

## Теория делимости

Будем рассматривать  $\mathbb{Z}$ .

**Определение.**  $q \in \mathbb{Z}$  делит  $n \in \mathbb{Z}$ , если  $\exists t \in \mathbb{Z} : n = qt$

*Обозначение.*  $q \mid n, n \div q$ .

*Пример.*  $m^5 - m \div 5$

*Решение. Случай 1:*  $m = 5k$

Тривиально.

**Случай 2:**  $m = 5k + 1$

$$\begin{aligned}(5k + 1)^5 - (5k + 1) &= (5k + 1)((5k + 1)^2 - 1)((5k + 1)^2 + 1) \\ &= (5k + 1)(5k + 1 - 1)(5k + 1 + 1)((5k + 1)^2 + 1) \div 5\end{aligned}$$

**Случай 3:**  $m = 5k + 2$

$$\begin{aligned}(5k + 2)^5 - (5k + 2) &= (5k + 2)(5k + 2 - 1)(5k + 3)((5k + 2)^2 + 1) \\ &= \dots (25k + 20k + 4 + 1) \div 5\end{aligned}$$

Остальные случаи опущены.

□

**Определение.**  $n, m \in \mathbb{Z}, d : n \div d, m \div d$

$d$  называется **общим делителем**  $n, m$ .

**Определение.**  $n, m$  **взаимно простые**, если:

$$n \div d, m \div d \Rightarrow d = \pm 1$$

**Теорема 1.**  $n \div ab \Leftrightarrow n \div a, n \div b$  и  $a, b$  взаимно простые.

*Упражнение.*

$$m(m + 1)(2m + 1) \div 6$$

Решение.

$$m(m+1) \div 2$$

Докажем  $m(m+1)(2m+1) \div 3$

**Случай 1:**  $m = 3k$

Тривиально.

**Случай 2:**  $m = 3k + 1$

$$2m + 1 = 6k + 3 \div 3$$

**Случай 3:**  $m = 3k + 2$

Тривиально.

□

Упражнение.  $\forall n \exists k : n^2 + (n+1)^2 = 4k + 1$

Решение.

$$n^2 + (n+1)^2 = 4k + 1$$

$$2n^2 + 2n + 1 = 4k + 1$$

$$2n^2 + 2n = 4k$$

$$n^2 + n = 2k$$

$$\underbrace{n(n+1)} = 2k$$

$$\div 2$$

□

Упражнение.

$$n^3(n^2+3) \div 4$$

Решение. Для чётных  $n$   $n^3 \div 4$ . Для  $n = 2k + 1$   $(2k+1)^2 + 3 = 4k^2 + 4k + 4 \div 4$ .

□

**Определение.**  $a, b \in \mathbb{Z}$  сравнимы по модулю  $n$ , если  $a - b \div n$ .

Обозначение.  $a \equiv b \pmod{n}$

Пример.  $4 \equiv 1 \pmod{3}, 8 \equiv 2 \pmod{3}, 151 \equiv 11 \pmod{10}$

$$\left. \begin{array}{l} a - c \vdots n \\ b - d \vdots n \end{array} \right\} \Rightarrow \begin{cases} a = nk + c \\ b = nj + d \end{cases}$$

$$\triangleleft ab = \underbrace{n^2kj + nkd + njc + cd}_{\vdots n}$$

$$1. \ a \equiv c \pmod{n}, b \equiv d \pmod{n} \Rightarrow a + b \equiv c + d \pmod{n}, ab \equiv cd \pmod{n}$$

Упражнение.  $a^7 - a + 56 \vdots 7$

Решение. Случай 1:  $a \equiv 0$

$$0 + 0 + 56 \equiv 0$$

Случай 2:  $a \equiv 1$

$$1 - 1 + 56 \equiv 0$$

Случай 3:  $a \equiv 2$

$$128 - 2 + 56 \equiv 70 + 56 \equiv 0$$

Остальные случаи опущены. □

Упражнение.

$$m^2 + n^2 \vdots 7 \Rightarrow n \vdots 7, m \vdots 7$$

Решение.

$m \equiv$	$m^2 \equiv$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

□

**Определение.**  $\{a_1 \dots a_n\}$  называется **полной системой вычетов**  $\pmod{n}$ , если  $\forall a \in \mathbb{Z} \exists j : a \equiv a_j \pmod{n}$

**Теорема 2.**

- $\{a_1 \dots a_n\}$  — полная система вычетов  $\bmod n$
- $k$  взаимно просто с  $n$

Тогда  $\{ka_1 \dots ka_n\}$  — полная система вычетов  $\bmod n$ .