§ 4. Вычисление наибольшего общего делителя и наименьшего общего кратного

Сохраним обозначения из параграфа 2. Для натурального числа n запись $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ означает каноническое разложение на простые множители.

Рассматривая одновременно два или более чисел, удобно включить в разложение каждого числа все простые делители этих чисел, отсутствующие – в нулевых степенях ($p^0 = 1$ для любого числа p). Например, для $715 = 5\cdot11\cdot13$, $364 = 2\cdot7\cdot13$ можно записать $715 = 2^0\cdot5\cdot7^0\cdot11\cdot13$, $364 = 2^2\cdot5^0\cdot7\cdot11^0\cdot13$.

Пусть $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $m = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, где $p_1<p_2<\dots<p_s$, k_i, $l_i \geq 0$ для всех $i = 1, 2, ..., s$. Верны следующие утверждения:

1. НОД(n, m) = $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где α_i – меньший из показателей k_i, l_i, $i = 1,\dots,s$. (IV)

2. НОК(n, m) = $p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, где β_i – больший из показателей k_i, l_i, $i = 1,\dots,s$. (V)

Пример 17. Доказать, что **НОД(n, m)·НОК(n, m) = nm.**

Решение. НОД(n, m)·НОК(n, m) = $p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_s^{\alpha_s+\beta_s}$, однако для каждого i от 1 до s из пары чисел α_i, β_i одно равно k_i, другое l_i, так что $\alpha_i + \beta_i = k_i + l_i$, откуда НОД($n$, m)·НОК(n, m) = $p_1^{k_1+l_1} p_2^{k_2+l_2} \dots p_s^{k_s+l_s} = nm$, что и требовалось доказать.

3. *Количество делителей $d(n)$ числа* $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ вычисляется по формуле $d(n)=(k_1+1)(k_2+1)\dots(k_m+1)$. (VI)

В самом деле, любой делитель имеет вид $d = p_1^{l_1} p_2^{l_2} \dots p_m^{l_m}$, где каждый показатель степени l_i, независимо от остальных, принимает $k_i + 1$ значений, поэтому эти количества надо перемножить. Так, количество делителей числа $496 = 2^4\cdot31$ (пример 13) равно $(4 + 1)(1 + 1) = 10$.

Пример 18. Найти общий вид натуральных чисел, имеющих ровно 2009 делителей.

Решение. По условию, число $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ имеет, в силу (VI), $d(n) = (k_1 + 1)\dots(k_m + 1) = 2009 = 41\cdot 7^2$ делителей. Для $d(n)$ есть такие варианты разложения на множители: $2009 = 41\cdot 49 = 287\cdot 7 = 41\cdot 7\cdot 7$. Соответственно n имеет либо единственный простой делитель с показателем 2008, либо два различных простых делителя с показателями $k_1 = 40, k_2 = 48$ или $k_1 = 6, k_2 = 286$, либо три различных простых делителя с показателями $k_1 = k_2 = 6, k_3 = 40$.

Ответ: $n = p^{2008}$, где p – простое число, либо $n = p_1^{40} p_2^{48}$ или $n = p_1^6 p_2^{286}$, где p_1, p_2 – различные простые числа, либо $n = p_1^6 p_2^6 p_3^{40}$, где p_1, p_2, p_3 – различные простые числа.

Примечание. Из формулы (VI) ясно, что число n, имеющее нечётное число делителей, является квадратом натурального числа, и обратно, так как в этом случае все показатели в каноническом разложении числа n будут чётными.

Понятия наибольшего общего делителя и наименьшего общего кратного легко распространить на любой конечный набор натуральных чисел $a_1, a_2, \dots, a_m$. А именно, натуральное число d называется их наибольшим общим делителем, если оно делит (без остатка) все данные числа и само делится на любой их общий делитель. Натуральное число N называется наименьшим общим кратным чисел $a_1, a_2, \dots, a_m$, если N кратно всем этим числам и делит любое их общее кратное. Правила вычисления НОД и НОК по каноническим разложениям такие же, как и для двух чисел. При этом их можно находить последовательно, пользуясь равенствами

$$\text{НОД}(a_1, a_2, a_3) = \text{НОД}(\text{НОД}(a_1, a_2), a_3) \text{ и}$$

$$\text{НОК}(a_1, a_2, a_3) = \text{НОК}(\text{НОК}(a_1, a_2), a_3).$$

Пример 19. (МГУ, олимпиада «Ломоносов-2007») Натуральные числа *a, b, c* таковы, что НОК(*a,b*) = 120, НОК(*a,c*) = 150. Найти НОК(*b,c*).

