Занятие 7

Число d называется *наибольшим общим делителем* (НОД) чисел a и b, если (1) $d \mid a$ и $d \mid b$, а также (2) для всех x из $x \mid a$ и $x \mid b$ следует $x \leqslant d$. В этом случае пишем $d = (a, b)$.

Лемма 1. *Для любых чисел a, b, q*

1. *если $a \neq 0$ или $b \neq 0$, то существует d, т. ч. $d = (a, b)$, причем $(a, b) > 0$;*
2. *если $a \neq 0$, то $(a, 0) = |a|$ и $(a, a) = |a|$;*
3. *если $a \neq 0$ или $b \neq 0$, то $(a, b) = (|a|, |b|)$ и $(a, b) = (b, a)$;*
4. *если $a \neq 0$ или $b \neq 0$, то $(a, b) = (a + bq, b)$;*
5. *если $a \neq 0$ или $b \neq 0$, и $a \mid b$, то $(a, b) = |a|$.*

Доказательство. Пусть, без ограничения общности, $a \neq 0$. Единица является общим делителем a и b. С другой стороны, любой делитель числа a не превосходит $|a|$. Поэтому одно из целых чисел отрезка $[1, |a|]$ есть НОД a и b. Теперь очевидны равенства $(a, 0) = |a|$, $(a, a) = |a|$ и $(a, b) = (b, a)$.

Напомним, что для всех чисел x верно $x = |x| \cdot \operatorname{sgn} x$ и $|x| = x \cdot \operatorname{sgn} x$, где $\operatorname{sgn} x = 1$ при $x > 0$, $\operatorname{sgn} x = -1$ при $x < 0$ и $\operatorname{sgn} x = 0$ при $x = 0$. Отсюда легко следует, что $d \mid a$ и $d \mid b$ имеем место тогда и только тогда, когда $d \mid |a|$ и $d \mid |b|$. Значит, *множества* общих делителей пар чисел a, b и $|a|, |b|$ совпадают — следовательно, совпадают и наибольшие их элементы: $(a, b) = (|a|, |b|)$.

Нетрудно видеть, что множества общих делителей пар чисел a, b и $a+bq, b$ совпадают. В самом деле, если, например, если $d \mid (a+bq)$ и $d \mid b$, то $d \mid bq$ и $d \mid a = (a+bq)-bq$. Итак, $(a, b) = (a + bq, b)$.

Допустим, что $a \mid b$. Если $a = 0$, то и $b = 0$. Поэтому в условиях последнего утверждения $a \neq 0$. Из вышесказанного видно, что $(a, b) = |a|$. □

Практически вычислить (a, b) при условии $b > 0$ позволяет следующий *алгоритм Евклида*, использующий (очевидный) алгоритм деления с остатком:

> Поделим a на b с остатком r_2 и выпишем r_2. Если $r_2 = 0$, завершаем алгоритм. Иначе поделим b на r_2 с остатком r_3, который выпишем. Если $r_3 > 0$, продолжаем. Далее, для $k = 4, 5, \ldots$ делим r_{k-2} на r_{k-1} с остатком r_k (выписываем). Если $r_k = 0$, останавливаемся.

В духе самого Евклида и классической древности алгоритм можно было бы сформулировать так: «подели a на b; далее делитель дели на остаток, пока этот остаток ненулевой».

Лемма 2 (разд. 4.8 Учебника)**.** *Для любых чисел $b > 0$ и a алгоритм Евклида завершает работу за конечное число шагов, причем, если $r_{n+1} = 0$, то $(a, b) = r_n$.*

Доказательство. Для первых k остатков, вычисленных алгоритмом, выполняются утверждения:

$$\begin{array}{lcll} a & = & bq_1 + r_2, & 0 < r_2 < b; \\ b & = & r_2q_2 + r_3, & 0 < r_3 < r_2; \\ r_2 & = & r_3q_3 + r_4, & 0 < r_4 < r_3; \\ \dots & & & \\ r_{k-2} & = & r_{k-1}q_{k-1} + r_k, & 0 \leqslant r_k < r_{k-1}. \end{array}$$

Для завершения алгоритма достаточно, чтобы нашлось n, т. ч. $r_{n+1} = 0$, т. е.

$$\begin{array}{lcll} r_{n-2} & = & r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} & = & r_nq_n. & \end{array}$$

В самом деле, в цепи остатков $b > r_2 > r_3 > \ldots > r_k > \ldots \geqslant 0$ должен найтись минимальный элемент r_{n+1}. Если этот элемент положительный, то возможно сделать еще шаг алгоритма и получить $r_{n+2} < r_{n+1}$, т. е. r_{n+1} не будет минимальным. Следовательно, $r_{n+1} = 0$.

