# Элементы теории чисел

grznych

10 декабря 2019 г.

## Содержание

# 1 Основные понятия и теоремы

*Целые числа* включают в себя числа натуральные ($\mathbb{N}$), противоположные к натуральным (отрицательные) и ноль. Как обычно, множество целых чисел будем обозначать символом $\mathbb{Z}$, а принадлежность числа $x$ множеству целых чисел будем обозначать выражением $x \in \mathbb{Z}$. Все числа здесь и далее считаются целыми, если не сказано обратное.

Основные свойства целых чисел и операций (сложение, вычитание, умножение, деление) над ними будем считать уже известными. Таким образом, если $a, b \in \mathbb{Z}$, то $a + b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$, $ab \in \mathbb{Z}$, однако $\frac{a}{b}$ может быть как целым, так и не целым.

**Замечание.** Напомним, что

$$|x| = \begin{cases} x, & \text{если } x \geqslant 0; \\ -x, & \text{если } x < 0. \end{cases}$$

$$\operatorname{sgn}(x) = \begin{cases} 1, & \text{если } x > 0; \\ 0, & \text{если } x = 0; \\ -1, & \text{если } x < 0. \end{cases}$$

Проверьте, что $x = \operatorname{sgn}(x)|x|$ и $|x| = \operatorname{sgn}(x)x$.

Докажите, что $|a| < x$ тогда и только тогда, когда $-x < a < x$.

## 1.1 Деление с остатком

**Определение** (делимость)**.** *$a$ делится на $b$ ($b$ делит $a$)*, если существует такое целое число $q$, что $a = bq$.

**Обозначение.** $a \vdots b$ ($b \mid a$).

**Пример 1.** Любое целое число $a$ является делителем 0, так как $0 = 0 \times a$. Из этого же следует, что на ноль делится только ноль.

**Лемма 1.** Если $a \vdots b$ и $a \neq 0$, то $|a| \geqslant |b|$.

*Доказательство.* Действительно, из $a = bq$ и $a \neq 0$ следует, что $|q| \geqslant 1$. Значит, $|a| = |b||q| \geqslant |b|$. □

**Лемма 2.** Если $a \vdots b$ и $|a| < |b|$, то $a = 0$.

*Доказательство.* Так как $|a| = |b||q| < |b|$, то, сократив неравенство на $|b|$, получим $|q| < 1$, то есть $q = 0$. Значит, $a = 0$. □

**Лемма 3.** $a \vdots b$ и $b \vdots a$ тогда и только тогда, когда $|a| = |b|$.

*Доказательство.* Если $a \neq 0$, то $b \neq 0$. Тогда из ***леммы 1*** следует, что $|a| \geqslant |b|$ и $|b| \geqslant |a|$, то есть $|a| = |b|$.

Если $a = 0$, то с необходимостью $b = 0$, то есть $|a| = |b|$. □

**Лемма 4.** Если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.

*Доказательство.* Из $a = ba_1$ и $b = cb_1$ следует, что $a = c(b_1a_1)$. □

**Лемма 5.** Если $a \vdots c$ и $b \vdots c$, то $(a \pm b) \vdots c$.

*Доказательство.* Действительно, из $a = ca_1$ и $b = cb_1$ следует, что $a \pm b = c(a_1 \pm b_1)$. □

**Замечание.** Аналогично доказывается, что если $a \vdots c$ и $b \vdots c$, то $(ab) \vdots c$.

**Лемма 6.** $a \vdots b$ тогда и только тогда, когда $ac \vdots bc$ и $c \neq 0$.

*Доказательство.* Если $a \vdots b$, то $a = bq$. Умножив это равенство на $c$, получим $ac = bcq$, а значит, $ac \vdots bc$.

Обратно. Если $ac \vdots bc$, то $ac = bcq$. Сократив это равенство на $c$, получим $a = bq$, а значит, $a \vdots b$. □

**Теорема 1** (о делении с остатком)**.** Пусть $a, b \in \mathbb{Z}$ и $b \neq 0$. Тогда существует единственная пара чисел $(q, r)$ такая, что $a = bq + r$, где $0 \leqslant r < |b|$.

*Доказательство.* **Существование.** По ***принципу Архимеда*** для $|b| > 0$ существует такое число $p$, что

$$|b|p \leqslant a < |b|(p+1).$$

Пусть $q = \operatorname{sgn}(b)p$ и $r = a - bq = a - |b|p$, тогда из предыдущих неравенств следует

$$0 \leqslant a - |b|p < |b|,$$

то есть $0 \leqslant r < |b|$ и $a = bq + r$.

**Единственность.** Действительно, предположим, что существует ещё одна пара чисел $(q_1, r_1)$ такая, что $a = bq_1 + r_1$, где $0 \leqslant r_1 < |b|$. Отсюда получаем, что $bq + r = bq_1 + r_1$, то есть

$$r - r_1 = b(q_1 - q). \tag{1}$$

Значит, $(r - r_1) \vdots b$. Так как $-|b| < -r_1$ и $r < |b|$, получаем

$$r - |b| < r - r_1 < |b| - r_1. \tag{2}$$

С другой стороны, так как $0 \leqslant r$ и $-r_1 \leqslant 0$, находим $-|b| \leqslant r - |b|$ и $|b| - r_1 \leqslant |b|$. И, объединив эти неравенства с неравенствами (2), получаем

$$-|b| \leqslant r - |b| < r - r_1 < |b| - r_1 \leqslant |b|,$$

то есть $-|b| < r - r_1 < |b|$, а значит, $|r - r_1| < |b|$.

