Наибольший общий делитель и наименьшее общее кратное

Определение 1.6. Целое число $d \neq 0$ называется *наибольшим общим делителем* целых чисел $a_1, a_2, \ldots, a_k$ (обозначается $d = \text{НОД}(a_1, a_2, \ldots, a_k)$), если выполняются следующие условия:

1) каждое из чисел $a_1, a_2, \ldots, a_k$ делится на d;
2) если $d_1 \neq 0$ — другой общий делитель чисел $a_1, a_2, \ldots, a_k$, то d делится на d_1.

Пример 1.9. НОД(12345, 24690) = 12345; НОД(12345, 54321) = = 3; НОД(12345, 12541) = 1. □

Ненулевые целые числа a и b называются *ассоциированными* (обозначается $a \sim b$), если a делится на b и b делится на a.

Теорема 1.2 (об ассоциированных числах). Числа a и b ассоциированы тогда и только тогда, когда $a = \pm b$.

Доказательство. Пусть a делится на b, тогда существует такое целое число c, что $a = b \cdot c$. Поскольку $|c| \geq 1$, получаем $|a| = |b| \cdot |c| \geq |b| \cdot 1 = |b|$, то есть $|a| \geq |b|$.

В то же время b делится на a. Проводя аналогичные выкладки, получаем $|b| \geq |a|$. Таким образом, $|a| = |b|$, то есть $a = \pm b$. □

Теорема 1.3 (о единственности наибольшего общего делителя). Пусть числа $a_1, a_2, \ldots, a_k$ целые и d_1 — их наибольший общий делитель. Целое число d_2 является наибольшим общим делителем чисел $a_1, a_2, \ldots, a_k$ тогда и только тогда, когда $d_2 \sim d_1$.

Теорема 1.4 (о существовании и линейном представлении наибольшего общего делителя). Для любых целых чисел $a_1, a_2, \ldots, a_k$ существует наибольший общий делитель d, и его можно представить в виде линейной комбинации этих чисел: $d = c_1a_1 + c_2a_2 + \ldots + c_ka_k$, где $c_i \in \mathbb{Z}$.

Пример 1.10. Наибольший общий делитель чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять, например,

$$7 = 7 \cdot 91 + (-6) \cdot 105 + 0 \cdot 154$$

или

$$7 = 4 \cdot 91 + 1 \cdot 105 - 3 \cdot 154. \qquad \square$$

Определение 1.7. Целые числа $a_1, a_2, \ldots, a_k$ называются *взаимно простыми в совокупности*, если НОД$(a_1, a_2, \ldots, a_k) = 1$. Целые числа a и b называются *взаимно простыми*, если НОД$(a, b) = 1$.

Определение 1.8. Целые числа $a_1, a_2, \ldots, a_k$ называются *попарно взаимно простыми*, если НОД$(a_i, a_j) = 1$ для всех $1 \le i \ne j \le k$.

Пример 1.11. Числа 3, 6, 8 взаимно просты в совокупности, так как НОД(3, 6, 8) = 1. Числа 3, 5, 8 попарно взаимно просты. $\square$

Взаимно простые числа обладают следующими свойствами.

1. Для того чтобы целые числа $a_1, a_2, \ldots, a_k$ были взаимно простыми в совокупности, необходимо и достаточно, чтобы существовали такие целые числа $c_1, c_2, \ldots, c_k$, что $c_1a_1 + c_2a_2 + \ldots + c_ka_k = 1$.

$1'$. Для того чтобы целые числа a, b были взаимно простыми, необходимо и достаточно, чтобы существовали такие целые числа m, n, что $ma + nb = 1$.

2. Пусть произведение ab делится на c и НОД$(a, c) = 1$. Тогда b делится на c.

3. Если НОД$(a, b) = 1$, НОД$(a, c) = 1$, то НОД$(a, bc) = 1$.

4. Если НОД$(a, b_1) = 1$, НОД$(a, b_2) = 1$, …, НОД$(a, b_k) = 1$, то НОД$(a, b_1 b_2 \ldots b_k) = 1$.

5. Пусть целые числа $a_1, a_2, \ldots, a_l, b_1, b_2, \ldots, b_k$ таковы, что НОД$(a_i, b_j) = 1$ для всех $1 \le i \le l$, $1 \le j \le k$. Тогда НОД$(a_1 a_2 \ldots a_l, b_1 b_2 \ldots b_k) = 1$.

6. Пусть целое число a делится на b_1 и на b_2, НОД$(b_1, b_2) = 1$. Тогда a делится на произведение $b_1 b_2$.

