

# Модульная арифметика. Сравнимость по модулю, полная и приведенная системы вычетов. Теоремы Эйлера и Ферма

ceagest

## 1 Сравнимость по модулю

**Определение 1.1.** Будем рассматривать целые числа в связи с их остатками от деления на данное целое положительное  $m$ , которое назовём модулем. Каждому целому числу соответствует определённый остаток от деления его на  $m$ . Если двум целым  $a$  и  $b$  соответствует один и тот же остаток  $r$ , то они называются равноостаточными по модулю  $m$  или сравнимыми по модулю  $m$ . Сравнимость чисел  $a$  и  $b$  по модулю  $m$  записывается так:

$$a \equiv b \pmod{m}$$

**Теорема 1.1.** Следующие утверждения эквивалентны:

1.  $a \equiv b \pmod{m}$
2.  $(a - b) : m$
3.  $a = b + mt$ , где  $t \in \mathbb{Z}$

*Доказательство.*  $1 \iff 2$  очевидно из определения.  $2 \iff 3$  легко получается из того, что  $(a - b) : m \iff a - b = mt$ , где  $t \in \mathbb{Z}$ .  $\square$

### 1.1 Свойства сравнений по модулю

1. Два числа, сравнимые с третьим, сравнимы между собой.
2. Сравнения можно почленно складывать.
3. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, переменяя знак на обратный.
4. Сравнения можно почленно перемножать.
5. Обе части сравнения можно возвести в одну степень.
6. К каждой части сравнения можно добавить число, кратное модулю.
7. Обе части сравнения можно умножить на одно и то же целое.
8. Обе части сравнения и их модуль можно разделить на их общий делитель.
9. Обе части сравнения и их модуль можно умножить на одно и то же целое.
10. Обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.
11. Если сравнение имеет место по модулю  $m$ , то оно имеет место и по модулю  $d$  — любому делителю числа  $m$ .
12. Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число.
13. Если  $a \equiv b \pmod{m}$ , то  $(a, m) = (b, m)$ .

*Доказательство.* 1. Очевидно из определения.

2. Пусть  $a_1, a_2$  и  $b_1, b_2$  таковы, что  $\forall i \in \{1, 2\} \quad \hookrightarrow \quad a_i \equiv b_i \pmod{m}$ . Тогда из теоремы 1.1:

$$\begin{cases} a_1 = b_1 + mt_1 \\ a_2 = b_2 + mt_2 \end{cases}$$

Отсюда получаем, что  $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2) \iff a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

3. Пусть  $a + b \equiv c \pmod{m} \iff (a + b) - c : m \iff a - (c - b) : m \iff a \equiv c - b \pmod{m}$

4. Пусть  $a_1, a_2$  и  $b_1, b_2$  таковы, что  $\forall i \in \{1, 2\} \quad \hookrightarrow \quad a_i \equiv b_i \pmod{m}$ . Тогда из теоремы 1.1:

$$\begin{cases} a_1 = b_1 + mt_1 \\ a_2 = b_2 + mt_2 \end{cases}$$

Отсюда получаем, что  $a_1 a_2 = (b_1 + mt_1)(b_2 + mt_2) = b_1 b_2 + m(b_1 + b_2 + mt_1 t_2) \iff a_1 a_2 \equiv b_1 b_2 \pmod{m}$

5. Лёгкое следствие свойства 4.

6. Лёгкое следствие свойства 2.

7. Лёгкое следствие свойства 4.

8. Пусть  $a \equiv b \pmod{m}, a = a_1 d, b = b_1 d, m = m_1 d$ . Тогда  $a = b + mt \iff a_1 d = b_1 d + m_1 d t \iff a_1 = b_1 + m_1 t \iff a_1 \equiv b_1 \pmod{m}$

9. Доказательство аналогично пункту 8

10. Легкое следствие из того, что  $a \equiv b \pmod{m} \iff (a - b) : m$

11. Легкое следствие из того, что  $a \equiv b \pmod{m} \iff (a - b) : m$

12. Легкое следствие из того, что  $a \equiv b \pmod{m} \iff a = b + mt$

13. Легкое следствие из того, что  $a \equiv b \pmod{m} \iff a = b + mt$

□

## 2 Полная система вычетов

**Определение 2.1.** Числа, сравнимые по модулю  $m$ , образуют класс чисел по модулю  $m$ . Всем числам класса соответствует один и тот же остаток  $r \implies$  все числа класса по модулю  $m$  имеют вид  $mq + r$ , где  $q \in \mathbb{Z}$ . Соответственно  $m$  различным значениям  $r$  имеем  $m$  классов чисел по модулю  $m$ .