Тогда из ***леммы 2*** получаем $r - r_1 = 0$, то есть $r = r_1$.

В итоге из равенства (1) получаем $0 = b(q_1 - q)$ и, так как $b \neq 0$, $q_1 - q = 0$, то есть $q = q_1$, что и требовалось. □

**Определение.** Число $q$ называется *неполным частным*, а число $r$ — *остатком* от деления $a$ на $b$.

## 1.2 Наибольший общий делитель

**Обозначение.** Здесь и далее $\mathbb{N}_n = \{\, 1, \ldots, n \,\}$.

**Определение.** Пусть среди чисел $a_1, \ldots, a_n$ есть хотя бы одно не равное нулю. Тогда $d \in \mathbb{N}$ называется *общим делителем* чисел $a_1, \ldots, a_n$, если $a_i \vdots d$ для любого $i \in \mathbb{N}_n$. Наибольшее число из общих делителей этих чисел называется *наибольшим общим делителем* и обозначается $(a_1, \ldots, a_n)$.

**Обозначение.** Здесь и далее

$$\mathcal{D}_{a_1,\ldots,a_n} = \{\, d \in \mathbb{N} \mid \forall i \in \mathbb{N}_n \quad a_i \vdots d \,\} -$$

множество, состоящее из всех общих делителей чисел $a_1, \ldots, a_n$. Тогда $\mathcal{D}_a = \{\, d \in \mathbb{N} \mid a \vdots d \,\}$ — множество, состоящее из всех делителей числа $a$.

**Определение.** Числа $a_1, \ldots, a_n$ называются *взаимно простыми*, если $(a_1, \ldots, a_n) = 1$.

**Утверждение 1.** Если $a \vdots b$, то $\mathcal{D}_{a,b} = \mathcal{D}_b$, в частности $(a, b) = |b|$.

**Замечание.** Чтобы доказать равенство двух множеств, сперва нужно показать, что $\mathcal{D}_{a,b} \subseteq \mathcal{D}_b$, а затем, что $\mathcal{D}_b \subseteq \mathcal{D}_{a,b}$.

*Доказательство.* Покажем, что $\mathcal{D}_{a,b} \subseteq \mathcal{D}_b$. Если $d \in \mathcal{D}_{a,b}$, то по определению $a \vdots d$ и $b \vdots d$, а значит, $d \in \mathcal{D}_b$.

Покажем теперь, что $\mathcal{D}_b \subseteq \mathcal{D}_{a,b}$. Действительно, если $d \in \mathcal{D}_b$, то $b \vdots d$. И, так как по условию $a \vdots b$, из ***леммы 4*** получаем, что $a \vdots d$, то есть $d \in \mathcal{D}_{a,b}$.

Так как $\mathcal{D}_{a,b} = \mathcal{D}_b$, наибольшие элементы этих множеств равны, но из ***леммы 1*** следует, что $|b|$ и есть наибольший элемент множества $\mathcal{D}_b$ (***проверьте!***). Значит, $(a, b) = |b|$. □

**Утверждение 2.** Если $a = bq + c$, то $\mathcal{D}_{a,b} = \mathcal{D}_{b,c}$, в частности $(a, b) = (b, c)$.

*Доказательство.* Действительно, если $d \in \mathcal{D}_{a,b}$, то $a \vdots d$ и $b \vdots d$, а значит, по ***лемме 5*** $c \vdots d$, то есть $d \in \mathcal{D}_{b,c}$. В итоге получаем $\mathcal{D}_{a,b} \subseteq \mathcal{D}_{b,c}$. Аналогично доказывается, что $\mathcal{D}_{b,c} \subseteq \mathcal{D}_{a,b}$. Значит, $\mathcal{D}_{a,b} = \mathcal{D}_{b,c}$.

Так как множества общих делителей равны, равны будут и наибольшие в них элементы, то есть $(a, b) = (b, c)$. □

**Теорема 2** (алгоритм Евклида)**.** Пусть $a, b \in \mathbb{Z}$ и $b \neq 0$. Тогда, используя ***теорему о делении с остатком***, получим ряд равенств

$$\begin{array}{rcll} a & = & bq + r_1, & 0 < r_1 < |b|; \\ b & = & r_1 q_1 + r_2, & 0 < r_2 < r_1; \\ r_1 & = & r_2 q_2 + r_3, & 0 < r_3 < r_2; \\ \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} & = & r_n q_n. & \end{array} \tag{3}$$

При этом $\mathcal{D}_{a,b} = \mathcal{D}_{r_n}$ и $(a, b) = r_n$.