Решение. Так как НОК(*a,b*) = 120 = $2^3\cdot 3\cdot 5$, а НОК(*a,c*) = 150 = $2\cdot 3\cdot 5^2$, то, согласно правилу (V), $b \vdots 2^3 = 8,\ c \vdots 5^2 = 25$, а, поскольку числа 8 и 25 взаимно простые, то, по свойству 5 делимости, $\text{НОК}(b, c) \vdots (8\cdot 25) = 200$. С другой стороны, НОК($a,b,c$) = НОК($a$, НОК($b,c$)) = $2^3 \cdot 3 \cdot 5^2$ = 600 делится на НОК(b,c), следовательно, НОК(b,c) = 200 (это возможно при $b = 2^3 \cdot 5$, $c = 2 \cdot 5^2$, $a = 1$) или НОК(b,c) = 600 (что возможно при $b = 3 \cdot 2^3 \cdot 5$, $c = 5^2$, $a = 3$).

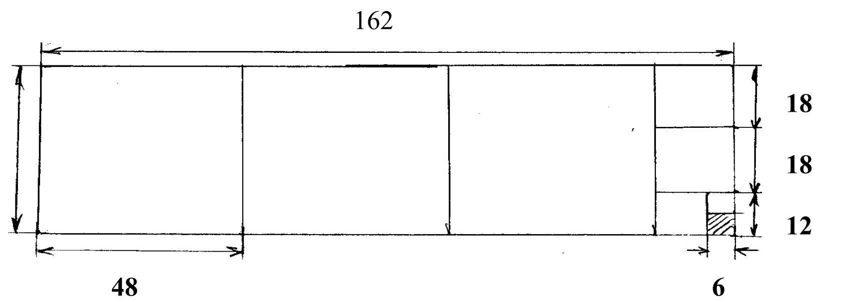
Ответ: НОК(b,c) = 200 или 600.

При решении уравнений в целых числах приходится использовать разложение целых чисел не только на положительные, но и на отрицательные множители. В таком случае каноническим разложением следует считать разложение $n = (\pm p_1^{k_1})(\pm p_2^{k_2})\ldots(\pm p_s^{k_s})$, причём знаки можно комбинировать любым способом так, чтобы знак произведения совпадал со знаком числа n.

Чтобы найти НОД двух натуральных чисел a и b, не обязательно знать их разложения на простые множители. Существует иной способ, использующий многократное деление с остатком. Он известен как **алгоритм Евклида.**

Вначале покажем способ на наглядном примере.

Пример 20. От прямоугольника 162мм × 48мм отрезали несколько квадратов со стороной 48 мм, пока не остался прямоугольник, у которого одна сторона короче 48 мм. От полученного прямоугольника отрезают квадраты, у которых сторона равна меньшей стороне прямоугольника, до тех пор, пока это возможно. Чему равна сторона последнего квадрата?



Решение. Начертим заданный прямоугольник.

Откладываем 48 мм на большой стороне прямоугольника. Так как $162 = 3 \cdot 48 + 18$, то получим три квадрата 48 мм × 48 мм и прямоугольник 48 мм × 18 мм ($r_1 = 18$ есть остаток от деления числа 162 на 48). На большей стороне нового прямоугольника откладываем его меньшую сторону: $48 = 2 \cdot 18 + 12$. Получим два квадрата 18 мм × 18 мм и прямоугольник 18 мм × 12 мм ($r_2 = 12$ есть остаток от деления 48 на 18). Этот прямоугольник содержит в себе один квадрат 12 мм × 12 мм и прямоугольник

12 мм × 6 мм, который, в свою очередь, состоит из двух квадратов 6 мм × 6 мм.

Ответ: сторона последнего квадрата равна 6 мм.

