

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ  
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ  
УНИВЕРСИТЕТ»

Р.С. Адамова

## **ТЕОРИЯ ЧИСЕЛ**

Часть 1

*Учебно-методическое пособие*

Воронеж  
Издательский дом ВГУ  
2017

## § 1. Делимость в множестве натуральных чисел

Пусть  $a, b \in \mathbb{N}$ .

Определение 1. Говорят, что  $a$  делится на  $b$ , если существует  $q \in \mathbb{N}$  такое, что

$$a = b \cdot q$$

При этом пишут  $a : b$ . Число  $q$  называют частным от деления  $a$  на  $b$ , число  $a$  называют кратным числа  $b$  (обозначают  $a : b$ ), а  $b$  – делителем числа  $a$ . Если  $a$  не делится на  $b$ , пишут  $a \nmid b$ .

**Теорема 1.** Если  $a > b$  и  $a \nmid b$ , то существуют, и притом единственным образом, числа  $q, r \in \mathbb{N}$  такие, что

$$a = bq + r, \quad r < b. \quad \square \quad (1)$$

При этом  $q$  называют неполным частным, а  $r$  – остатком от деления  $a$  на  $b$ .

Такое представление числа  $a$  называется делением с остатком.

Определение 2. Наибольшим общим делителем системы натуральных чисел  $a_1, a_2, \dots, a_k$  называется наибольший среди их общих делителей.

Он обозначается  $\text{НОД}(a_1, a_2, \dots, a_k)$  или, короче,  $(a_1, a_2, \dots, a_k)$ .

Определение 3. Наименьшим общим кратным системы натуральных чисел  $a_1, a_2, \dots, a_k$  называется наименьшее среди их общих кратных.

Оно обозначается  $\text{НОК}(a_1, a_2, \dots, a_k)$  или  $[a_1, a_2, \dots, a_k]$ .

**Теорема 2.** Наибольший общий делитель и наименьшее общее кратное обладают следующими свойствами:

1. Любое общее кратное чисел  $a_1, a_2, \dots, a_k$  делится на их наименьшее общее кратное.
2. Наибольший общий делитель чисел  $a_1, a_2, \dots, a_k$  делится на любой общий делитель этих чисел.
3. Если  $[a_1, a_2, \dots, a_k] = m$ , то  $[a_1, a_2, \dots, a_k, a_{k+1}] = [m, a_{k+1}]$ .
4. Если  $(a_1, a_2, \dots, a_k) = d$ , то  $(a_1, a_2, \dots, a_k, a_{k+1}) = (d, a_{k+1})$ .
5. При одновременном делении чисел  $a_1, a_2, \dots, a_k$  на любой их общий делитель  $c$  то же самое происходит и с их НОД и НОК, то есть

## § 2. Алгоритм Евклида

### § 2. Алгоритм Евклида

Для нахождения НОД и НОК любого конечного семейства чисел достаточно, в силу теорем 2 и 3, уметь находить НОД двух чисел. Пусть даны два натуральных числа  $a$  и  $b$ ,  $a \geq b$ . Если  $a \div b$ , то  $\text{НОД}(a, b) = b$ .

Рассмотрим другую ситуацию:  $a > b$ ,  $a \nmid b$ . Выполним процесс последовательного деления.

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \end{aligned} \tag{5}$$

.....

$$\begin{aligned} r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1} \end{aligned}$$

Такой процесс действительно конечен, так как остатки  $r_1, r_2, r_3, \dots$  — натуральные числа, убывающие с возрастанием номера. Он называется алгоритмом Евклида последовательного деления  $a$  на  $b$ .

**Теорема 4.** Наибольшим общим делителем чисел  $a$  и  $b$  ( $a > b$ ,  $a \nmid b$ ) является последний остаток в процессе алгоритма Евклида последовательного деления  $a$  на  $b$ .

Доказательство. Пусть  $d = (a, b)$ . Тогда  $a, b \div d$ . Из алгоритма (5) последовательно получаем  $r_1 \div d, r_2 \div d, \dots, r_n \div d$ . В тоже время, рассматривая этот алгоритм с конца, получим последовательно  $r_{n-1} \div r_n, r_{n-2} \div r_n, \dots, b \div r_n, a \div r_n$ .

