(Будет только в задачах) Элементарная теория чисел: делимость, деление с остатком, вычеты. Свойства арифметических действий с вычетами. Наибольший общий делитель. Взаимно простые числа. Обратимость вычетов. Малая теорема Ферма. Теорема Эйлера. Расширенный алгоритм Евклида.

# 1 Основные понятия теории чисел

1. Делимость

2. Деление с остатком

   **Определение 1.1.** *Будем говорить, что целое число $a$ делится на целое ненулевое число $b$ с остатком $r$, если:*

   $$\exists q \in \mathbb{Z} : a = bq + r, 0 \leq r < |b|$$

3. Простые числа

   **Определение 1.2.** *Целое число $p$ называется простым, если оно не имеет никаких натуральных делителей, кроме $1$ и $p$.*

4. Наибольший общий делитель

   **Определение 1.3.** *Наибольшим общим делителем двух целых чисел $a$ и $b$ будем называть такое целое число $d$ (обозначается $НОД(a, b)$), что выполнено следующее:*

   *(a)* $a = da', a' \in \mathbb{Z}$ *и* $b = db', b' \in \mathbb{Z}$

   *(b)* $d$ *– наибольший такой натуральный (эквивалентно тому, что любой общий делитель $a$ и $b$ является также делителем $d$)*

5. Взаимная простота

   **Определение 1.4.** *Целые числа $a$ и $b$ называют взаимно простыми, если $НОД(a, b) = 1$.*

   **Теорема 1.1.** *Пусть $a, b \in \mathbb{Z} : НОД(a, b) = 1$ и $ac \vdots b$. Тогда $c \vdots b$.*

6. Наименьшее общее кратное

   **Определение 1.5.** *Наибольшим общим кратным двух целых чисел $a$ и $b$ будем называть такое наименьшее натуральное число $m$, что $m \vdots a$ и $m \vdots b$.*

   **Теорема 1.2.** $НОК(a, b) \cdot НОД(a, b) = ab$.

7. Основная теорема арифметики

   **Теорема 1.3.** *Любое натуральное число $m$ единственным образом представимо в виде произведения его простых делителей, то есть:*

   $$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

   *где $p_i$ – простые, $\alpha_i \in \mathbb{N}$.*

# 2 Арифметика остатков

**Определение 2.1.** *Будем говорить, что целое число $a$ сравнимо с целым числом $b$ по модулю $m$, и записывать это $a \equiv b \pmod m$, если $(a - b) \vdots m$*

**Определение 2.2.** *Множество всех чисел, сравнимых с $a$ по модулю $m$, называется классом вычетов по модулю $m$, и обозначается $[a]_m$*

**Определение 2.3.** *Любое число класса вычетов по модулю $m$ называется вычетом по модулю $m$.*

**Теорема 2.1.**

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{cases} \implies \begin{cases} a + c \equiv b + d \ (mod\ m) \\ ac \equiv bd \ (mod\ m) \end{cases}$$

**Теорема 2.2.**

$$\begin{cases} ac \equiv bc \ (mod\ m) \\ НОД(c, m) = 1 \end{cases} \implies a \equiv b \ (mod\ m)$$

*Доказательство.*

$$\begin{cases} ac \equiv bc \ (mod\ m) \\ \text{НОД}(c, m) = 1 \end{cases} \iff \begin{cases} ac - bc \vdots m \\ \text{НОД}(c, m) = 1 \end{cases} \iff \begin{cases} c(a - b) \vdots m \\ \text{НОД}(c, m) = 1 \end{cases} \implies (a - b) \vdots m$$

□

# 3 Обратимость остатков

**Теорема 3.1.**

$$\forall a, b \in \mathbb{Z}\ \exists x, y \in \mathbb{Z} : НОД(a, b) = ax + by$$

*Доказательство.* Требуемое очевидно следует из алгоритма Евклида, так как в любой момент времени НОД берется от линейной комбинации чисел $a$ и $b$. □

## 3.1 Существование обратного по простому модулю

**Теорема 3.2.** *Уравнение $a \cdot x \equiv 1 \ (mod\ p)$, где $p$ –простое, разрешимо в целых числах тогда и только тогда, когда $a \not\vdots p$.*

*Первое доказательство.* Есть лишь два случая:

1. $a \vdots p$. Тогда очевидно, что решений нет.

2. $a \not\vdots p$. Тогда $\text{НОД}(a, p) = 1 \implies \exists x, y \in \mathbb{Z} : ax + py = 1$. Рассмотрим полученное равенство по модулю $p$:

   $$ax + py \equiv 1 \ (mod\ p) \implies ax \equiv 1 \ (mod\ p)$$

   Итого в этом случае получаем, что уравнение разрешимо в целых числах, что и требовалось.