Убедимся, что последний ненулевой остаток r_n равен (a, b). По лемме 1, имеем

$$(a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

□

Алгоритм Евклида дает не только сам НОД, но и позволяет выразить его линейно по a и b. Это обстоятельство играет центральную роль в решении линейных уравнений в целых числах и сравнений.

Теорема 3 (о линейном представлении НОД; соотношение Безу; разд. 4.7 Учебника)**.** *Для любых a, b, т. ч. $a \neq 0$ или $b \neq 0$, существуют числа u, v, для которых*

$$au + bv = (a, b).$$

Доказательство. Предположим, утверждение верно, если одно из чисел a, b положительно. Тогда, по лемме 1, имеем $(a, b) = (|a|, |b|) = |a|u' + |b|v' = au' \operatorname{sgn} a + bv' \operatorname{sgn} b$.

Допустив теперь, без ограничения общности, что $b > 0$, воспользуемся алгоритмом Евклида. Именно, покажем, что для любого r_k (в частности, для r_n) найдутся u, v, т. ч. $r_k = au + bv$. Для r_2 и r_3 утверждение очевидно. Рассуждая по индукции, рассмотрим $k > 3$, предположив $r_{k-2} = au'' + bv''$ и $r_{k-1} = au' + bv'$. Имеем

$$r_k = r_{k-2} - r_{k-1}q_{k-1} = a(u'' - u'q_{k-1}) + b(v'' - v'q_{k-1}).$$

□

Найдем, например, $(481, 1177)$ с помощью алгоритма Евклида и выразим НОД через исходные числа.

$$\begin{aligned}
481 &= 1177 \cdot 0 + 481;\\
1177 &= 481 \cdot 2 + 215;\\
481 &= 215 \cdot 2 + 51;\\
215 &= 51 \cdot 4 + 11;\\
51 &= 11 \cdot 4 + 7;\\
11 &= 7 \cdot 1 + 4;\\
7 &= 4 \cdot 1 + 3;\\
4 &= 3 \cdot 1 + 1;\\
3 &= 1 \cdot 3.
\end{aligned}$$

Итак, $(481, 1177) = 1$. Найдем u и v, т. ч. $481u + 1177v = 1$. Обозначим $a = 481$ и $b = 1177$ и станем последовательно выражать все отличные от a и b остатки:

$$\begin{aligned}
215 &= -2a + b;\\
51 &= a - 2 \cdot 251 = a - 2(-2a + b) = 5a - 2b;\\
11 &= 215 - 4 \cdot 51 = -2a + b - 4(5a - 2b) = -22a + 9b;\\
7 &= 51 - 4 \cdot 11 = 5a - 2b - 4(-22a + 9b) = 93a - 38b;\\
4 &= 11 - 7 = -22a + 9b - 93a + 38b = -115a + 47b;\\
3 &= 7 - 4 = 93a - 38b + 115a - 47b = 208a - 85b;\\
1 &= 4 - 3 = -115a + 47b - 208a + 85b = -323a + 132b.
\end{aligned}$$

Итак, $u = -323$ и $v = 132$.

Решением сравнения

$$ax \equiv b \pmod{m} \tag{1}$$

мы называем любое удовлетворяющее ему число x_0, т. ч. $0 \leqslant x_0 < m$.

Теорема 4 (линейное сравнение с одним неизвестным; разд. 4.6 Учебника)**.** *Пусть $d = (a, m)$. Если $d \mid b$, сравнение (1) имеет в точности d различных решений:*

$$x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m',$$

где x_0 есть единственное решение сравнения

$$a'x \equiv b' \pmod{m'}, \tag{2}$$

в котором $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Если же $d \nmid b$, сравнение (1) не имеет решений.

Доказательство. Сравнение (1) для произвольного x эквивалентно существованию k, т. ч. $ax = b + km$. Это равенство невозможно, если $d \nmid b$. В противном случае, оно эквивалентно равенству $a'x = b' + km'$ (сократили на d).