7. Если a делится на каждое из попарно взаимно простых чисел $b_1, b_2, \ldots, b_k$, то a делится на произведение $b_1 b_2 \ldots b_k$.

Определение 1.9. Целое число M называется *наименьшим общим кратным* целых чисел $a_1, a_2, \ldots, a_k$, $a_i \ne 0$ для $i = 1, 2, \ldots, k$, (обозначается $M = \text{НОК}(a_1, a_2, \ldots, a_k)$), если выполняются следующие условия:

1) M делится на каждое из чисел $a_1, a_2, \ldots, a_k$;
2) если M_1 — другое общее кратное чисел $a_1, a_2, \ldots, a_k$, то M_1 делится на M.

Пример 1.12. $\text{НОК}(12345, 24690) = 24690$; $\text{НОК}(12345, 54321) = 223530915$; $\text{НОК}(12345, 12541) = 154818645$. □

Наибольший общий делитель и наименьшее общее кратное двух положительных целых чисел связаны соотношением:

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab.$$

Пример 1.13. $\text{НОД}(12345, 24690) \cdot \text{НОК}(12345, 24690) = 12345 \times 24690 = 304798050$; $\text{НОД}(12345, 54321) \cdot \text{НОК}(12345, 54321) = 3 \times 223530915 = 670592745 = 12345 \cdot 54321$; $\text{НОД}(12345, 12541) \cdot \text{НОК}(12345, 12541) = 1 \cdot 154818645 = 12345 \cdot 12541$. □

1.3. Вычисление наибольшего общего делителя

1.3.1. Алгоритм Евклида

Для вычисления наибольшего общего делителя двух целых чисел применяется способ повторного деления с остатком, называемый *алгоритмом Евклида*.

Алгоритм 1.1. Алгоритм Евклида.

Вход. Целые числа a, b; $0 < b \le a$.

Выход. $d = \text{НОД}(a, b)$.

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$.
2. Найти остаток r_{i+1} от деления r_{i-1} на r_i.

3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$. В противном случае положить $i \leftarrow i + 1$ и вернуться на шаг 2.

4. Результат: d. □

Сложность алгоритма Евклида равна $O(\log^2 a)$.

Для доказательства корректности алгоритма Евклида нам понадобятся две леммы.

Лемма 1.5. Если числа a и b целые и a делится на b, то $b = \text{НОД}(a, b)$.

Доказательство. Пусть $d = \text{НОД}(a, b)$, тогда по теореме 1.4 существуют такие целые числа m, n, что $d = ma + nb$. Поскольку a делится на b, то сумма в правой части равенства делится на b, а значит и d делится на b. В то же время b делится на d как на наибольший общий делитель. Таким образом, числа d и b ассоциированы и равны с точностью до знака. □

Лемма 1.6. Для любых целых чисел a, b, c выполняется равенство $\text{НОД}(a + cb, b) = \text{НОД}(a, b)$.

Доказательство. Пусть $d = \text{НОД}(a, b)$. Тогда a делится на d, b делится на d, значит, по свойству 2 делимости, и сумма $a + cb$ делится на d, то есть d — общий делитель чисел $a + cb$ и b.

Пусть d_1 — произвольный общий делитель чисел $a + cb$ и b. Тогда число $a = (a + cb) - cb$ делится на d_1, то есть d_1 — общий делитель чисел a и b. А так как делитель d наибольший, то d делится на d_1, и d — наибольший общий делитель чисел $a + cb$ и b. □

Пример 1.14. Используя алгоритм Евклида, найдем такие целые числа n, для которых дробь $\dfrac{3n+4}{8n+5}$ несократима [4]. Дробь несократима, если ее числитель и знаменатель взаимно просты. Построим последовательность наибольших общих делителей, используя лемму 1.6:

$$\text{НОД}(3n+4,\, 8n+5) = \text{НОД}(3n+4,\, 2\cdot(3n+4)+2n-3) =$$

$$= \text{НОД}(3n+4,\, 2n-3) = \text{НОД}(2n-3+n+7,\, 2n-3) =$$

$$= \text{НОД}(n+7,\, 2n-3) = \text{НОД}(n+7,\, 2\cdot(n+7)-17) = \text{НОД}(n+7,\, -17) =$$

$$= \text{НОД}(n+7,\, 17).$$

Таким образом, чтобы дробь была несократима, нужно, чтобы число $n+7$ не делилось на 17, то есть чтобы n имело вид $17q+r$, где $0 \le r \le 16$, $r \ne 10$. Действительно, при $r = 10$ получаем

$$\frac{3(17q+10)+4}{8(17q+10)+5} = \frac{3\cdot 17q+34}{8\cdot 17q+85} = \frac{17(3q+2)}{17(8q+5)} = \frac{3q+2}{8q+5}. \qquad \square$$

Теорема 1.7. Для любых a, $b > 0$ алгоритм Евклида останавливается и выдаваемое им число d является наибольшим общим делителем чисел a и b.