Итак,  $r_n$  — общий делитель чисел  $a$  и  $b$  и поэтому  $d \div r_n$ . Вместе с делимостью  $r_n \div d$  это дает, что  $r_n = d$ . ■

Из алгоритма (5) выпишем все последовательные неполные частные:  $q_1, q_2, \dots, q_n$  и по ним запишем выражение

$$\begin{aligned} q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots}} \dots + \frac{1}{q_{n-1} + \frac{1}{q_n}} \end{aligned} \tag{6}$$

Это выражение называется цепной дробью, построенной по числам

$q_1, q_2, \dots, q_n$ . Ее значение обозначается  $|q_1, q_2, \dots, q_n|$ , число  $n$  называется д л и н о й этой цепной дроби. ■□

**Теорема 5.** Если  $a > b$  и  $a \nmid b$ , то наибольший общий делитель чисел  $a$  и  $b$  может быть выражен через них с помощью определителя:

$$\text{НОД}(a, b) = (-1)^{n+1} \begin{vmatrix} a & b \\ P & Q \end{vmatrix}, \quad (7)$$

где  $P$  и  $Q$  - числитель и знаменатель несократимой дроби  $\frac{P}{Q}$ , равной значению цепной дроби (6),  $n$  - длина этой цепной дроби.

Доказательство. Если  $n=1$ , то в алгоритме Евклида только одно неполное частное, и легко видеть, что утверждение теоремы справедливо. Покажем, как из справедливости утверждения для значения  $n=k-1$  вытекает справедливость для следующего. Запишем алгоритм Евклида при значении  $n=k$ :

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ &\dots\dots\dots \\ r_{k-2} &= r_{k-1} \cdot q_k + r_k \\ r_{k-1} &= r_k \cdot q_{k+1}. \end{aligned} \quad (8)$$

Будем рассматривать алгоритм, начиная со второй строки. По существу, мы видим алгоритм нахождения наибольшего общего делителя для чисел  $b$  и  $r_1$ . Согласно предположению индукции будем иметь

$$\text{НОД}(b, r_1) = (-1)^k \begin{vmatrix} b & r_1 \\ P_1 & Q_1 \end{vmatrix}, \quad (9)$$

где  $P_1$  и  $Q_1$  - числитель и знаменатель несократимой дроби  $\frac{P_1}{Q_1} = |q_2, q_3, \dots, q_k|$ . Как видно из алгоритма (8),  $\text{НОД}(a, b) = \text{НОД}(b, r_1)$ .

Согласно (9) имеем

$$\text{НОД}(a, b) = (-1)^k \begin{vmatrix} b & r_1 \\ P_1 & Q_1 \end{vmatrix} = (-1)^k \begin{vmatrix} b & bq_1 + r_1 \\ P_1 & P_1q_1 + Q_1 \end{vmatrix} = (-1)^{k+1} \begin{vmatrix} a & b \\ P_1q_1 + Q_1 & P_1 \end{vmatrix}.$$

Осталось показать, что  $q_1P_1 + Q_1$  и  $P_1$  - числитель и знаменатель несократимой дроби, равной  $|q_1, q_2, \dots, q_n|$ . Дробь  $\frac{q_1P_1 + Q_1}{P_1}$  несократима,

## § 2. Алгоритм Евклида

---

так как в противном случае оказалась бы сократимой дробь  $\frac{P_1}{Q_1}$  и, кроме того, она представима в виде

$$q_1 + \frac{Q_1}{P_1} = q_1 + \frac{1}{\frac{P_1}{Q_1}} = q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_{k-1} + \frac{1}{q_k}}},$$

то есть равна  $|q_1, q_2, \dots, q_k|$ . ■□

□

□

**Пример 2.** Положим  $a = 272$ ,  $b = 50$ . Выполним алгоритм Евклида

$$\begin{array}{ll} 272 = 50 \cdot \mathbf{5} + 22 & \text{НОД}(272, 50) = 2, \\ 50 = 22 \cdot \mathbf{2} + 6 & \\ 22 = 6 \cdot \mathbf{3} + 4 & |5, 2, 3, 1| = 5 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1}}} = \frac{49}{9} \\ 6 = 4 \cdot \mathbf{1} + 2 & \\ 4 = 2 \cdot \mathbf{2} & \end{array}$$

$P = 49, Q = 9, n = 4.$

$$2 = (-1)^{4+1} \begin{vmatrix} 272 & 50 \\ 49 & 9 \end{vmatrix} = -272 \cdot 9 + 50 \cdot 49$$

### Схема вычисления цепной дроби.

Пусть нужно вычислить

$$\left| q_1, q_2, \dots, q_n \right| = q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_n}}$$

Составим таблицу, записав в верхней строке числа, определяющие цепную дробь, в *обратном* порядке:

$$\begin{array}{c|cccc} & q_n & q_{n-1} & \dots & q_2 & q_1 \\ \hline 1 & q_n & & & & \end{array} \quad (10)$$

Заполним нижнюю строку по правилу:

- каждое следующее число получается, если к произведению чисел, стоящих над ним и перед ним, прибавить предпоследнее из имеющихся чисел в нижней строке.

