

Элементы теории чисел

grznuch

10 декабря 2019 г.

Содержание

1	Основные понятия и теоремы	2
1.1	Деление с остатком	2
1.2	Наибольший общий делитель	5
1.3	Наименьшее общее кратное	10
2	Сравнение по модулю	12
2.1	Свойства сравнений	12
2.2	Свойства, связанные с сокращением	14
2.3	Классы вычетов	15
2.4	Сравнения первой степени	17

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 дальше 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

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

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

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). Если $\frac{a}{b}$ целое, то мы говорим, что a делится на b (обозначение $a : b$) или что b делит a (обозначение $b \mid a$). Таким образом, $a = bq$, где $q = \frac{a}{b} \in \mathbb{Z}$, то есть a представляется произведением b на целое. При этом a будем называть *кратным* числа b , а b — *делителем* числа a .

Замечание. Очевидно, что $a : b$ тогда и только тогда, когда $a = bq$, где $q \in \mathbb{Z}$.

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 $a : b$ и $a \neq 0$, то $|a| \geq |b|$.

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

Лемма 2. Если $a : b$ 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, $a = 0$. \square

Лемма 3. $a : b$ и $b : a$ тогда и только тогда, когда $|a| = |b|$.

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

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

Лемма 4. Если $a : b$ и $b : c$, то $a : c$.

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

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

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

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

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

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

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

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 $0 \leq r < |b|$.

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

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

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

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

то есть $0 \leq r < |b|$ 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 $0 \leq r_1 < |b|$. Отсюда получаем, что $bq + r = bq_1 + r_1$, то есть

$$r - r_1 = b(q_1 - q). \quad (1)$$

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

$$r - |b| < r - r_1 < |b| - r_1. \quad (2)$$

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

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

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. \square

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

1.2 Наибольший общий делитель

Определение. Число $d \in \mathbb{N}$ называется *общим делителем* чисел a_1, a_2, \dots, a_n , если $a_i : d$ для любого $i = \overline{1, n}$. Наибольшее число из общих делителей этих чисел называется *наибольшим общим делителем* и обозначается (a_1, a_2, \dots, a_n) .

Замечание. Здесь и далее

$$\mathcal{D}_{a_1, a_2, \dots, a_n} = \{ d \in \mathbb{N} \mid \forall i = \overline{1, n} \quad a_i : d \} -$$

множество, состоящее из всех общих делителей чисел a_1, a_2, \dots, a_n . Тогда $\mathcal{D}_a = \{ d \in \mathbb{N} \mid a : d \}$ — множество, состоящее из всех делителей числа a .

Замечание. Чем является множество \mathcal{D}_0 ? Есть ли в нём наибольший элемент? Чему равен $(0, 0)$?

Определение. Числа a_1, a_2, \dots, a_n называются *взаимно простыми*, если $(a_1, a_2, \dots, a_n) = 1$.

Утверждение 1. Если $a : b$, то $\mathcal{D}_{a,b} = \mathcal{D}_b$, в частности если $b \neq 0$, то $(a, b) = |b|$.

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 $a : d$ и $b : d$, 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 $b : d$. И, так как по условию $a : b$, из **леммы 4** получаем, что $a : d$, то есть $d \in \mathcal{D}_{a,b}$.

Так как $b \neq 0$ и $\mathcal{D}_{a,b} = \mathcal{D}_b$, наибольшие элементы этих множеств равны, но $|b|$ и есть наибольший элемент множества \mathcal{D}_b (**докажите!**). Значит, $(a, b) = |b|$. \square

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

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

[illegible]

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

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

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

Доказательство. Пусть $d \in \mathcal{D}_{a,b}$, тогда $a:d$ и $b:d$, а значит, из равенств (3) и **леммы 5** последовательно получаем

$$r_1 \vdots d, \quad r_2 \vdots d, \quad \dots, \quad r_{n-2} \vdots d, \quad r_{n-1} \vdots d, \quad (a, b) = r_n \vdots d,$$

то есть $d \in \mathcal{D}_{(a,b)}$.