*Доказательство.* Так как $|b| > r_1 > r_2 > r_3 > \cdots \geqslant 0$, с необходимостью на каком-то шаге алгоритма возникнет остаток $r_{n+1} = 0$, то есть алгоритм закончится.

Используя ***утверждения 1 и 2***, получаем

$$\mathcal{D}_{a,b} = \mathcal{D}_{b,r_1} = \mathcal{D}_{r_1,r_2} = \cdots = \mathcal{D}_{r_{n-2},r_{n-1}} = \mathcal{D}_{r_{n-1},r_n} = \mathcal{D}_{r_n},$$

а значит, $(a, b) = r_n$. □

**Следствие 2.1.** $\mathcal{D}_{a,b} = \mathcal{D}_{(a,b)}$.

**Замечание.** Отсюда очевидно, что наибольший общий делитель делится на любой общий делитель.

**Следствие 2.2** (соотношение Безу)**.** Существуют такие числа $u$ и $v$, что

$$\boxed{au + bv = (a, b).}$$

*Доказательство.* Действительно, из равенств (3) получаем

$$\begin{aligned} (a, b) = r_n &= r_{n-2} - r_{n-1} q_{n-1}; \\ r_{n-1} &= r_{n-3} - r_{n-2} q_{n-2}; \\ &\vdots \\ r_3 &= r_1 - r_2 q_2; \\ r_2 &= b - r_1 q_1; \\ r_1 &= a - bq. \end{aligned}$$

Заменяя в первом равенстве сначала $r_{n-1}$, затем $r_{n-2}$, $\ldots$, $r_2$, $r_1$ соответствующими равенствами и упрощая выражение, найдём числа $u$ и $v$ такие, что $(a, b) = r_n = au + bv$. $\square$

**Пример 2.** Найдём такие $u$ и $v$, что $(-78)u + (-66)v = (-78, -66)$. С помощью алгоритма Евклида получаем следующие равенства:

$$\begin{aligned}
(-78) &= (-66) \times 2 + 54, && 0 < 54 < |-66| = 66;\\
(-66) &= 54 \times (-2) + 42, && 0 < 42 < 54;\\
54 &= 42 + 12, && 0 < 12 < 42;\\
42 &= 12 \times 3 + 6, && 0 < 6 < 12;\\
12 &= 6 \times 2.
\end{aligned}$$

Таким образом, $(-78, -66) = 6$. Теперь выразим остатки из полученных равенств:

$$\begin{aligned}
6 &= 42 + 12 \times (-3);\\
12 &= 54 + 42 \times (-1);\\
42 &= (-66) + 54 \times 2;\\
54 &= (-78) + (-66) \times (-2).
\end{aligned}$$

Начнём последовательно в первом равенстве заменять остатки:

$$\begin{aligned}
6 &= 42 + \boxed{12} \times (-3) =\\
&= 42 + \underline{(54 + 42 \times (-1))} \times (-3) =\\
&= 54 \times (-3) + \boxed{42} \times 4 =\\
&= 54 \times (-3) + \underline{((-66) + 54 \times 2)} \times 4 =\\
&= (-66) \times 4 + \boxed{54} \times 5 =\\
&= (-66) \times 4 + \underline{((-78) + (-66) \times (-2))} \times 5 =\\
&= \boxed{(-78)} \times 5 + \boxed{(-66)} \times (-6).
\end{aligned}$$

Значит, $u = 5$ и $v = -6$.

**Утверждение 3.** Пусть $m \in \mathbb{N}$, тогда $(am, bm) = (a, b)m$.

*Доказательство.* Действительно, умножив соотношения (3) почленно на $m$, получим новые соотношения, где вместо $a$, $b$, $r_1$, $r_2$, $\ldots$, $r_{n-1}$, $r_n$ будут числа

$$am,\ \ bm,\ \ r_1m,\ \ r_2m,\ \ \ldots,\ \ r_{n-1}m,\ \ r_nm,$$

а значит, $(am, bm) = (a, b)m$. □

**Утверждение 4.** Пусть $d \in \mathcal{D}_{a,b}$, тогда $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$, в частности

$$\boxed{\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.}$$

*Доказательство.* Действительно, из ***утверждения 3*** следует

$$(a, b) = \left(\frac{a}{d}d, \frac{b}{d}d\right) = \left(\frac{a}{d}, \frac{b}{d}\right)d,$$

что и требовалось.

Последнее утверждение получается, если в качестве $d$ взять $(a, b)$. □

**Утверждение 5.** Если $(a, b) = 1$, то $(ac, b) = (c, b)$.

**Замечание.** Докажем равенство с помощью ***леммы 3***, то есть сначала докажем, что $(c, b) \vdots (ac, b)$, а затем, что $(ac, b) \vdots (c, b)$.

*Доказательство.* Действительно, так как $ac \vdots (ac, b)$ и $b \vdots (ac, b)$, получаем $bc \vdots (ac, b)$. Значит, используя ***следствие 2.1***,

$$(ac, b) \in \mathcal{D}_{ac,bc} = \mathcal{D}_{(ac,bc)}.$$

Отсюда и из ***утверждения 3*** следует $|c| = (ac, bc) \vdots (ac, b)$. Значит, $(ac, b) \in \mathcal{D}_{c,b} = \mathcal{D}_{(c,b)}$, то есть $(c, b) \vdots (ac, b)$.

