Бинарный алгоритм Евклида

Этот вариант алгоритма Евклида оказывается более быстрым при реализации на компьютере, поскольку использует двоичное представление чисел a и b. *Бинарный алгоритм Евклида* основан на следующих свойствах наибольшего общего делителя (считаем, что $0 < b \le a$):

1) если оба числа a и b четные, то $\text{НОД}(a, b) = 2 \cdot \text{НОД}\left(\frac{a}{2}, \frac{b}{2}\right)$;

2) если число a нечетное, число b четное, то $\text{НОД}(a, b) = \text{НОД}\left(a, \frac{b}{2}\right)$;

3) если оба числа a и b нечетные, $a > b$, то $\text{НОД}(a, b) = \text{НОД}(a - b, b)$;

4) если $a = b$, то $\text{НОД}(a, b) = a$.

Пример 1.16. Вычислим наибольший общий делитель чисел $a = 30 = (11110)_2$, $b = 20 = (10100)_2$, используя двоичную систему счисления. Оба числа четные, поэтому, согласно свойству 1, $\text{НОД}(a, b) = \text{НОД}((10100)_2, (11110)_2) = 2 \cdot \text{НОД}((1010)_2, (1111)_2)$. Теперь первое число четное, второе — нечетное, поэтому, согласно свойству 2, $\text{НОД}(a, b) = 2 \cdot \text{НОД}((101)_2, (1111)_2) =$ по свойству 3 $= 2 \cdot \text{НОД}((101)_2, (1010)_2) =$ по свойству $2 = 2 \cdot \text{НОД}((101)_2, (101)_2)$. Наконец, по свойству 4

получаем: НОД$((101)_2, (101)_2) = (101)_2 = 5$. Таким образом, НОД$(a, b) =$ $= 2 \cdot 5 = 10$. □

Алгоритм 1.2. Бинарный алгоритм Евклида [6].

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

Выход. $d =$ НОД(a, b).

1. Положить $g \leftarrow 1$.
2. Пока оба числа a и b четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.
3. Положить $u \leftarrow a$, $v \leftarrow b$.
4. Пока $u \neq 0$, выполнять следующие действия.
   4.1. Пока u четное, полагать $u \leftarrow \frac{u}{2}$.
   4.2. Пока v четное, полагать $v \leftarrow \frac{v}{2}$.
   4.3. При $u \ge v$ положить $u \leftarrow u - v$. В противном случае положить $v \leftarrow v - u$.
5. Положить $d \leftarrow gv$.
6. Результат: d. □

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

Аналогичный алгоритм можно построить для полиномов $a(x)$, $b(x)$ с целыми коэффициентами от одной переменной x, только вместо деления на 2 следует использовать деление на x, а условие $a \ge b$ заменить условием $\deg(a) \ge \deg(b)$ для степеней полиномов.

Пример 1.17. Пусть $a(x) = x^5 + 3x^4 + 3x^3 + 2x^2$, $b(x) = x^4 + 2x^3 +$ $+ 2x^2 + x$. Найдем $d(x) =$ НОД$(a(x), b(x))$.

Применяем алгоритм 1.2 (записываем только коэффициенты):

Номер шага	$u(x)$						$v(x)$						
	x^5	x^4	x^3	x^2	x^1	x^0	x^5	x^4	x^3	x^2	x^1	x^0	
1	1	3	3	2	0	0		1	2	2	1	0	$g(x) = 1$
2		1	3	3	2	0			1	2	2	1	$g(x) = x$
4.1			1	3	3	2							
4.3			$u(x) = -(u(x) - 2 \cdot v(x))$										
			1	1	1	0							
4.1				1	1	1							
4.3				$v(x) = v(x) - u(x)$									
									1	1	1	0	
4.2										1	1	1	
4.3				$u(x) = u(x) - v(x)$									
						0							

Таким образом, $d(x) = \text{НОД}(a(x), b(x)) = x(x^2 + x + 1)$.

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида находит наибольший общий делитель d чисел a и b и его линейное представление, то есть целые числа x и y, для которых $ax + by = d$, и не требует «возврата», как в рассмотренном примере.

Алгоритм 1.3. Расширенный алгоритм Евклида.

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

Выход. $d = $ НОД(a, b); такие целые числа x, y, что $ax + by = d$.

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$, $i \leftarrow 1$.
2. Разделить с остатком r_{i-1} на r_i: $r_{i-1} = q_i r_i + r_{i+1}$.
3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$, $x \leftarrow x_i$, $y \leftarrow y_i$. В противном случае положить $x_{i+1} \leftarrow x_{i-1} - q_i x_i$, $y_{i+1} \leftarrow y_{i-1} - q_i y_i$, $i \leftarrow i + 1$ и вернуться на шаг 2.
4. Результат: d, x, y. □

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

Корректность определения чисел x и y, вычисляемых алгоритмом 1.2, показывает следующая лемма.

Лемма 1.10. На каждой итерации алгоритма 1.3 выполняется равенство $ax_i + by_i = r_i$ при $i \ge 0$.