Аналогично если $d \in \mathcal{D}_{(a,b)}$, то, используя сначала **лемму 4**, последовательно получаем

$$r_n = (a, b) : d, \quad r_{n-1} : d, \quad r_{n-2} : d, \quad \dots, \quad r_2 : d, \quad r_1 : d, \quad b : d, \quad a : d,$$

то есть $d \in \mathcal{D}_{a,b}$. □

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

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

Доказательство. Действительно, из равенств (3) получаем

$$\begin{aligned} (a, b) &= r_n = r_{n-2} - r_{n-1}q_{n-1}; \\ r_{n-1} &= r_{n-3} - r_{n-2}q_{n-2}; \\ &\vdots \\ r_3 &= r_1 - r_2q_2; \\ r_2 &= b - r_1q_1; \\ r_1 &= a - bq. \end{aligned}$$

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

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 $a, b, r_1, r_2, \dots, r_{n-1}, r_n$ будут числа

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

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) . \square

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

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

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

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

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

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

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

то есть $(ac, b) : (c, b)$.

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

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

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

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

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

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

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

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

1.3 Наименьшее общее кратное

Определение. Число $m \in \mathbb{N}$ называется *общим кратным* чисел a_1, a_2, \dots, a_n , если $m : a_i$ для любого $i = \overline{1, n}$. Наименьшее число из общих кратных этих чисел называется *наименьшим общим кратным* и обозначается $[a_1, a_2, \dots, a_n]$.

Замечание. Здесь и далее

$$\mathcal{M}_{a_1, a_2, \dots, a_n} = \{ m \in \mathbb{N} \mid \forall i = \overline{1, n} \quad m : a_i \} —$$

множество, состоящее из всех общих кратных чисел a_1, a_2, \dots, a_n . Тогда $\mathcal{M}_a = \{ m \in \mathbb{N} \mid m : a \}$ — 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

$$m = \frac{|ab|}{d}t, \quad (4)$$

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 $m : a$, $m = |a|k$. С другой стороны, из $m : b$ следует $|a|k : |b|$, а значит, $da_1k : db_1$. Из **леммы 6** получаем $a_1k : b_1$. В конечном итоге с помощью **утверждения 6** получаем $k : b_1$, 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 $m : a$. Аналогично показывается, что $m : b$. Значит, m — общее кратное a и b . \square

Теорема 3 (формула для наименьшего общего кратного).

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

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

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**. \square

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 $m : [a, b]$, то есть $m \in \mathcal{M}_{[a,b]}$.

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

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:

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

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 $(a - b) : m$.

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

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

то есть $(a - b) : m$.

Обратно, пусть $(a - b) : m$ и $b = mp + r$, где $0 \leq r < m$. Покажем, что остатки от деления a и b на m равны. Действительно, из $(a - b) : m$ 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 $(a_1 - b_1) : m$ и $(a_2 - b_2) : m$ следует

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

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

Замечание. Пусть $a_1 + b \equiv c \pmod{m}$ и $a_1 \equiv a_2 \pmod{m}$. Покажите, что тогда $a_2 + b \equiv c \pmod{m}$.

Замечание. Покажите, что $a + b \equiv c \pmod{m}$ тогда и только тогда, когда $a \equiv c - b \pmod{m}$.

Замечание. Покажите, что $a \equiv b \pmod{m}$ тогда и только тогда, когда $a + mk \equiv b \pmod{m}$ для любого $k \in \mathbb{Z}$.

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 $(a_1 - b_1) : m$, $(a_2 - b_2) : m$,

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

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

Замечание. Пусть $a_1 b \equiv c \pmod{m}$ и $a_1 \equiv a_2 \pmod{m}$. Покажите, что тогда $a_2 b \equiv c \pmod{m}$.

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

Замечание. Покажите, что если $a \equiv b \pmod{m}$, то $ac \equiv bc \pmod{m}$ для любого $c \in \mathbb{Z}$.

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 $(a - b) : m_1$ и $(a - b) : m_2$ тогда и только тогда, когда $(a - b) : [m_1, m_2]$. \square

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 $(ad - bd) : m$ следует $d(a - b) : m$, а, так как $(d, m) = 1$, из **утверждения 6** следует $(a - b) : m$, 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 5. $9 \equiv 15 \pmod{6}$, но $3 \not\equiv 5 \pmod{6}$ (общий делитель не взаимно прост с модулем: $(3, 6) \neq 1$, поэтому **сокращать нельзя!**).