Так как $b \vdots (c, b)$ и $c \vdots (c, b)$, получаем $ac \vdots (c, b)$. Значит,

$$(c, b) \in \mathcal{D}_{ac,b} = \mathcal{D}_{(ac,b)},$$

то есть $(ac, b) \vdots (c, b)$.

В конечном итоге из ***леммы 3*** следует, что $(ac, b) = (c, b)$. □

**Замечание.** В каком месте доказательства используется $(a, b) = 1$?

**Утверждение 6.** Если $(a, b) = 1$ и $ac \vdots b$, то $c \vdots b$.

*Доказательство.* Действительно, из ***утверждения 1*** следует

$$(ac, b) = |b|.$$

С другой стороны, из ***утверждения 5*** следует $|b| = (ac, b) = (c, b)$, а значит, $c \vdots b$. □

**Пример 3.** $(5 \times 14) \vdots 7$, значит, $14 \vdots 7$, так как $(5, 7) = 1$.

**Пример 4.** $(8 \times 9) \vdots 6$, но $9 \not\vdots 6$, так как $(8, 6) \neq 1$.

## 1.3 Наименьшее общее кратное

**Определение.** Пусть среди чисел $a_1, \ldots, a_n$ есть хотя бы одно не равное нулю. Тогда $m \in \mathbb{N}$ называется *общим кратным* чисел $a_1, \ldots, a_n$, если $m \vdots a_i$ для любого $i \in \mathbb{N}_n$. Наименьшее число из общих кратных этих чисел называется *наименьшим общим кратным* и обозначается $[a_1, \ldots, a_n]$.

**Обозначение.** Здесь и далее

$$\mathcal{M}_{a_1,\ldots,a_n} = \{\, m \in \mathbb{N} \mid \forall i \in \mathbb{N}_n \quad m \vdots a_i \,\} —$$

множество, состоящее из всех общих кратных чисел $a_1, \ldots, a_n$. Тогда $\mathcal{M}_a = \{\, m \in \mathbb{N} \mid m \vdots a \,\}$ — множество, состоящее из всех кратных числа $a$.

**Утверждение 7.** Пусть $d = (a, b)$, тогда число $m$ — общее кратное чисел $a$ и $b$, если и только если оно представимо в виде

$$m = \frac{|ab|}{d} t, \tag{4}$$

где $t \in \mathbb{N}$.

**Замечание.** Выше делается два утверждения (***«если и только если»!***):

1. любое общее кратное представимо в виде (4);
2. любое число вида (4) является общим кратным.

Поэтому доказать нужно оба этих утверждения.

*Доказательство.* Докажем сперва первый пункт ***замечания***. Пусть $|a| = da_1$, $|b| = db_1$ и $m$ — общее кратное $a$ и $b$.

Из ***утверждения 4*** следует $(a_1, b_1) = 1$. Так как $m \vdots a$, $m = |a|k$. С другой стороны, из $m \vdots b$ следует $|a|k \vdots |b|$, а значит, $da_1k \vdots db_1$. Из ***леммы 6*** получаем $a_1k \vdots b_1$. В конечном итоге с помощью ***утверждения 6*** получаем $k \vdots b_1$, то есть $k = b_1t$, где $t \in \mathbb{N}$ (***почему?***).

В итоге получаем

$$dm = d|a|k = d|a|b_1t = |ab|t,$$

то есть $m = \frac{|ab|}{d}t$, что и требовалось.

Докажем теперь второй пункт ***замечания***. Пусть $m = \frac{|ab|}{d}t$, тогда $m = |a|b_1t$, то есть $m \vdots a$. Аналогично показывается, что $m \vdots b$. Значит, $m$ — общее кратное $a$ и $b$. □

**Теорема 3** (формула для наименьшего общего кратного)**.**

$$\boxed{[a, b] = \frac{|ab|}{(a, b)}.} \tag{5}$$

*Доказательство.* Так как $m = \frac{|ab|}{d}t$ — общее кратное $a$ и $b$, наименьшее общее кратное $[a, b]$ получается при $t = 1$. В итоге получаем формулу $[a, b] = \frac{|ab|}{(a,b)}$. □

**Следствие 3.1.** Пусть $m$ — общее кратное чисел $a$ и $b$, тогда

$$m = [a, b]t,$$

где $t \in \mathbb{N}$.

**Замечание.** Отсюда очевидно, что любое общее кратное делится на наименьшее общее кратное.

*Доказательство.* Следует из ***формул 4 и 5***. □

**Утверждение 8.** $\mathcal{M}_{a,b} = \mathcal{M}_{[a,b]}$.

*Доказательство.* Действительно, если $m \in \mathcal{M}_{a,b}$, то из ***следствия 3.1*** получаем $m \vdots [a,b]$, то есть $m \in \mathcal{M}_{[a,b]}$.

