ac \Rightarrow b|(bc, ac) = c$$

   ■
8. $(a, b) = (a - b, b)$

Теорема 1.2.6 (Линейное представление НОД)**.**

$$(a, b) = d \Rightarrow \exists u, v : u \cdot a + v \cdot b = d$$

Доказательство. Из алгоритма Евклида:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \Rightarrow d = r_n = r_{n-2} - r_{n-1} \cdot q_n$$

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} \Rightarrow d = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1})q_n$$

Из следующей строки выражаем r_{n-2} и т.д. $\Rightarrow$ останутся a и $b \Rightarrow d = u \cdot a + v \cdot b$ ■