Пример 1.19. Найдем наибольший общий делитель чисел $a = 1092$, $b = 988$ и его линейное представление алгоритмом 1.3. Промежуточные результаты сведем в таблицу:

i	r_i	x_i	y_i	q_i
1	1092	1	0	
2	988	0	1	1
3	104	1	–1	9
4	**52**	**–9**	**10**	2

Таким образом, НОД(1092, 988) = 52 = 1092 · (–9) + 988 · 10. □

Расширенный алгоритм Евклида можно реализовать и в двоичном виде.

Алгоритм 1.4. Расширенный бинарный алгоритм Евклида [6].

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

Выход. $d = $ НОД(a, b); такие целые числа x, y, что $ax + by = d$.

1. Положить $g \leftarrow 1$.
2. Пока оба числа a и b четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.
3. Положить $u \leftarrow a$, $v \leftarrow b$, $A \leftarrow 1$, $B \leftarrow 0$, $C \leftarrow 0$, $D \leftarrow 1$.

4. Пока $u \neq 0$, выполнять следующие действия.

4.1. Пока u четное:

4.1.1. Положить $u \leftarrow \frac{u}{2}$.

4.1.2. Если оба числа A и B четные, то положить $A \leftarrow \frac{A}{2}$, $B \leftarrow \frac{B}{2}$. В противном случае положить $A \leftarrow \frac{A+b}{2}, B \leftarrow \frac{B-a}{2}$.

4.2. Пока v четное:

4.2.1. Положить $v \leftarrow \frac{v}{2}$.

4.2.2. Если оба числа C и D четные, то положить $C \leftarrow \frac{C}{2}$, $D \leftarrow \frac{D}{2}$. В противном случае положить $C \leftarrow \frac{C+b}{2}, D \leftarrow \frac{D-a}{2}$.

4.3. При $u \geq v$ положить $u \leftarrow u - v$, $A \leftarrow A - C$, $B \leftarrow B - D$. В противном случае положить $v \leftarrow v - u$, $C \leftarrow C - A$, $D \leftarrow D - B$.

5. Положить $d \leftarrow gv, x \leftarrow C, y \leftarrow D$.

6. Результат: d, x, y. □

Сложность этого алгоритма равна $O(\log^2 a)$. Здесь по аналогии с леммой 1.10 на каждом шаге выполняются соотношения $u = aA + bB$ и $v = aC + bD$. Если все три числа u, A и B четные, то обе части равенства $u = aA + bB$ можно разделить на 2 (первое условие шага 4.1.2). Если же при четном u хотя бы одно из чисел A, B нечетное, то соотношение $u = aA + bB$ преобразуется в $u = aA + bB + ab - ab = a(A + b) + b(B - a)$ (второе условие шага 4.1.2). То же справедливо и для чисел v, C, D.

Пример 1.20. Найдем наибольший общий делитель чисел $a = 1092$, $b = 988$ и его линейное представление алгоритмом 1.4.

На шаге 1 полагаем $g = 1$. Шаг 2 выполняем два раза, получаем $a = 273$, $b = 247$, $g = 4$. Последовательность дальнейших шагов алгоритма 1.4 сведем в таблицу:

Шаг	u	v	A	B	C	D
3	273	247	1	0	0	1
4.3	26		1	−1		
4.1	13		124	−137		
4.3		234			−124	138
4.2		117			−62	69
4.3		104			−186	206
4.2		52			−93	103
4.2		26			77	−85
4.2		13			162	−179
4.3	0		−38	42		

На шаге 5 полагаем $d = 4 \cdot 13 = 52$, $x = 162$, $y = -179$.

Проверка: $1092 \cdot 162 + 988 \cdot (-179) = 176904 - 176852 = 52$. □

Как видно из примеров, линейное представление $ax + by = \text{НОД}(a, b)$ не единственно. Выведем общий вид коэффициентов x и y. Пусть есть другое представление $ax' + by' = \text{НОД}(a, b)$. Тогда $a(x' - x) + b(y' - y) = 0$. Найдем такие целые числа s, t, для которых $as = bt$. Запишем $a = a_1 \cdot \text{НОД}(a, b)$, $b = b_1 \cdot \text{НОД}(a, b)$, где $\text{НОД}(a_1, b_1) = 1$. Отсюда $a_1 s = b_1 t$, и это равенство выполняется для $s = b_1 k$, $t = a_1 k$, где k — произвольное целое число. Получаем

$$x' = x + \frac{bk}{\text{НОД}(a,b)}, \quad y' = y - \frac{ak}{\text{НОД}(a,b)},$$

для произвольного целого числа k.

В примере 1.19 $a = 1092$, $b = 988$, НОД$(a, b) = 52$, $x = -9$, $y = 10$. Тогда значения x', y' определяются равенствами

$$x' = -9 + 19k, y' = 10 - 21k.$$

Значения $x' = 162$, $y' = -179$ из примера 1.20 получаем при $k = 9$.