□

*Второе доказательство.* Если $a \vdots p$, то очевидно решений нет. Далее $a \not\vdots p$. Рассмотрим множество всевозможных ненулевых остатков по модулю $p$:

$$A = \{1, 2, \ldots, p - 1\}$$

Умножим каждый из элементов множества $A$ на $a$. Получим следующий ряд:

$$a \cdot 1, a \cdot 2, \ldots, a \cdot (p - 1)$$

Заметим, что все элементы этого ряда попарно несравнимы по модулю $p$. Действительно, если от противного существуют такие $i$ и $j$ из ряда, что $a \cdot i \equiv a \cdot j \ (mod\ p)$, то $a(i - j) \vdots p \implies i = j$, откуда получаем противоречие. Значит элементы этого ряда суть перестановка элементов множества $A$ по модулю $p$. Но тогда среди них существует число, равное 1 по модулю $p$, что и требовалось. □

# 4 Малая теорема Ферма

**Теорема 4.1.** *Пусть $a \not\vdots p$ и $p$ – простое. Тогда $a^{p-1} \equiv 1 \ (mod\ p)$*

*Доказательство.* Перемножим все элементы из множества $A$ и все элементы ряда из предыдущего доказательства. Так как в ряду все элементы попарно несравнимы по модулю $p$, и их ровно $p$ штук, то выполнено:

$$1 \cdot 2 \ldots (p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \ldots (a \cdot (p-1)) \ (mod\ p)$$

Тогда:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod\ p)$$

Но $(p-1)!$ взаимнопросто с $p$. Значит:

$$a^{p-1} \equiv 1 \ (mod\ p),$$

что и требовалось. □

# 5 Теорема Эйлера

**Определение 5.1.** *Пусть функция $\varphi\colon \mathbb{N} \to \mathbb{N}$ такая, что $\forall n \in \mathbb{N} \hookrightarrow \varphi(n)$ есть количество таких натуральных чисел $m$, что $m$ взаимнопросто с $n$ и $m \leq n$. Такую функцию будем называть функцией Эйлера.*

**Теорема 5.1** (Эйлера)**.** *Пусть НОД$(a, m) = 1$. Тогда:*

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

*Доказательство.* Рассмотрим множество всех остатков по модулю $m$, которые взаимнопросты с $m$:

$$A = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$$

Теперь также рассмотрим следующий ряд:

$$a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}$$

По аналогии с доказательством малой теоремы Ферма получим, что все числа этого ряда попарно несравнимы по модулю $m$, а значит элементы ряда суть перестановка элементов множества $A$ по модулю $m$. Тогда имеем:

$$(ar_1)(ar_2) \ldots (ar_{\varphi(m)}) \equiv r_1 r_2 \ldots r_{\varphi(m)} \ (mod\ m)$$

Так как $r_1 r_2 \ldots r_{\varphi(m)}$ взаимно просто с $m$, то окончательно:

$$a^{\varphi(m)} \equiv 1 \ (mod\ m),$$

что и требовалось. □

# 6 Расширенный алгоритм Евклида

## 6.1 Немного воспоминаний

Обычный алгоритм Евклида основывается на следующем замечании:

**Лемма 6.1.** *НОД$(a, b)$ = НОД$(a - b, b)$ (полагаем $a \geq b$)*

В соответствии с этим, обычный алгоритм Евклида делает некоторую последовательность делений, то есть, полагая $a_0 = a, a_1 = b$, выполнено (до тех пор, пока $a_{i+1} \neq 0$):

$$a_{i-1} = a_i q_i + a_{i+1}, \quad 0 \leq a_{i+1} < |a_i|$$

Пусть $a_{t+1}$ – последний ненулевой остаток. Тогда НОД$(a_0, a_1) = a_{t+1}$.

### 6.2 Расширяем возможности

Расширенный алгоритм Евклида позволяет представить $d = \text{НОД}(a, b)$ в виде линейной комбинации $a$ и $b$, то есть найти такие $x, y \in \mathbb{Z}$, что:

$$d = ax + by$$

**Алгоритм.** Положим

$$x_t = -1, \quad y_t = q_{t+1},$$

где $q_{t+1}$ – последнее частное. Положим также

$$x_i = y_{i+1}, \quad y_i = x_{i+1} - q_{i+1}y_{i+1}$$

Легко показать по индукции, что на каждом шаге выполнено:

$$x_i a_i + y_i a_{i+1} = \text{НОД}(a_0, a_1)$$

Тогда ясно, что в тот момент времени, когда алгоритм дойдёт до $x_0$ и $y_0$, будет выполнено:

$$x_0 a_0 + y_0 a_1 = \text{НОД}(a_0, a_1)$$

Легко видеть, что получили искомые коэффициенты разложения.