При таком заполнении таблицы справедлива следующая теорема.

**Теорема 6.** Последними числами в нижней строке таблицы (10) будут последовательно числа  $Q$  и  $P$  – знаменатель и числитель несократимой дроби, равной  $\left| q_1, q_2, \dots, q_n \right|$ .

Доказательство. Утверждение верно, когда  $n=2$ . Предположим, что оно справедливо при  $n=k-1$ . Рассмотрим схему при  $n=k$ :

$$\begin{array}{c|cccc} & q_k & q_{k-1} & \dots & q_2 & q_1 \\ \hline 1 & q_k & \dots & & Q_1 & Q & P \end{array}$$

Поскольку утверждение верно при  $n=k-1$ , то дробь  $\frac{Q}{Q_1}$  – несократимая и

$\frac{Q}{Q_1} = \left| q_2, q_3, \dots, q_k \right|$ . Поэтому дробь

$$\frac{P}{Q} = \left| q_1, q_2, \dots, q_k \right| = q_1 + \frac{1}{\left| q_2, q_3, \dots, q_k \right|} = q_1 + \frac{1}{\frac{Q}{Q_1}} = \frac{q_1 Q + Q_1}{Q}.$$

## § 2. Алгоритм Евклида

Полученная дробь несократима, так как в противном случае наибольший общий делитель  $P$  и  $Q$ , отличный от единицы, оказался бы общим делителем для  $Q$  и  $Q_1$ , что невозможно. ■□

Пример 3. Мы видели в примере (2), что  $|5, 2, 3, 1| = \frac{49}{9}$ . Проведем вычисление этого числа по схеме (10):

$$\begin{array}{c|cccc} & 1 & 3 & 2 & 5 \\ \hline 1 & 1 & 4 & 9 & 49 \end{array}$$

$$9 = Q, \quad 49 = P, \quad \frac{P}{Q} = \frac{49}{9} = |5, 2, 3, 1|.$$

**Теорема 7.** НОД чисел  $a_1, a_2, \dots, a_k$  является наименьшим натуральным числом в множестве всех линейных комбинаций этих чисел с целыми коэффициентами.

Доказательство. НОД  $(a_1, a_2, \dots, a_k)$  представляется в виде их линейной комбинации. В самом деле, при  $k=2$  это следует из теоремы 5 и из того, что  $\text{НОД}(a_1, a_2) = a_2$ , если  $a_1 \div a_2$ . При  $k=3$  имеем:

$\text{НОД}(a_1, a_2, a_3) = \text{НОД}(a_1, \text{НОД}(a_2, a_3)) = n_1 a_1 + m_1(a_2, a_3) = n_1 a_1 + n_2 a_2 + n_3 a_3$  при некоторых  $m_1, n_1, n_2, n_3 \in \mathbb{Z}$ . Аналогично поступаем при любом  $k > 3$ .

Пусть теперь  $d = n_1 a_1 + n_2 a_2 + \dots + n_k a_k$ , где  $n_1, n_2, \dots, n_k \in \mathbb{Z}$ , и  $d$  — наименьшее натуральное число среди комбинаций такого вида. Тогда  $d \div \text{НОД}(a_1, \dots, a_k)$ , так как все числа  $a_1, a_2, \dots, a_k$  делятся на  $\text{НОД}(a_1, \dots, a_k)$ , и поэтому  $d \geq \text{НОД}(a_1, \dots, a_k)$ . С другой стороны,  $d \leq \text{НОД}(a_1, \dots, a_k)$  по построению. Следовательно,  $d = \text{НОД}(a_1, \dots, a_k)$ . ■

Пример 4.  $\text{НОД}(12, 42, 32) = 2$  и  $2 = 1 \cdot 12 - 1 \cdot 42 + 1 \cdot 32$ .