Алгоритм Евклида

Рассмотрим задачу поиска наибольшего общего делителя g для двух натуральных чисел a и b. Алгоритм Евклида для решения этой задачи основан на наблюдении, что d – общий делитель чисел (a, b) тогда и только тогда, когда d – общий делитель чисел $(a - b, b)$. Действительно, пусть d – общий делитель (a, b). Следовательно, $a = dn$, $b = dm$ для некоторых целых n, m и $a - b = d(n - m)$. Значит, d – общий делитель для $(a - b, b)$. В обратную сторону доказательство аналогично. Таким образом, переход от пары чисел (a, b) к паре $(a - b, b)$ сохраняет множество общих делителей, а следовательно, и наибольший общий делитель. Применяя этот переход несколько раз, получаем, что пара $(a - kb, b)$, где k – некоторое натуральное число, имеет те же общие делители, что и пара (a, b).

Пусть, не ограничивая общности, $a > b$. Поделим a на b с остатком, т.е. найдем $q, r : a = qb + r,\ 0 \leq r < b$. Теперь можно перейти от пары (a, b) к паре $(b, a - qb) = (b, r)$ с сохранением множества общих делителей. Далее этот процесс можно повторить, переходя от пары (b, r) к паре (r, r_2), где $b = q_2 r + r_2$. При каждом таком переходе числа в паре уменьшаются, но остаются неотрицательными. Следовательно, за конечное число шагов образуется пара вида $(r_n, 0)$, для которой наибольший общий делитель $g = r_n$. В результате общая схема алгоритма Евклида выглядит следующим образом:

$$
\begin{aligned}
&r_{-2} = a,\\
&r_{-1} = b,\\
&r_{-2} = r_{-1}q_0 + r_0,\ r_0 < r_{-1},\ \text{// Делим } r_{-2} \text{ на } r_{-1} \text{ с остатком}\\
&r_{-1} = r_0 q_1 + r_1,\ r_1 < r_0,\ \text{// Делим } r_{-1} \text{ на } r_0 \text{ с остатком}\\
&\dots\\
&r_{n-2} = r_{n-1}q_n + r_n,\ \text{// Делим } r_{n-2} \text{ на } r_{n-1} \text{ с остатком}\\
&r_{n-1} = r_n q_{n+1}.
\end{aligned}
\tag{1}
$$

Наибольший общий делитель $g = r_n$.

Пример. Найдём $g = \text{НОД}(252, 105)$. Применяя схему (1), получаем:

$$
\begin{aligned}
252 &= 105 \cdot 2 + 42,\\
105 &= 42 \cdot 2 + 21,\\
42 &= 21 \cdot 2.
\end{aligned}
$$

Отсюда $g = 21$.

Для поиска наибольшего общего делителя трех и более чисел можно воспользоваться свойством

$$\text{НОД}(a, b, c) = \text{НОД}(a, \text{НОД}(b, c))$$

и запускать алгоритм Евклида несколько раз. Для поиска наименьшего общего кратного двух чисел можно воспользоваться свойством

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

Для $g = \text{НОД}(a, b)$ справедлива теорема Безу: найдутся $x, y \in \mathbb{Z}$ такие, что $g = ax + by$. Это утверждение легко доказать, «раскручивая» схему (1) в обратную сторону. Действительно, $g = r_n = r_{n-2} - r_{n-1}q_n$. Подставляя в это равенство значение $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, получаем, что $g = -q_n r_{n-3} + (1 + q_n q_{n-1})r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$ для некоторых $\alpha, \beta \in \mathbb{Z}$. Продолжая эти рассуждения, получим утверждение теоремы. Модификация схемы (1), позволяющая вместе с наибольшим общим делителем найти числа x, y из теоремы Безу, получила название *расширенного алгоритма Евклида.*

