Алгебра 1

Igor Engel

Определение 0.1. $a \vdots b \equiv \exists x \in \mathbb{Z} \quad a = bx$

1 Свойства

Лемма 1.0.1. $\forall a, b, c \in \mathbb{Z} \quad a \vdots b \wedge b \vdots c \implies a \vdots c$

Доказательство.

$$b = cx_1.$$

$$a = bx_2 = c(x_1 x_2).$$

□

Лемма 1.0.2. $\forall a_1, b_1, a_2, b_2 \in \mathbb{Z} \quad a_1 \vdots b_1 \wedge a_2 \vdots b_2 \implies a_1 a_2 \vdots b_1 b_2$

Доказательство.

$$a_1 = b_1 x_1.$$

$$a_2 = b_2 x_2.$$

$$a_1 a_2 = (b_1 b_2)(x_1 x_2).$$

□

Лемма 1.0.3. $\forall a, b, c \in \mathbb{Z} \quad a \vdots c \wedge b \vdots c \implies (a + b) \vdots c$

Доказательство.

$$a = cx_1.$$

$$b = cx_2.$$

$$a + b = cx_1 + cx_2 = c(x_1 + x_2).$$

□

Лемма 1.0.4. $\forall a, b \in \mathbb{Z} \quad a \vdots b \implies \pm a \vdots \pm b$

Доказательство.

$$a = bx = -b \cdot (-x).$$

$$-a = b \cdot (-x) = -bx.$$

□

Лемма 1.0.5. $\forall a \in \mathbb{Z} \quad a \vdots a$

Доказательство.

$$a = a(1).$$

□

Лемма 1.0.6. $\forall a \in \mathbb{Z} \quad a \vdots 1$

Доказательство.

$$a = 1(a).$$

□

Лемма 1.0.7. $\forall a, b \in \mathbb{Z} \quad a \vdots b \wedge b \vdots a \implies a = \pm b$

Доказательство.

$$a = bx_1.$$

$$b = ax_2 = bx_1x_2 \implies x_1x_2 = 1.$$

$$x_1x_2 = 1 \implies x_1 = x_2 = \pm 1.$$

$$x_1 = \pm 1 \implies a = \pm b.$$

□

2 Теоремы

Теорема 2.1 (Теорема о делении с остатком)**.**

$$\forall a \in \mathbb{Z} \quad \forall b \in \mathbb{Z} \setminus \{0\} \quad \exists! q, r \in \mathbb{Z} \quad a = bq + r \wedge r \in [0; |b|)\,.$$

Доказательство. Докажем для $a, b \geq 0$ существование по индукции: Для $a < b$ утверждение тривиально:

$$a = b_0 + a.$$

Из того, что разложение существует для a следует существование для $a + b$:

$$a = bq + r \implies a + b = b\,(q + 1) + r.$$

Докажем единственность. Предположим что существуют два разложения:

$$a = bq + r = bq' + r'.$$

Вычтем одно из другого:

$$b(q - q') + (r - r') = 0 \implies (r' - r) = b(q - q').$$

Если предположить что $q \neq q'$

$$\begin{cases} |b(q - q')| \geq |B| \\ |(r' - r)| < |B| \end{cases}$$

Что невозможно. Значит $q = q'$:

$$(r' - r) = b(q - q') = b(q - q) = 0 \implies r = r'.$$

Значит, второе разложение равно первому. □

3 НОД

Определение 3.1. Общий делитель чисел a и b - такое число d, что $a \vdots d$ и $b \vdots d$

Определение 3.2. $d = (a,b) = \text{НОД}(a,\, b) \equiv \forall d' \in \mathbb{Z} \quad a \vdots d \wedge b \vdots d \wedge ((a \vdots d' \wedge b \vdots d') \implies d \vdots d')$

Лемма 3.2.1. Пусть $a, b \in \mathbb{Z}$ и $a \neq 0$ или $b \neq 0$.

$$A \equiv \{z \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} \quad z = ax + by\}.$$

Тогда,

$$\exists d \in \mathbb{N} \quad A = d \cdot \mathbb{Z} = \{z \in \mathbb{Z} \mid \exists x \in \mathbb{Z} \quad z = dx\}.$$

$$d = (a,b) = \min_{d' \in A \cup \mathbb{N}} d'.$$

Доказательство. $d = \min\limits_{d' \in A \cup \mathbb{N}} d'$ и $A \subseteq d \cdot \mathbb{Z}$. Предположим $a, b \neq 0$

$$z = ax + by = dq + r \quad q \in \mathbb{Z} \quad r \in [0, d)\,.$$

$$d = ax' + by'.$$

$$r = z - dq = ax + by - aqx' - bqy' = a(x - qx') + b(y - qy') \implies r \in A \implies r \notin \mathbb{N} \implies r = 0.$$

$$r = 0 \implies z \vdots d \implies z \in d \cdot \mathbb{Z}.$$

□

Доказательство. $A = d \cdot \mathbb{Z}$:

$$\forall z \in d \cdot \mathbb{Z} \quad \exists c \in \mathbb{Z} \quad z = dc.$$

$$d = ax + by \implies z = dc = acx + bcy \implies z \in A \implies d \cdot \mathbb{Z} \subseteq A.$$

$$A \subseteq d \cdot \mathbb{Z} \wedge d \cdot \mathbb{Z} \subseteq A \implies A = d \cdot \mathbb{Z}.$$

□

Доказательство. d - общий делитель a и b

$$a = a(1) + b(0) \implies a \in A \implies a \vdots d.$$

$$b = a(0) + b(1) \implies b \in A \implies b \vdots d.$$

□

Доказательство. $d = (a,b)$
Пусть d' - общий делитель a и b.