Обратно, если $m \in \mathcal{M}_{[a,b]}$, то $m \vdots [a,b]$. И, так как $[a,b] \vdots a$, из ***леммы 4*** получаем $m \vdots a$. Аналогично показывается, что $m \vdots b$. В итоге $m \in \mathcal{M}_{a,b}$. □

# 2 Сравнение по модулю

**Определение.** Пусть $m \in \mathbb{N}$, тогда числа $a$ и $b$ называются *сравнимыми по модулю* $m$, если их остатки от деления на $m$ равны, при этом число $m$ называется *модулем*. Сравнимость чисел $a$ и $b$ по модулю $m$ записывается так:

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

**Замечание.** Очевидно, что если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

**Утверждение 9.** $a \equiv b \pmod{m}$ в том и только в том случае, когда $(a - b) \vdots m$.

*Доказательство.* Действительно, из $a \equiv b \pmod{m}$ следует, что $a = mq + r$ и $b = mp + r$, где $0 \leqslant r < m$. Тогда

$$a - b = mq + r - (mp + r) = m(q - p),$$

то есть $(a - b) \vdots m$.

Обратно, пусть $(a - b) \vdots m$ и $b = mp + r$, где $0 \leqslant r < m$. Покажем, что остатки от деления $a$ и $b$ на $m$ равны. Действительно, из $(a-b) \vdots m$ следует $a - b = mt$, то есть

$$a = mt + mp + r = m(t + p) + r,$$

а это и означает, что $a \equiv b \pmod{m}$. □

**Замечание.** Покажите, что $a \equiv b \pmod{m}$ тогда и только тогда, когда $a = b + mt$, где $t \in \mathbb{Z}$.

## 2.1 Свойства сравнений

**Утверждение 10.** Если $a_1 \equiv b_1 \pmod{m}$ и $a_2 \equiv b_2 \pmod{m}$, то $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

*Доказательство.* Действительно, из $(a_1 - b_1) \vdots m$ и $(a_2 - b_2) \vdots m$ следует

$$((a_1 + a_2) - (b_1 + b_2)) = ((a_1 - b_1) + (a_2 - b_2)) \vdots m,$$

а значит, $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$. □

**Утверждение 11.** Если $a_1 \equiv b_1 \pmod{m}$ и $a_2 \equiv b_2 \pmod{m}$, то $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

*Доказательство.* Действительно,

$$a_1 a_2 - b_1 b_2 = (a_1 a_2 - a_1 b_2) + (a_1 b_2 - b_1 b_2) = a_1(a_2 - b_2) + b_2(a_1 - b_1)$$

и, так как $(a_1 - b_1) \vdots m$, $(a_2 - b_2) \vdots m$,

$$(a_1 a_2 - b_1 b_2) = (a_1(a_2 - b_2) + b_2(a_1 - b_1)) \vdots m,$$

а значит, $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. □

**Замечание.** Покажите, что если $a \equiv b \pmod{m}$, то $a^k \equiv b^k \pmod{m}$ для любого $k \in \mathbb{N}$.

**Утверждение 12.** $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$ тогда и только тогда, когда

$$a \equiv b \pmod{[m_1, m_2]}.$$

*Доказательство.* Действительно, из ***утверждения 8*** следует (***проверьте!***), что $(a - b) \vdots m_1$ и $(a - b) \vdots m_2$ тогда и только тогда, когда $(a - b) \vdots [m_1, m_2]$. □

**Пример 5.** Вычислим остаток $13^{16} - 2^{55} \times 5^{15}$ от деления на 3.

$$13^{16} - 2^{55} \times 5^{15} \equiv 1^{16} - (-1)^{55} \times (-1)^{15} = 1 - 1 = 0 \pmod{3}.$$

**Пример 6.** Вычислим остаток $(116 + 17^{17})^{21} \times 7^{49}$ от деления на 8.

$$(116 + 17^{17})^{21} \times 7^{49} \equiv (4 + 1^{17})^{21} \times (-1)^{49} =$$
$$= -5^{21} = -5 \times 25^{10} \equiv 3 \times 1^{10} = 3 \pmod{8}$$

## 2.2 Свойства, связанные с сокращением

**Утверждение 13.** Если $(d, m) = 1$, то $ad \equiv bd \pmod{m}$ тогда и только тогда, когда $a \equiv b \pmod{m}$.

**Замечание.** Утверждение состоит в том, что обе части сравнения можно разделить на их общий делитель, если последний взаимно прост с модулем.

*Доказательство.* Из $(ad - bd) \vdots m$ следует $d(a - b) \vdots m$, а, так как $(d, m) = 1$, из ***утверждения 6*** следует $(a - b) \vdots m$, что и требовалось.

Обратно. Так как $a \equiv b \pmod{m}$ и $d \equiv d \pmod{m}$, из ***утверждения 11*** следует $ad \equiv bd \pmod{m}$.

**Замечание.** Условие $(d, m) = 1$ не понадобилось для доказательства этой части утверждения.

□

**Пример 7.** $9 \equiv 15 \pmod{6}$, но $3 \not\equiv 5 \pmod{6}$ (общий делитель не взаимно прост с модулем: $(3, 6) \neq 1$, поэтому ***сокращать нельзя!***).