Будем искать $x_i, y_i \in \mathbb{Z}$, для которых справедливо $r_i = ax_i + by_i$, где $r_i, i = -2, \ldots, n$ – остатки из алгоритма Евклида (1). Для $i = -2, -1$ решение записывается как

$$x_{-2} = 1,\ x_{-1} = 0,$$
$$y_{-2} = 0,\ y_{-1} = 1.$$

Пусть верно $r_{i-2} = ax_{i-2} + by_{i-2}$, $r_{i-1} = ax_{i-1} + by_{i-1}$. Тогда найдем x_i, y_i:

$$r_i = r_{i-2} - q_i r_{i-1} = (ax_{i-2} + by_{i-2}) - q_i(ax_{i-1} + by_{i-1}) = a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = ax_i + by_i.$$

Следовательно, $x_i = x_{i-2} - q_i x_{i-1}, y_i = y_{i-2} - q_i y_{i-1}$. В итоге расширенный алгоритм Евклида повторяет схему (1), в которой на каждом шаге дополнительно вычисляются x_i, y_i по приведённым формулам.

Пример. Расширим предыдущий пример и найдем $g, x, y \in \mathbb{Z} : g = 252x + 105y$. Сведём все вычисления в таблицу:

i	r_{i-2}	r_{i-1}	q_i	r_i	x_i	y_i
-2				252	1	0
-1				105	0	1
0	252	105	2	42	1	-2
1	105	42	2	21	-2	5
2	42	21	2	0	5	-12

Таким образом, $g = 21, x = -2, y = 5$.

Алгоритм Евклида (а также его расширенная версия) может быть применен не только для случая целых чисел. Он остаётся справедливым в любом евклидовом кольце R, т.е. таком целостном кольце, в котором для любых двух ненулевых элементов возможна процедура деления с остатком, причём норма остатка меньше нормы делителя:

$$\forall a, b \in R, b \neq 0 \quad a = bq + r,\ 0 \leq \mathrm{norm}(r) < \mathrm{norm}(b).$$

Примером евклидова кольца является кольцо многочленов $F[x]$ над произвольным полем F, где в качестве нормы выступает степень многочлена.

С помощью расширенного алгоритма Евклида легко находить обратные элементы в конечных полях. Пусть имеется поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(f(x))$, где $f(x)$ – неприводимый полином степени n над $\mathbb{F}_p$. Тогда обратный элемент h для некоторого многочлена g из поля $\mathbb{F}_p^n$ определяется условием:

$$g(x)h(x) \equiv 1 \mod f(x).$$

Данное уравнение эквивалентно следующему

$$f(x)a(x) + g(x)h(x) = 1.$$

Оно может быть решено путем применения расширенного алгоритма Евклида для пары многочленов (f, g). Заметим, что решение данного уравнения всегда существует, т.к. f – неприводимый полином, степень g всегда меньше, чем степень f, и поэтому НОД$(f, g) = 1$.

Пример. Найдём обратный элемент для $x^2 + x + 3$ в поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$. Для этого решим уравнение

$$(x^4 + x^3 + x^2 + 3)a(x) + (x^2 + x + 3)b(x) = 1 \tag{2}$$

с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^4 + x^3 + x^2 + 3$,
$r_{-1}(x) = x^2 + x + 3$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
$q_0(x) = x^2 + 5$,
$r_0(x) = 2x + 2$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2 - 5$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
$q_1(x) = 4x$,
$r_1(x) = 3$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2 + 5) = 4x^3 + 6x + 1$.

Заметим, что в итерациях алгоритма нет необходимости вычислять $x_i(x)$, т.е. коэффициент при $x^4 + x^3 + x^2 + 3$, т.к. нас интересует только коэффициент при $x^2 + x + 3$, т.е. $y_i(x)$. Алгоритм заканчивает свою работу на шаге 2, т.к. степень очередного остатка r_1 равна степени многочлена в правой части (2). Однако, сам остаток r_1 отличается от требуемого на константный множитель. Действительно, после шага 2 мы имеем

$$(x^4 + x^3 + x^2 + 3)x_1(x) + (x^2 + x + 3)y_1(x) = 3.$$

Чтобы получить решение уравнения (2), достаточно домножить последний результат на $3^{-1} = 5$:

$$h(x) = 5y_1(x) = 5(4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Если на последнем шаге алгоритма Евклида текущий остаток не является требуемым с точностью до константного множителя, то соответствующее уравнение не имеет решения.

Расширенный алгоритм Евклида также активно применяется для декодирования БЧХ кодов.