Пример 6. $5 \equiv 35 \pmod{6}$ (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 $k \in \mathbb{Z}$.

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

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

Пример 7. $9 \equiv 15 \pmod{6}$, поэтому $3 \equiv 5 \pmod{2}$.

Пример 8. 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 $(a - b) : m$ и $m : d$, из **леммы 4** получаем $(a - b) : d$, что и требовалось. \square

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 $a = b + mt$. \square

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 $0 \leq r < m$, количество классов вычетов по модулю m равно количеству различных остатков, то есть m .

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

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

1. $[0]_m \cup [1]_m \cup \dots \cup [m-1]_m = \mathbb{Z}$;
2. $[p]_m \cap [q]_m = \emptyset$ 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 $0 \leq r < m$, 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 $p, q \in \mathcal{P}_m$. \square

Пример 9. Все классы вычетов по модулю 5:

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

2.4 Сравнения первой степени

Здесь и далее мы будем решать сравнения вида

$$ax \equiv b \pmod{m}, \quad (6)$$

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 удовлетворяют.

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 $(b, m) = d$, $b = b_1d$ и $m = m_1d$. Значит, по *утверждению 14*

$$abu \equiv b \pmod{m}, \text{ если и только если } ab_1u \equiv b_1 \pmod{m_1}.$$

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

$$ab_1u \equiv b_1 \pmod{m_1}, \text{ если и только если } au \equiv 1 \pmod{m_1}.$$

Так как $au = 1 - mv = 1 - m_1dv$, получаем, что

$$au \equiv 1 \pmod{m_1}, \text{ если и только если } 1 - m_1dv \equiv 1 \pmod{m_1},$$

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. \square

Пример 10. 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:

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

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

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

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

Займёмся вторым пунктом. Пусть $a = a_1d$, $b = b_1d$ и $m = m_1d$. Из **утверждения 14** следует

$$ax \equiv b \pmod{m}, \text{ если и только если } a_1x \equiv b_1 \pmod{m_1}.$$

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 $a_1x \equiv b_1 \pmod{m_1}$ имеет единственное решение $[x_1]_{m_1}$. Без ограничения общности будем считать, что $x_1 \in \mathcal{P}_{m_1}$, то есть $0 \leq x_1 < m_1$. Исходное сравнение имеет столько решений, сколько элементов

$$[x_1]_{m_1} = \{x \in \mathbb{Z} \mid x = x_1 + m_1t, \text{ где } t \in \mathbb{Z}\}.$$

содержится в множестве \mathcal{P}_m .

Чтобы $x = x_1 + m_1t$ принадлежал множеству \mathcal{P}_m , необходимо

$$0 \leq x_1 + m_1t < m.$$

Если $t \leq -1$, то

$$x_1 + m_1t \leq x_1 - m_1 < 0,$$

что не подходит. Если $0 \leq t$, то

$$m \leq x_1 + m = x_1 + m_1d \leq x_1 + m_1t,$$

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

$$0 \leq x_1 \leq x_1 + m_1t \leq x_1 + m_1(d-1) < m_1 + m_1(d-1) = m_1d = m.$$

Таким образом, на t возникает ограничение $0 \leq t \leq d-1$. 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:

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

Заметим, что $au + mv = d$, если и только если $a_1u + m_1v = 1$. Воспользовавшись формулой из **утверждения 18**, получим все решения исходного сравнения:

$$[b_1u]_m, [b_1u + m_1]_m, [b_1u + 2m_1]_m, \dots, [b_1u + (d-1)m_1]_m.$$

Домножив и поделив на d , окончательно получим:

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

□

Пример 11. Решим сравнение $6x \equiv 15 \pmod{45}$. Это сравнение имеет 3 решения, так как $d = (6, 45) = 3$ и $15 : 3$. Найдём такие, числа u и v , что $6u + 45v = 3$.

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

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

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