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

Р. С. Адамова

ТЕОРИЯ ЧИСЕЛ

Учебно-методическое пособие

Воронеж
Издательский дом ВГУ
2018

§ 1. Делимость в множестве натуральных чисел

Пусть $a, b \in \boldsymbol{N}$.

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

$$a = b \cdot q$$

При этом пишут $a \,\vdots\, b$. Число q называют частным от деления a на b, число a называют кратным числа b (обозначают $a \,\vdots\, b$), а b – делителем числа a. Если a не делится на b, пишут $a \not\vdots\, b$.

Теорема 1. Если $a > b$ и $a \not\vdots\, b$, то существуют, и притом единственным образом, числа $q, r \in \boldsymbol{N}$ такие, что

$$a = b\,q + r, \qquad r < b. \;\square \tag{1}$$

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 $a_1, a_2, \ldots, a_k$ называется наибольший среди их общих делителей.

Он обозначается НОД $(a_1, a_2, \ldots, a_k)$ или, короче, $(a_1, a_2, \ldots, a_k)$.

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

Оно обозначается НОК $(a_1, a_2, \ldots, a_k)$ или $[a_1, a_2, \ldots, a_k]$.

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

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

$$\left(\frac{a_1}{c}, \frac{a_2}{c}, \ldots, \frac{a_k}{c}\right) = \frac{(a_1, a_2, \ldots, a_k)}{c} \tag{2}$$

$$\left[\frac{a_1}{c}, \ \frac{a_2}{c}, \ \ldots, \ \frac{a_k}{c}\right] = \frac{[a_1, \ a_2, \ \ldots, \ a_k]}{c}.$$

Доказательство.

§ 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 $a \vdots b$, то НОД$(a, b) = b$.

Рассмотрим другую ситуацию: $a > b$, $a \not\vdots b$. Выполним процесс последовательного деления.

$$
\begin{aligned}
a &= b \cdot q_1 + r_1 \\
b &= r_1 \cdot q_2 + r_2 \\
r_1 &= r_2 \cdot q_3 + r_3 \qquad (5) \\
&\ldots\ldots\ldots\ldots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n \\
r_{n-1} &= r_n \cdot q_{n+1}
\end{aligned}
$$

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

Теорема 4. Наибольшим общим делителем чисел a и b ($a > b$, $a \not\vdots b$) является последний остаток в процессе алгоритма Евклида последовательного деления a на b.

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

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

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

$$
q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} \qquad (6)
$$

Это выражение называется цепной дробью, построенной по числам $q_1, q_2, \ldots, q_n$. Ее значение обозначается $|q_1, q_2, \ldots, q_n|$, число n называется *длиной* этой цепной дроби. ■

Теорема 5. Если $a > b$ и $a \not\vdots b$, то наибольший общий делитель чисел a и b может быть выражен через них с помощью определителя:

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

где P и Q - числитель и знаменатель несократимой дроби $\dfrac{P}{Q}$, 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 $n = k$:

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

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

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

где P_1 и Q_1 - числитель и знаменатель несократимой дроби $\dfrac{P_1}{Q_1} = |q_2, q_3, \ldots, q_k|$. 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 $|q_1, q_2, \ldots, q_n|$. Дробь $\dfrac{q_1P_1 + Q_1}{P_1}$ несократима, так как в противном случае оказалась бы сократимой дробь $\dfrac{P_1}{Q_1}$ и, кроме того, она представима в виде

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

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

П р и м е р 2. Положим a = 272, b = 50. Выполним алгоритм Евклида

$$\begin{aligned} 272 &= 50 \cdot \mathbf{5} + 22 \\ 50 &= 22 \cdot \mathbf{2} + 6 \\ 22 &= 6 \cdot \mathbf{3} + 4 \\ 6 &= 4 \cdot \mathbf{1} + 2 \\ 4 &= 2 \cdot 2 \end{aligned} \qquad \begin{gathered} \text{НОД}\,(272, 50) = 2, \\ |\,5, 2, 3, 1\,| = 5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1}}} = \frac{49}{9} \\ P = 49, \quad Q = 9, \quad \text{n} = 4. \end{gathered}$$

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

Схема вычисления цепной дроби.

Пусть нужно вычислить

$$|\, q_1, q_2, \ldots, q_n \,| = q_1 + \cfrac{1}{q_2 + \dots \cfrac{}{\dots + \cfrac{1}{q_\text{n}}}}$$

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

$$\begin{array}{c|l} & q_n \;\; q_{\text{n}-1} \; \ldots \; q_2 \; q_1 \\ \hline 1 & q_n \end{array} \qquad (10)$$

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 $|q_1, q_2, \ldots, q_n|$.

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

	q_k	q_{k-1}	…	q_2	q_1	
1	q_k	…		Q_1	Q	P

Поскольку утверждение верно при $n = k–1$,то дробь $\dfrac{Q}{Q_1}$– несократимая и $\dfrac{Q}{Q_1} = |q_2, q_3, \ldots, q_k|$. Поэтому дробь

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

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 $|5, 2, 3, 1| = \dfrac{49}{9}$. Проведем вычисление этого числа по схеме (10) :

	1	3	2	5
1	1	4	9	49

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

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

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

НОД$(a_1, a_2, a_3) = (a_1(a_2, a_3)) = n_1a_1 + m_1(a_2, a_3) = n_1a_1 + n_2a_2 + n_3a_3$ при некоторых $m_1, n_1, n_2, n_3 \in \boldsymbol{Z}$. Аналогично поступаем при любом $k > 3$.

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

П р и м е р 4. НОД$(12, 42, 32) = 2$ и $2 = 1\cdot 12 - 1\cdot 42 + 1\cdot 32$.