Следовательно, если $d \mid b$, сравнение (1) эквивалентно сравнению (2) в том смысле, что им удовлетворяют одни и те же числа x. Однако отсюда, вообще говоря, не следует, что у этих сравнений одно и то же множество решений, поскольку в первом

случае мы ограничиваем бесконечную серию подходящих x числом m, а во втором — числом m'.

Очевидно, любое число, сравнимое по модулю m' с некоторым решением x_0 сравнения (2), само удовлетворяет этому сравнению. Поскольку $0 \leqslant x_0 < m' \leqslant m = dm'$, среди таких чисел решениями сравнения (1) будут в точности

$$x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'.$$

Обратно, если число x есть решение сравнения (1), оно также удовлетворяет сравнению (2) — как и сравнимый с x по модулю m' остаток x_0 при делении x на m'. Таким образом, x имеет вид $x_0 + km'$ для некоторого k из $0, \ldots, d-1$ и некоторого решения x_0 сравнения (2).

Остается показать, что сравнение (2) имеет единственное решение x_0. Имеем $(a', m') = 1$, откуда, в силу соотношения Безу,

$$ua' + vm' = 1$$

для некоторых u и v. Положим $x = ub'$. Тогда

$$a'x = b' - (vb')m',$$

откуда $a'x \equiv b' \pmod{m'}$. Возьмем за x_0 остаток при делении x на m'. Если сравнение (2) имеем какое-то еще решение x_1, то $a'(x_0 - x_1) \equiv 0 \pmod{m'}$, но это значит, что $m' \,|\, (x_0 - x_1)$. Поскольку $0 \leqslant x_0, x_1 < m'$, такое возможно лишь при $x_1 = x_0$. □

Задача 7.1. Найдите количество решений сравнения $39x \equiv 104 \pmod{221}$.

Решение. Имеем $(39, 221) = 13 \,|\, 104$. Поэтому у сравнения точно 13 различных решений. □

Теорема 5 (линейное уравнение с двумя неизвестными; разд 4.9 Учебника)**.** *Пусть $a \neq 0$ или $b \neq 0$, и $d = (a, b)$. Уравнение*

$$ax + by = c \tag{3}$$

имеет (целочисленное) решение тогда и только тогда, когда $d \,|\, c$. Если $d \,|\, c$, решениями уравнения (3) будут, в точности, пары

$$(x_0 - b't, y_0 + a't)$$

при всевозможных целых t, где $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $c' = \frac{c}{d}$ и пара (x_0, y_0) есть произвольное решение уравнения

$$a'x + b'y = c' \tag{4}$$

Доказательство. Очевидно, при $d \nmid c$ решений нет. Допустим $d \,|\, c$ и сократим уравнение (3) на d, получая эквивалентное ему уравнение (4). Далее рассматриваем только его.

Пусть (x_0, y_0) произвольное решение. Тогда пара $(x_0 - b't, y_0 + a't)$ будет решением при любых t. В самом деле,

$$a'(x_0 - b't) + b'(y_0 + a't) = a'x_0 + b'y_0 - a'b't + b'a't = a'x_0 + b'y_0 = 0.$$

Всякое решение получается из (x_0, y_0) таким образом. Действительно, пусть (x, y) некоторое решение. Тогда

$$a'(x_0 - x) + b'(y_0 - y) = c' - c' = 0,$$

т. е. $a'(x_0 - x) = b'(y - y_0)$. Учитывая $(a', b') = 1$, имеем $b' \,|\, (x_0 - x)$ и $a' \,|\, (y - y_0)$, т. е. $x = x_0 - b't_1$ и $y = y_0 + a't_2$. Подставляя эти значения в уравнение, получаем

$$ax_0 - a'b't_1 + by_0 + b'a't_2 = a'b'(t_2 - t_1) = 0,$$

откуда $t_1 = t_2$.

Остается показать, что уравнение (4) имеет решение. В силу соотношения Безу, найдутся u и v, такие что

$$ua' + vb' = 1.$$

Положив $x_0 = uc'$ и $y_0 = vc'$, получаем некоторое решение (x_0, y_0) уравнения (4). □

Задача 7.2. Найдите решения уравнения $45x - 37y = 25$ в целых числах.