**Пример 8.** $5 \equiv 35 \pmod{6}$ (а здесь взаимно прост: $(5, 6) = 1$, поэтому ***можем сократить!***), а значит, $1 \equiv 7 \pmod{6}$.

**Утверждение 14.** $a \equiv b \pmod{m}$ тогда и только тогда, когда

$$ak \equiv bk \pmod{mk}$$

для любого $k \neq 0$.

*Доказательство.* Из ***леммы 6*** следует, что $(a-b) \vdots m$ тогда и только тогда, когда $(ak - bk) \vdots mk$, что и требовалось. □

**Замечание.** Отсюда получаем, что обе части сравнения и модуль можно разделить на любой их общий делитель.

**Пример 9.** $9 \equiv 15 \pmod{6}$, поэтому $3 \equiv 5 \pmod{2}$.

**Пример 10.** Упростим $50 \equiv 110 \pmod{12}$. Для этого сперва найдём $(50, 110, 12) = 2$ и сократим всё сравнение на 2, получим

$$25 \equiv 55 \pmod{6}.$$

Затем, так как $(25, 55) = 5$ и $(5, 6) = 1$, получим

$$5 \equiv 11 \pmod{6}.$$

Здесь мы последовательно воспользовались двумя предыдущими утверждениями.

**Утверждение 15.** Если $a \equiv b \pmod{m}$ и $d \in \mathcal{D}_m$, то $a \equiv b \pmod{d}$.

*Доказательство.* Действительно, так как $(a-b) \vdots m$ и $m \vdots d$, из ***леммы 4*** получаем $(a-b) \vdots d$, что и требовалось. □

**Утверждение 16.** Если $a \equiv b \pmod{m}$, то $\mathcal{D}_{a,m} = \mathcal{D}_{b,m}$, в частности $(a, m) = (b, m)$.

*Доказательство.* Действительно, это следует из ***утверждения 2*** и $a = b + mt$. □

**Замечание.** Как очевидное следствие этого утверждения получаем, что если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число.

## 2.3 Классы вычетов

**Определение.** Множество

$$[a]_m = \{\, x \in \mathbb{Z} \mid x \equiv a \pmod{m} \,\} = \{\, x \in \mathbb{Z} \mid x = a + mt, \text{ где } t \in \mathbb{Z} \,\}$$

всех чисел, сравнимых с $a$ по модулю $m$, называется *классом вычетов $a$ по модулю $m$*.

**Замечание.** Докажите, что $[a]_m = [b]_m$ тогда и только тогда, когда $a \equiv b \pmod{m}$.

**Замечание.** Так как каждому остатку по модулю $m$ соответствует свой класс вычетов и на остаток $r$ имеется ограничение $0 \leqslant r < m$, количество классов вычетов по модулю $m$ равно количеству различных остатков, то есть $m$.

**Замечание.** Обозначим через $\mathcal{P}_m = \{\, 0, 1, 2, \ldots, m-1 \,\}$ — множество остатков по модулю $m$, то есть множество, содержащее по одному элементу из каждого класса вычетов по модулю $m$.

**Утверждение 17.** Множества $[0]_m$, $[1]_m$, …, $[m-1]_m$ образуют ***разбиение множества*** $\mathbb{Z}$, то есть

1. $[0]_m \cup [1]_m \cup \cdots \cup [m-1]_m = \mathbb{Z}$;
2. $[p]_m \cap [q]_m = \varnothing$ для любых $p, q \in \mathcal{P}_m$ таких, что $p \neq q$.

**Замечание.** Утверждение состоит в том, что любое целое число лежит в одном из $m$ классов вычетов и что эти классы попарно не пересекаются.

*Доказательство.* Докажем сперва первый пункт. Пусть $x \in \mathbb{Z}$, тогда по ***теореме о делении с остатком*** $x = mq + r$, где $0 \leqslant r < m$, то есть $x \equiv r \pmod m$, а значит, $x \in [r]_m$, где $r \in \mathcal{P}_m$, что и требовалось.

Докажем теперь второй пункт. Пусть $x \in [p]_m \cap [q]_m$, тогда

$$x \equiv p \pmod m \text{ и } x \equiv q \pmod m,$$

поэтому $p \equiv q \pmod m$. Значит, $p = q$ (***докажите!***), так как $p, q \in \mathcal{P}_m$. □

**Пример 11.** Все классы вычетов по модулю 5:

$$[0]_5 = \{\, x \in \mathbb{Z} \mid x \equiv 0 \pmod 5 \,\} = \{\, \ldots, -10, -5, 0, 5, 10, \ldots \,\};$$
$$[1]_5 = \{\, x \in \mathbb{Z} \mid x \equiv 1 \pmod 5 \,\} = \{\, \ldots, -9, -4, 1, 6, 11, \ldots \,\};$$
$$[2]_5 = \{\, x \in \mathbb{Z} \mid x \equiv 2 \pmod 5 \,\} = \{\, \ldots, -8, -3, 2, 7, 12, \ldots \,\};$$
$$[3]_5 = \{\, x \in \mathbb{Z} \mid x \equiv 3 \pmod 5 \,\} = \{\, \ldots, -7, -2, 3, 8, 13, \ldots \,\};$$
$$[4]_5 = \{\, x \in \mathbb{Z} \mid x \equiv 4 \pmod 5 \,\} = \{\, \ldots, -6, -1, 4, 9, 14, \ldots \,\}.$$

## 2.4 Сравнения первой степени

Здесь и далее мы будем решать сравнения вида

$$ax \equiv b \pmod{m}, \tag{6}$$

где $a, b, m$ — известные числа и $a \not\equiv 0 \pmod{m}$, то есть $a \notin [0]_m$.