Доказательство. По теореме о делении с остатком для любого $i \ge 1$ имеем $r_{i-1} = q_i r_i + r_{i+1}$, где $0 \le r_{i+1} < r_i$. Получаем монотонно убывающую последовательность неотрицательных целых чисел $r_1 > r_2 > r_3 > \ldots \ge 0$, ограниченную снизу. Такая последовательность не может быть бесконечной, следовательно, алгоритм Евклида останавливается.

Докажем теперь, что число d — наибольший общий делитель для чисел $r_1, r_2, \ldots, r_k$, где r_{k-1} делится на r_k. С учетом леммы 1.6 можем записать:

$$\text{НОД}(a, b) = \text{НОД}(r_0, r_1) = \text{НОД}(q_1 r_1 + r_2, r_1) = \text{НОД}(r_1, r_2) =$$

$$= \text{НОД}(r_2, r_3) = \ldots = \text{НОД}(r_{k-1}, r_k).$$

А по лемме 1.5 получаем $\text{НОД}(r_{k-1}, r_k) = r_k = d$. $\square$

Посмотрим, для каких целых чисел алгоритм Евклида выполняет больше всего итераций.

Напомним, что *последовательностью Фибоначчи* $\{F_k\}$, где $k \in \mathbb{N}$, называется последовательность, элементы которой связаны соотношением: $F_{k+1} = F_k + F_{k-1}$ для $k \geq 2$, при этом $F_1 = F_2 = 1$:

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

Найдем наибольший общий делитель для чисел Фибоначчи F_{k+2} и F_{k+1}: НОД(F_{k+2}, F_{k+1}) = по определению чисел Фибоначчи = НОД(F_{k+1} + + F_k, F_{k+1}) = по лемме 1.6 = НОД(F_{k+1}, F_k) = … = НОД(F_2, F_1) = = НОД(1, 1) = 1. Таким образом, для вычисления наибольшего общего делителя требуется ровно k итераций. □

Пример 1.15. Пусть $a = F_6 = 8$, $b = F_5 = 5$. Тогда за четыре шага: $8 = 1 \cdot 5 + 3$, $5 = 1 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$ — находим НОД(a, b) = 1. □

Лемма 1.8. При $k \geq 2$ справедливо неравенство $F_k \geq \phi^{k-2}$, где $\phi = \dfrac{1+\sqrt{5}}{2}$ — корень квадратного уравнения $x^2 - x - 1 = 0$ («золотое сечение»).

Доказательство [5] проведем методом математической индукции. При $k = 2$ имеем $F_2 = 1 \geq \phi^0 = 1$.

Индукционный переход:

$$F_{k+1} = F_k + F_{k-1} \geq \phi^{k-2} + \phi^{k-3} = \phi^{k-3}(\phi + 1) = \phi^{k-3}\phi^2 = \phi^{k-1}. \quad \square$$

Теорема 1.9 (Ламэ). Для целых чисел a, b, N таких, что $0 < b < a \leq N$, число итераций в алгоритме Евклида для a и b не превосходит $1 + \left[\log_\phi N\right]$.

Доказательство [5]. Пусть НОД(a, b) = НОД(r_0, r_1) = НОД(r_1, r_2) = = … = НОД(r_{k-1}, r_k) = r_k. Сначала индукцией по i докажем, что $F_i \leq r_{k-(i-1)}$ для $i = 1, 2, \ldots, k + 1$. При $i = 1$ имеем $F_1 = 1 \leq$ НОД(a, b) = r_k; при $i = 2$ —

$F_2 = 1 \le$ НОД$(a, b) = r_k < r_{k-1}$. Индукционный переход — делим с остатком r_{k-i} на r_{k+1-i}:

$$r_{k-i} = q_{k-(i-1)} r_{k-(i-1)} + r_{k-(i-2)} \ge r_{k-(i-1)} + r_{k-(i-2)} \ge F_i + F_{i-1} = F_{i-1}.$$

Отсюда

$$N \ge a = r_0 \ge F_{k+1} \ge \phi^{k-1}$$

(в последнем неравенстве мы воспользовались леммой 1.8). Логарифмируя неравенство $\phi^{k-1} \le N$, получаем требуемую оценку числа итераций в алгоритме Евклида: $k \le 1 + \left[\log_\phi N\right]$. □