**Определение 2.2.** Любое число класса называется вычетом по модулю  $m$  по отношению ко всем числам того же класса. Вычет, получаемый при  $q = 0$ , равный самому остатку  $r$ , называется наименьшим неотрицательным вычетом. Вычет  $p$ , самый малый по абсолютной величине, называется абсолютно наименьшим вычетом.

**Определение 2.3.** Взяв от каждого класса по одному вычету, получим полную систему вычетов по модулю  $m$ .

**Теорема 2.1.** Любые  $m$  чисел, попарно не сравнимые по модулю  $m$ , образуют полную систему вычетов по модулю  $m$ .

*Доказательство.* Действительно, будучи не сравнимыми, эти числа принадлежат к различным классам, а так как их  $m$ , то есть столько же, сколько и классов, то в каждый класс попадет по одному числу. □

**Теорема 2.2.** Если  $(a, m) = 1$  и  $x$  пробегает полную систему вычетов по модулю  $m$ , то  $ax + b$ , где  $b \in \mathbb{Z}$ , тоже пробегает полную систему вычетов по модулю  $m$ .

*Доказательство.* Действительно, чисел  $ax + b$  будет столько же, сколько и чисел  $x$ , то есть  $m$  штук. Предположим, что  $x_1 \not\equiv x_2$  и  $ax_1 + b \equiv ax_2 + b \pmod{m} \iff a(x_1 - x_2) : m$ . Но  $(a, m) = 1 \implies (x_1 - x_2) : m \iff x_1 \equiv x_2 \pmod{m}$ . Получаем противоречие. Итого, числа  $ax + b$  попарно не сравнимы по модулю  $m$ , и при этом их ровно  $m$  штук. Значит по теореме 2.1 получаем требуемое. □

### 3 Приведённая система вычетов

**Определение 3.1.** Числа одного и того же класса по модулю  $m$  имеют с модулем один и тот же НОД. Особенно важны классы, для которых этот НОД равен единице, то есть классы, содержащие числа, взаимно простые с модулем. Взяв от каждого такого класса по одному вычету, получим приведенную систему вычетов по модулю  $m$ .

**Теорема 3.1.** Любые  $\varphi(m)$  чисел, попарно несравнимых по модулю  $m$  и взаимно простых с модулем, образуют приведенную систему вычетов по модулю  $m$ .

*Доказательство.* Действительно, будучи несравнимыми и взаимно простыми с модулем, эти числа тем самым принадлежат к различным классам, содержащим числа, взаимно простые с модулем  $a$ , так как их  $\varphi(m)$ , то в каждый класс попадет ровно по одному числу.  $\square$

### 4 Теорема Эйлера

**Теорема 4.1.** Пусть  $m > 1, m \in \mathbb{Z}, (a, m) = 1$ . Тогда:

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

*Доказательство.* Пусть  $x$  пробегает приведенную систему вычетов, составленную из наименьших неотрицательных вычетов:

$$r_1, r_2, \dots, r_k, k = \varphi(m)$$

Тогда наименьшие неотрицательные вычеты чисел  $ax$ , будут проходить ту же систему, возможно, в другом порядке  $\rho_1, \rho_2, \dots, \rho_k$ . Перемножим почленно сравнения вида  $ar_i \equiv \rho_i \pmod{m} \quad \forall i \in \{1, 2, \dots, k\}$  и сократим на  $r_1 r_2 \dots r_k = \rho_1 \rho_2 \dots \rho_k$ . Получим требуемое.  $\square$

### 5 Теорема Ферма

**Теорема 5.1.** Пусть  $p$  – простое и  $a$  не делится на  $p$ . Тогда:

$$a^{p-1} \equiv 1 \pmod{p}$$

*Доказательство.* Лёгкое следствие из теоремы Эйлера  $\square$