**Замечание.** Если $ax_1 \equiv b \pmod{m}$ и $x_2 \in [x_1]_m$, то (***проверьте!***) $ax_2 \equiv b \pmod{m}$. Это означает, что если $x_1$ удовлетворяет сравнению (6), то любое число, сравнимое с $x_1$ по модулю $m$, также будет удовлетворять этому сравнению.

**Определение.** Класс вычетов $[x_1]_m$ называется *решением сравнения* (6), если $ax_1 \equiv b \pmod{m}$. При таком соглашении сравнение (6) будет иметь столько решений, сколько элементов $\mathcal{P}_m$ ему удовлетворяет.

**Утверждение 18.** Если $(a, m) = 1$, то сравнение $ax \equiv b \pmod{m}$ имеет единственное решение. Более того, если числа $u$ и $v$ такие, что $au + mv = 1$, то решением является класс вычетов $[bu]_m$.

**Замечание.** Существование таких чисел $u$ и $v$ гарантируется ***теоремой о соотношении Безу***.

*Доказательство.* Докажем сперва, что $[bu]_m$ является решением. Пусть $(b, m) = d$, $b = b_1 d$ и $m = m_1 d$. Значит, по ***утверждению 14***

$$\boxed{abu \equiv b \pmod{m}, \text{ если и только если } ab_1 u \equiv b_1 \pmod{m_1}}.$$

Из ***утверждения 4*** следует $(b_1, m_1) = 1$, поэтому с помощью ***утверждения 13*** получаем

$$\boxed{ab_1 u \equiv b_1 \pmod{m_1}, \text{ если и только если } au \equiv 1 \pmod{m_1}}.$$

Так как $au = 1 - mv = 1 - m_1 dv$, получаем, что

$$\boxed{au \equiv 1 \pmod{m_1}, \text{ если и только если } 1 - m_1 dv \equiv 1 \pmod{m_1}},$$

а это выполняется тогда и только тогда, когда $\boxed{1 \equiv 1 \pmod{m_1}}$.

Таким образом, мы получили такое утверждение:

$$\boxed{abu \equiv b \pmod{m} \text{ тогда и только тогда, когда } 1 \equiv 1 \pmod{m_1}}.$$

И, так как $1 \equiv 1 \pmod{m_1}$ — верное утверждение, верным будет и $abu \equiv b \pmod{m}$, что и требовалось.

Теперь докажем единственность решения. Пусть $[x_1]_m, [x_2]_m$ — два решения сравнения. Тогда из $ax_1 \equiv b \pmod{m}$ и $ax_2 \equiv b \pmod{m}$ следует $ax_1 \equiv ax_2 \pmod{m}$. Так как $(a, m) = 1$, из ***утверждения 13*** следует $x_1 \equiv x_2 \pmod{m}$, то есть $[x_1]_m = [x_2]_m$, что и требовалось. □

**Пример 12.** Решим сравнение $7x \equiv 3 \pmod{45}$, воспользовавшись предыдущим утверждением, так как $(7, 45) = 1$. Для этого найдём такие $u$ и $v$, что $7u + 45v = 1$. Сперва применим алгоритм Евклида:

$$\begin{aligned} 45 &= 7 \times 6 + 3, & 0 &\leqslant 3 < 7; \\ 7 &= 3 \times 2 + 1, & 0 &\leqslant 1 < 3; \\ 3 &= 3 \times 1. \end{aligned}$$

Теперь проделаем процедуру замены остатков:

$$\boxed{1 =} 7 - 3 \times 2 = 7 - (45 - 7 \times 6) \times 2 = \boxed{7 \times 13 + 45 \times (-2)}.$$

Значит, $u = 13$, а решением будет $[13 \times 3]_{45} = [39]_{45}$.

**Замечание.** Здесь и далее

$$\mathcal{R}_{a,b,m} = \{\, x \in \mathbb{Z} \mid ax \equiv b \pmod{m} \,\} —$$

множество чисел, удовлетворяющих сравнению $ax \equiv b \pmod{m}$.

**Определение.** Сравнения $a_1x \equiv b_1 \pmod{m_1}$ и $a_2x \equiv b_2 \pmod{m_2}$ называются *равносильными*, если $\mathcal{R}_{a_1,b_1,m_1} = \mathcal{R}_{a_2,b_2,m_2}$.

