**Московский физико-технический институт**
**Физтех-школа прикладной математики и информатики**

# ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

II СЕМЕСТР

Лектор: *Райгородский*

$h\nu$

Автор: *Киселев Николай*
*Репозиторий на Github*

весна 2025

# Содержание

# 1 ОТА

Эту часть конспекта для вас затеха: Иван Бирюков

**Теорема 1.1.**

*1)* $\forall n > 1\ \exists!$ *его представление в виде*

$$n = p_1 p_2 \dots p_s$$

*Комментарий:* $p_1, p_2, \dots, p_s$ *- простые числа, единственность с точностью до порядка множителей*

*2)* $p_i$ *- i-ое простое число Тогда* $\forall n\ \exists!\ (\alpha_1, \alpha_2, \dots, \alpha_n)$*:*

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

**Следствие.** $\nu_p(n)$ - max степень вхождения $p$ в $n \Longrightarrow n\ \not\vdots p^{\nu_p(n)+1}$

**Сейчас мы приведем несколько доказательств этой теоремы**

## 1.1 Первое доказательство (не было доведено)

*Доказательство.* Найдем существование разложения по индукции по n:

База: $n = 2$. Переход: $n = ab \to \left(p_{a_1}^{\alpha_{a_1}} p_{a_2}^{\alpha_{a_2}} \dots p_{a_s}^{\alpha_{a_s}}\right) \cdot \left(p_{b_1}^{\alpha_{b_1}} p_{b_2}^{\alpha_{b_2}} \dots p_{b_k}^{\alpha_{b_k}}\right)$ или $n$ - простое

Осталось понять единственность.

Пойдем от противного: пусть $\exists\ min\ n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_k$

Для простоты упорядочим простые числа в обоих разложениях.

Если $p_1 = q_1$, то у числа $\frac{n}{p_1}$ есть 2 разложения. Значит, $p_1 \neq q_1 \to n \geqslant p_1 p_2 \geqslant p_1^2$

Аналогично получается $n \geqslant q_1^2 \to n \geqslant max(p_1^2, q_1^2) \geqslant q_1(p_1 + 2) > q_1 p_1 + 1$

Рассмотрим число $x = n - p_1 q_1$. Оно меньше $n$ и больше 1, а тогда у него есть единственное разложение на простые сомножители $\tau_1, \tau_2, \dots, \tau_m$:

$x = p_1(p_2 \dots p_s - q_1) = q_1(q_2 \dots q_k - p_1) = \tau_1 \dots \tau_m$, в наборе $\tau : \tau_1 \leqslant \dots \leqslant p_1 \leqslant q_1 \leqslant \tau_m$ □

## 1.2 Второе доказательство

**Лемма 1.1** (Евклида)**.** *$p$ - простое. Тогда $mn \vdots p \to m \vdots p$ или $n \vdots p$*

**Лемма 1.2** (Евклида 2.0)**.** $(m, k) = 1, mn \vdots k \to n \vdots k$

$2 \Longrightarrow 1$ :. $k = p, m\ \not\vdots p \to (m, p) = 1 \to n \vdots k$ □

*Доказательство.* Докажем единственность по лемме Евклида:

$n = p_1 \underbrace{\dots p_s}_{m} = q_1 \dots q_l$

По лемме Евклида $p_1 = q_1$ или $m \vdots q_1$. Повторяя процедуру, получим, что $p_i = q_1$, сократим на него и повторим алгоритм. □

**Докажем теперь лемму Евклида 2.0**

*Доказательство.* По линейному представлению НОДа $\exists x\ \exists y:\ mx + ky = 1$

$$mx + ny = 1 \to \underbrace{mn}_{\vdots k}\, x + \underbrace{k}_{\vdots k}\, ny = n \to n \vdots k$$

□

**Доказательство этой же леммы через идеалы:**

**Определение 1.1.** I - идеал в $\mathbb{Z}$, если:

1. $\forall a, b\ \in I : a + b = I$
2. $\forall a\ \in I\ \forall b\ \in \mathbb{Z} : ab \in I$

*Доказательство.* Зафиксируем $m$ и определим $I_m = \{a \mid ma \vdots p\} \to n$, $p$ *лежат в идеале*

**Лемма 1.3.** *Пусть $d$ - минимальное положительное число в $I$*
*Тогда $I = \{cd \mid c \in \mathbb{Z}\}$*

*Следует из деления элемента с остатком* □

А тогда $d = 1$ или $d = p$. Во втором случае $n \vdots p$, в первом - $m \vdots p$