Решение. Имеем $(45, -37) = 1 \,|\, 25$, так что решения существуют. С помощью алгоритма Евклида находим u и v, такие что $45u + 37v = 1$. Имеем $u = 14$ и $v = -17$. Отсюда видно, что одним из решений нашего уравнения будет пара $(14 \cdot 25, 17 \cdot 25)$. Все решения образуют множество

$$\{(14 \cdot 25 + 37t, 17 \cdot 25 + 45t) \mid t \in \mathbb{Z}\}.$$

□

Задача 7.3. Сколько положительных делителей имеет число $2^{10} \cdot 3^5 \cdot 5^3$?

Решение. Вследствие «основной теореме арифметики», любой делитель имеет вид $2^a \cdot 3^b \cdot 5^c$, где $0 \leqslant a \leqslant 10$, $0 \leqslant b \leqslant 5$ и $0 \leqslant c \leqslant 3$, причем наборы (a, b, c) взаимнооднозначно соответствуют делителям. Таких наборов ровно $11 \cdot 6 \cdot 4$, как и делителей. □

Задача 7.4. Пусть $(a, b) = 1$. Найдите все возможные значения $(a + b, a^2 + b^2)$.

Решение. Пусть $a + b$ и $a^2 + b^2$ имеют общий простой делитель p. Каким он может быть? В силу $p \,|\, (a + b)^2 = a^2 + b^2 + 2ab$, имеем $p \,|\, 2ab$. Значит, $p \,|\, 2$ и $p = 2$, или же $p \,|\, ab$. В последнем случае верно $p \,|\, a$ или $p \,|\, b$. Но если $p \,|\, a$, то, в силу $p \,|\, (a + b)$, и $p \,|\, b$, а значит, $(a, b) \geqslant p$, что не так. Аналогично, отвергаем случай $p \,|\, b$.

Итак, $p = 2$. Какая наибольшая степень 2 может делить $a + b$ и $a^2 + b^2$? Покажем, что уже 4 не будет общим делителем. В самом деле, иначе $4 \,|\, 2ab$, откуда $2 \,|\, ab$. Но, раз $4 \,|\, (a + b)$, числа a и b одной четности, и тогда $(a, b) \geqslant 2$, что не так.

Допустим, что $d = (a+b, a^2+b^2)$. Если $d \neq 1$, число d имеет простой делитель p. Но мы показали, что тогда $p = 2$ и, кроме того, $4 \nmid d$. Отсюда следует, что $d = 2$. Итак, $d = 1$ или $d = 2$.

Легко видеть, что оба случая возможны. Например, $(1+1, 1^2+1^2) = 2$ и $(1+2, 1^2+2^2) = 1$. □

Задача 7.5. Найдите остаток при делении числа $N = \underbrace{111\ldots111}_{105}$ на 107. (Использована десятичная система.)

Решение. Легко видеть, что $9N + 1 = 10^{105}$. Число 107 простое, так что по малой теореме Ферма $10^{106} \equiv 1 \pmod{107}$. Значит, если $x = 10^{105}$, то $10x \equiv 1 \pmod{107}$. Это сравнение имеет единственное решение $x_0 = 75$, которое нетрудно угадать или найти с помощью алгоритма Евклида. Получаем $10^{105} \equiv 75 \pmod{107}$.

Имеем $9N \equiv 74 \pmod{107}$. Алгоритм Евклида (или счастливая догадка) дает представление $(9, 107) = 1 = 9 \cdot 12 + 107 \cdot (-1)$. Значит, подходит $N = 12 \cdot 74$. Однако,

$$N \equiv 12 \cdot 74 \equiv 6 \cdot 148 \equiv 6 \cdot 41 \equiv 2 \cdot 123 \equiv 2 \cdot 16 \equiv 32 \pmod{107}.$$

□

Задача 7.5. Существует ли решение уравнения $6x + 10y + 15z = 29$

a) в целых числах?

b) в неотрицательных целых числах?