Заметим, что длина стороны последнего полученного квадрата есть не что иное, как наибольший общий делитель его сторон, т.к. НОД (162, 48) = 6. И он был найден в результате нескольких делений с остатком (при разрезании прямоугольника на квадраты).

Опишем **алгоритм Евклида**.

Допустим, что $a > b,$ и разделим a на b с остатком: $a = bq_0 + r_1$.

Если $r_1 = 0$, то d = НОД$(a,b) = b$; если $r_1 \neq 0$, то **НОД(a,b) = НОД(b,r_1)**. В самом деле, так как a, b делятся на d , то и r_1 делится на d , по свойству 1 делимости. Наоборот, если c делитель b и r_1 , то число $a = bq_0 + r_1$ будет делиться на c , т.е. c является общим делителем a и b.

Затем разделим b на r_1: $b = r_1q_1 + r_2$. Если $r_2 = 0$, то НОД $(b,r_1) = r_1 = d$. В случае $r_2 \neq 0$ получим d = НОД(b,r_1) = НОД(r_1,r_2). Теперь разделим r_1 с остатком на $r_2 < r_1$: $r_1 = r_2q_2 + r_3$ и т.д. Так как после каждого деления числа уменьшаются: $a > b > r_1 > r_2 >, \ldots$ то найдётся такой номер $k,$ что $r_{k-2} = r_{k-1}q_{k-1} + r_k$, $r_k \neq 0,$ $r_{k-1} = r_kq_k$. На этом процесс закончится, причём d = НОД(a,b) = НОД $(r_{k-1}, r_k) = r_k$.

Пример 21. Найти НОД(1176, 315).

Решение оформим в виде последовательности делений с остатком.

1176=3·315+231			315=1·231+84			231=2·84+63			84=1·63+**21**			63 = 3·**21**	
a	b	r_1	b	r_1	r_2	r_1	r_2	r_3	r_2	r_3	$\boldsymbol{r_4}$	r_3	$\boldsymbol{r_4=d}$

Ответ: НОД(1176, 315) = 21.

Примечание. С помощью алгоритма Евклида

можно найти такие целые числа x, y, что $ax + by = d$ **.**

Покажем это для чисел примера 24. Имеем $d = r_4 = r_2 - r_3$, $r_3 = r_1 - 2r_2$, $r_2 = b - r_1$, $r_1 = a - 3b$. Подставляя эти соотношения, находим $d = r_2 - (r_1 - 2r_2) = 3r_2 - r_1 = 3(b - r_1) - r_1 = 3b - 4r_1 = 3b - 4(a - 3b) = -4a + 15b$.

Окончательно, – 4·1176 + 15·315 = 21.

В следующем примере не обойтись без алгоритма Евклида. Разложить приведённые в нём числа на простые множители вряд ли возможно без математического пакета.

Пример 22. Найти НОД и НОК чисел a = 11…11 (20 цифр) и b = 22…22 (10 цифр).

Решение. Поскольку первое число нечётное, то 2 не является общим делителем данных чисел. Поэтому НОД(a, b) = НОД(a, 1111111111) = 1111111111, так как $\underbrace{11...11}_{20}=\underbrace{11...11}_{10}\cdot\underbrace{10...01}_{11}$.

Ответ: 1111111111 (10 цифр).

Общий делитель приходится искать при исследовании сократимости рациональных дробей целого аргумента.

Пример 23. Определить, на какие натуральные числа может сокращаться дробь $\dfrac{5x-1}{3x+4}$ при целых x.

Решение. Пусть d — общий делитель числителя и знаменателя. Тогда $\begin{cases}5x-1=dk,\\ 3x+4=dl\end{cases}$ для подходящих целых k, l. Исключим x из этих уравнений:

$\begin{cases}15x-3=3dk,\\ 15x+20=5dl\end{cases}$ $\Rightarrow d(5l-3k)=23$, а т.к. 23 – простое число, то d = 23.

Ответ: *на* 23.

Замечание. Чтобы найти все значения x, при которых это возможно, требуется решить уравнение $\mathbf{5l-3k=1}$. Решение подобных уравнений в целых числах рассматривается в следующем параграфе.