$$d \in A \implies d = ax + by.$$

$$a \vdots d' \implies (ax) \vdots d'.$$

$$b \vdots d' \implies (by) \vdots d'.$$

$$(ax) \vdots d' \wedge (by) \vdots d' \implies (ax + by) \vdots d' \implies d \vdots d' \implies d = (a,b)\,.$$

□

4 Простые числа

Определение 4.1. Назовём множество простых чисел $\mathbb{P}$, тогда

$$\mathbb{P} \equiv \{p \in \mathbb{N} \setminus \{1\} \mid \forall d \in \mathbb{N} \quad p \,\vdots\, d \implies d \in \{1, p\}\}.$$

Лемма 4.1.1.

$$p \in \mathbb{P} \equiv \forall a, b \in \mathbb{Z} \quad (ab) \,\vdots\, p \implies \left[\begin{array}{l} a \,\vdots\, p \\ b \,\vdots\, p \end{array}\right.$$

Доказательство. Необходимость.

$$d = (a, p) \in \{1, p\}.$$

$$d = p \implies a \,\vdots\, p.$$

$$d = 1 \implies \exists x, y \in \mathbb{Z} \quad 1 = ax + py \implies b = abx + pby.$$

$$(ab) \,\vdots\, p \implies (abx) \,\vdots\, p.$$

$$p \,\vdots\, p \implies (pby) \,\vdots\, p.$$

$$(abx) \,\vdots\, p \wedge (pby) \,\vdots\, p \implies (abx + pby) \,\vdots\, p \implies b \,\vdots\, p.$$ □

Доказательство. Достаточность.
Если $\exists n, m \in \mathbb{Z} \cup (1; p) \quad nm = p$, то

$$\left[\begin{array}{l} n \,\vdots\, p \\ m \,\vdots\, p \end{array}\right. .$$

но $n, m < p$, так-что таких n, m не существует. □

5 ОТА

Теорема 5.1 (Основная теорема арифметики)**.** $\forall a \in \mathbb{Z} \setminus \{0\} \exists! \epsilon \in \{-1, 1\}, p_1 \dots p_k \in \mathbb{P} \quad \epsilon \prod\limits_{i=1}^{k} p_1 i$
Примечание: $p_1 \dots p_k$ единственно с точностью до перестановки

Доказательство. Существование.

$$a > 0 \implies \epsilon = 1.$$

$$a < 0 \implies \epsilon = 1.$$

$$|a| \in \mathbb{P} \implies k = 1, p = a.$$

$$|a| \notin \mathbb{P} \implies \exists n, m \in \mathbb{Z} \cup [1; a) \quad nm = a.$$ □

Доказательство. Единственность. Если $a = \epsilon \prod_{i=1}^{k} p_i = \epsilon' \prod\limits_{i=1}^{n} q_i$

Доказательство. $\epsilon = \epsilon'$

$$a > 0 \implies \epsilon = \epsilon' = 1.$$

$$a < 0 \implies \epsilon = \epsilon' = -1.$$ □

Предположим, что $k \leq n$. (Для $k \geq n$ доказательство симметрично)

Доказательство. $p_1 \dots p_k = q_1 \dots q_k$
Для $k = 0$ утверждение тривиально.
Для $k > 0$:

$$\prod_{i=1}^{k} p_i \,\vdots\, q_1 \wedge q_1 \in \mathbb{P} \implies \exists i p_i \,\vdots\, q_1.$$

Тогда, на это p_i можно скоратить, и получить разложение с $k' = k - 1$ □

Доказательство. $k = n$
После сокращения всех p_i, $k = 0$. Значит,

$$a' = \prod_{i=1}^{0} p_i = 0 = \prod_{i=1}^{n-k} q_i \implies n - k = 0 \implies n = k.$$ □

Лемма 5.1.1.

$$\forall a, b \in Z \setminus \{0\}.$$

$$a = \epsilon_a \prod_{i=1}^{k} p_i^{\alpha_i}.$$

$$b = e_b \prod_{n=1}^{k} p_i^{\beta_i}.$$

$$a \,\vdots\, b \equiv \forall i \in [1, k] \quad \alpha_i \geq \beta_i.$$

Доказательство. Достаточность.

$$c = \epsilon' \prod_{i=1}^{k} p_i^{\alpha_i - \beta_i} \implies bc = a \implies a \,\vdots\, b.$$ □

Доказательство. Необходимость.

$$a \,\vdots\, b \implies a = bc \implies c = \epsilon' \prod_{i=1}^{k} p_i^{\gamma_i} \implies \alpha_i = \beta_i + \gamma_i \implies \alpha_i \geq \beta_i.$$ □

Лемма 5.1.2.

$$\forall a, b \in Z \setminus \{0\}.$$

$$a = \epsilon_a \prod_{i=1}^{k} p_i^{\alpha_i}.$$

$$b = e_b \prod_{n=1}^{k} p_i^{\beta_i}.$$

$$\phi_i = \min\left(\alpha_i, \beta_i\right).$$

$$d = (a, b) = \prod_{i=1}^{k} p_i^{\phi_i}.$$

Доказательство.

$$\forall i \in [1, k) \quad \phi_i \leq \alpha_i, \beta_i \implies a \,\vdots\, d, b \,\vdots\, d.$$

$$\forall d' \in Z, a \,\vdots\, d', b \,\vdots\, d' \quad d' = \prod_{i=1}^{k} p_i^{\gamma_i}.$$

$$\forall i \in [1, k) \quad \gamma_i \leq \alpha_i, \beta_i \implies \gamma_i \leq \phi_i \implies d \,\vdots\, d'.$$ □