Решение. **a)** Если угадать подходящее z, мы можем воспользоваться известным нам критерием существования решения уравнения с двумя неизвестными. Пусть $z = 1$. Тогда уравнение равносильно уравнению $6x + 10y = 29 - 15 = 14$, которое имеет решение (x_0, y_0), так как $(6, 10) = 2 \mid 14$. Значит, тройка $(x_0, y_0, 1)$ есть решение исходного уравнения.

b) Пусть (x_0, y_0, z_0) есть некоторое такое решение. Имеем $6 + 10 + 15 > 29$, так что хотя бы одно из чисел x_0, y_0 или z_0 равно нулю. Но тогда оставшиеся два числа образуют решение одного из уравнений

$$\begin{aligned} 6x + 10y &= 29 \\ 6x + 15z &= 29 \\ 10y + 15z &= 29. \end{aligned}$$

Однако, ни одно из этих уравнений не имеет целочисленного решения, поскольку число 29 просто и не делится на неединичный НОД коэффициентов при неизвестных. Следовательно, решений нужного вида не существует. □

Задача 7.7. Докажите, что для положительных x, y, z выполняются равенства:

a) $\text{НОК}(x, y) = \dfrac{xy}{\text{НОД}(x, y)}$;

b) $\text{НОК}(x, y, z) = \dfrac{xyz \cdot \text{НОД}(x, y, z)}{\text{НОД}(x, y) \cdot \text{НОД}(x, z) \cdot \text{НОД}(y, z)}$;

c) попробуйте выразить $\text{НОК}(x_1, \ldots, x_n)$ аналогичным образом.

Решение. **a)** По «основной теореме арифметики», каждое положительное число x однозначно представимо в виде произведения

$$\prod_{i\in\mathbb{N}} p_i^{x_i},$$

где p_i есть i-ое простое и все числа x_i целые неотрицательные, причем лишь конечно многие из них отличны от нуля. Легко тогда видеть, применяя ту же теорему, что

$$\text{НОК}(x,y) = \prod_{i\in\mathbb{N}} p_i^{\max(x_i,y_i)} \quad \text{и} \quad \text{НОД}(x,y) = \prod_{i\in\mathbb{N}} p_i^{\min(x_i,y_i)}.$$

Тождество $\max(x_i,y_i) = x_i + y_i - \min(x_i,y_i)$ тогда показывает, что степень каждого простого числа p_i слева и справа в требуемом равенстве одинакова, а значит, и числа слева и справа одинаковы.

b) Достаточно проверить тождество $\max(a,b,c) = a+b+c-\min(a,b)-\min(a,c)-\min(b,c)+\min(a,b,c)$. Из соображений симметрии, достаточно рассмотреть случай $a \leqslant b \leqslant c$. Тогда прямое вычисление дает требуемое.

c) Нужно получить аналогичное тождество для произвольного n. Это легко сделать, используя *формулу включений и исключений* (разд. 6.4 Учебника): обобщение равенства $|A \cup B| = |A| + |B| - |A \cap B|$ — взяв за A_{x_i} множество $1,\ldots,x_i$ (в частности, A_0 пустое), и заметив, что $|A_{x_{i_1}} \cup \ldots \cup A_{x_{i_k}}| = \max(x_{i_1},\ldots,x_{i_k})$ и $|A_{x_{i_1}} \cap \ldots \cap A_{x_{i_k}}| = \min(x_{i_1},\ldots,x_{i_k})$. □

Задача 7.8. a) Верно ли, что для всякого n существует такая арифметическая прогрессия $\{a_k\}_{k\in\mathbb{N}}$, что числа $a_1,\ldots,a_n$ попарно взаимно просты?

b) Верно ли, что существует такая арифметическая прогрессия $\{a_k\}_{k\in\mathbb{N}}$, что для всякого n числа $a_1,\ldots,a_n$ попарно взаимно просты?

Решение. **a)** Верно. Выберем простое $a_1 = p > n$ и разность $d = n!$. Допустим, что $q\,|(p+kn!)$ и $q\,|(p+mn!)$ для простого q и некоторых целых неотрицательных $k < m < n$. Тогда $q\,|(m-k)n!$. Отсюда $q\,|\,n!$ или $q\,|(m-k)$. Однако $0 < m-k < n$, а значит, $(m-k)\,|\,n!$. Выходит, во всяком случае $q\,|\,n!$. Но тогда $q\,|\,p$ и, следовательно, $q = p$. С другой стороны, $q \leqslant n < p$. Противоречие.

b) Неверно. Допустим, такая прогрессия с разностью $d \neq 0$ есть. В ней обязательно найдется член a_k, т. ч. $|a_k| > 1$. Имеем $(a_k, a_{k+|a_k|}) = (a_k, a_k + d|a_k|) = |a_k| > 1$. Таким образом, при $n > k + |a_k|$ условие нарушается.

□