Историческая сводка. Числа, которые, наподобие числа 496, равны сумме своих собственных делителей, ещё в древности были названы *совершенными.* Первые совершенные числа 6 и 28 были известны в древнем Вавилоне, следующее за 496 совершенное число 8128.

Евклид, живший в 3 веке до н.э. и три тома своего труда «Начала» посвятивший арифметике, доказал, что множество простых чисел бесконечно. Составлять таблицу простых чисел начали ещё древние греки (школа Пифагора, V век до н.э.). По мере накопления простых чисел стало ясно, что никакой общей формулы для их вычисления не существует. Поэтому стали искать формулы, дающие много простых чисел.

Пьер Ферма занимался изучением чисел вида $F=2^m+1$. Такие числа могут быть простыми только при $m=2^k$ (k = 0, 1, 2, ...). В самом деле, если допустить, что $m = 2^k l$, причём число l нечётное, то $F = \left(2^{2^k}\right)^l + 1 =$ $= \left(2^{2^k} + 1\right)\left(2^{2^k - 1} - 2^{2^k - 2} + \cdots\right)$, по формуле (II). Первые числа Ферма $F_k = 2^{2^k} + 1$: $F_0 = 2$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$ являются простыми. Однако больше ни одного простого числа Ферма по сей день не обнаружено, даже с помощью современных компьютеров! Между прочим, числа Ферма участвуют в решении задачи построения правильных многоугольников циркулем и линейкой. Гаусс доказал, что правильный n-угольник только тогда может быть построен, когда разложение n на простые множители имеет вид $n = 2^m \cdot p_1 p_2 \ldots p_s$, $m \geq 0, p_1, ..., p_s$ – различные простые числа Ферма.

Числа вида $2^n - 1$ могут быть простыми лишь при простом n: если $n = mk$, то $2^n - 1$ делится на $2^m - 1$ и $2^k - 1$. Простые числа вида $2^p - 1$ (p – простое число) называют числами Мерсенна и обозначают $M(p)$ (Мерсенн – французский математик, 1588–1648). Наибольшие из известных пока простых чисел являются числами Мерсенна. С 1995 года охота за простыми числами приняла глобальный характер: был создан проект поиска простых чисел с помощью компьютеров, объединённых сетью Интернета (GIMPS – the Great Internet Mersenne Prime Search). С такими огромными числами оказалось возможным работать только благодаря организации взаимодействия сотен тысяч компьютеров (на специальном сайте PrimeNet, http://www.mersenne.org). На сегодняшний день (начало 2010 года) известны 47 простых чисел M(p). 23 августа и 6 сентября 2008 года проверена простота двух очередных чисел Мерсенна, самое большое из них, M(43112609) (№ 45), состоит из 12978189 цифр; более 10 миллионов цифр имеет также число M(37156667) (№ 46). Самое свежее открытие 47-го простого числа Мерсенна произошло 12 апреля 2009 года, в нём 12834064 цифры.

Числа Мерсенна тесно связаны с совершенными числами. Теорема 36 в «Началах» Евклида гласит: если число $n = 2^p - 1$ простое, то число $N = n \cdot 2^{p-1}$ является совершенным. Эту теорему нам сейчас легко доказать. Так как число n простое, то все собственные делители N имеют вид 2^k, где $0 \leq k \leq p-1$, или $n \cdot 2^k$ при $0 \leq k \leq p-2$. Их сумма, согласно формуле (I), равна

$$1 + 2 + \ldots + 2^{p-1} + n \cdot (1 + 2 + \ldots + 2^{p-2}) = \frac{2^p - 1}{2 - 1} + n \cdot \frac{2^{p-1} - 1}{2 - 1} =$$

$$= n \cdot 2^{p-1} + (2^p - 1) - n = N.$$

Леонард Эйлер (1707 – 1783), швейцарский математик, который долгое время работал в Петербурге и прославился трудами по теории чисел, алгебре и другим разделам математики, показал, что любое четное совершенное число можно представить в таком виде. Так что каждое новое простое число Мерсенна даёт и ещё одно совершенное число. Всего известны 52 чётных совершенных числа. Нечётных совершенных чисел до сих пор не открыто, а попытки любителей доказать их отсутствие элементарными средствами воспринимаются специалистами почти как попытки элементарно доказать Великую теорему Ферма.