**Утверждение 19.** Сравнение $ax \equiv b \pmod{m}$, где $(a, m) = d \neq 1$,

1. не имеет решений, если $b \not\vdots d$;
2. имеет ровно $d$ решений, если $b \vdots d$; более того, если числа $u$ и $v$ такие, что $au + mv = d$, то решениями будут классы вычетов

$$\left[\frac{bu}{d}\right]_m, \left[\frac{bu+m}{d}\right]_m, \left[\frac{bu+2m}{d}\right]_m, \ldots, \left[\frac{bu+(d-1)m}{d}\right]_m.$$

*Доказательство.* Первый пункт напрямую следует из ***утверждения 16***.

Займёмся вторым пунктом. Пусть $a = a_1 d$, $b = b_1 d$ и $m = m_1 d$. Из ***утверждения 14*** следует

$$\boxed{ax \equiv b \pmod{m}, \text{ если и только если } a_1 x \equiv b_1 \pmod{m_1}}.$$

Значит (***проверьте!***), $\mathcal{R}_{a,b,m} = \mathcal{R}_{a_1,b_1,m_1}$. Из ***утверждения 4*** следует $(a_1, m_1) = 1$, а значит, сравнение $a_1 x \equiv b_1 \pmod{m_1}$ имеет единственное решение $[x_1]_{m_1}$. Без ограничения общности будем считать, что $x_1 \in \mathcal{P}_{m_1}$, то есть $0 \leqslant x_1 < m_1$. Исходное сравнение имеет столько решений, сколько элементов

$$[x_1]_{m_1} = \{\, x \in \mathbb{Z} \mid x = x_1 + m_1 t, \text{ где } t \in \mathbb{Z} \,\}.$$

содержится в множестве $\mathcal{P}_m$.

Чтобы $x = x_1 + m_1 t$ принадлежал множеству $\mathcal{P}_m$, необходимо

$$0 \leqslant x_1 + m_1 t < m.$$

Если $t \leqslant -1$, то

$$x_1 + m_1 t \leqslant x_1 - m_1 < 0,$$

что не подходит. Если $d \leqslant t$, то

$$m \leqslant x_1 + m = x_1 + m_1 d \leqslant x_1 + m_1 t,$$

что также не подходит. Если $0 \leqslant t \leqslant d - 1$, то

$$\boxed{0 \leqslant} x_1 \leqslant \boxed{x_1 + m_1 t} \leqslant x_1 + m_1(d-1) \boxed{<} m_1 + m_1(d-1) = m_1 d = \boxed{m}.$$

Таким образом, на $t$ возникает ограничение $0 \leqslant t \leqslant d-1$. Каждому значению $t$ из этого промежутка соответствует свой элемент $\mathcal{P}_m$, равный $x_1 + m_1 t$. И, так как каждому элементу $\mathcal{P}_m$ отвечает своё решение, получаем $d$ решений исходного сравнения:

$$[x_1]_m, \ \ [x_1 + m_1]_m, \ \ [x_1 + 2m_1]_m, \ \ \ldots, \ \ [x_1 + (d-1)m_1]_m.$$

Заметим, что $au + mv = d$, если и только если $a_1 u + m_1 v = 1$. Воспользовавшись формулой из ***утверждения 18***, получим все решения исходного сравнения:

$$[b_1 u]_m, \ \ [b_1 u + m_1]_m, \ \ [b_1 u + 2m_1]_m, \ \ \ldots, \ \ [b_1 u + (d-1)m_1]_m.$$

Домножив и поделив на $d$, окончательно получим:

$$\left[\frac{bu}{d}\right]_m, \left[\frac{bu+m}{d}\right]_m, \left[\frac{bu+2m}{d}\right]_m, \ldots, \left[\frac{bu+(d-1)m}{d}\right]_m.$$

□

**Пример 13.** Решим сравнение $6x \equiv 15 \pmod{45}$. Это сравнение имеет 3 решения, так как $d = (6, 45) = 3$ и $15 \vdots 3$. Найдём такие, числа $u$ и $v$, что $6u + 45v = 3$.

$$\begin{aligned} 45 &= 6 \times 7 + 3, && 0 \leqslant 3 < 6; \\ 6 &= 3 \times 2. \end{aligned}$$

Значит, $3 = 6 \times (-7) + 45$, то есть $u = -7$. Получим следующие решения:

$$\begin{aligned} [10]_{45} &= \left[\frac{15 \times (-7)}{3}\right]_{45}, \\ [25]_{45} &= \left[\frac{15 \times (-7) + 45}{3}\right]_{45}, \\ [40]_{45} &= \left[\frac{15 \times (-7) + 2 \times 45}{3}\right]_{45}. \end{aligned}$$

**Замечание.** Можно было решить это сравнение, не используя готовые формулы. Сократив всё сравнение на 3, получаем

$$2x \equiv 5 \pmod{15}.$$

Найдя его решение, равное $[10]_{15}$, все решения исходного сравнения получаем, прибавляя с каждым разом 15, то есть

$$[10]_{45},\ \ [10+15]_{45} = [25]_{45},\ \ [10+15\times 2]_{45} = [40]_{45}.$$