КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 5

Вычисление наибольшего общего делителя

Данный материал демонстрирует разбор задания, посвященного вычислению наибольшего общего делителя с помощью расширенного алгоритма Евклида.

Наибольшим общим делителем целых чисел a и b называется такое целое число $d \geq 1$, которое удовлетворяет следующим условиям:

1) d есть общий делитель a и b;

2) если $d' \in \mathbb{Z}$ есть любой общий делитель a и b, то d делится на d'.

Наибольший общий делитель чисел a и b принято обозначать $\text{НОД}(a, b)$. Если $\text{НОД}(a, b) = 1$, то a и b называются взаимно простыми числами.

Наибольший общий делитель двух целых чисел легко может быть найден с помощью алгоритма Евклида.

Вход: целые числа $a \geq b > 0$.

Выход: $d = \text{НОД}(a, b)$.

Шаг 1. Пока $b \neq 0$, выполнять следующее:

Шаг 1.1. Вычислить $r \leftarrow a \bmod b$.

Шаг 1.2 Присвоить $a \leftarrow b$, $b \leftarrow r$.

Шаг 2. Возврат (a).

Если кроме $\text{НОД}(a, b)$, нужно найти также и целочисленную линейную комбинацию a и b, то есть выражение $xa + yb = \text{НОД}(a, b)$, для этого применяется расширенный алгоритм Евклида.

Вход: целые числа $a \geq b > 0$.

Выход: $d = \text{НОД}(a, b)$ и целые x, y, такие, что $xa + yb = d$.

Шаг 1. Полагаем $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.

Шаг 2. Пока $b > 0$, выполнять следующее:

Шаг 2.1. $q \leftarrow [{}^{a}/_{b}]$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.

Шаг 2.2. $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$.

Шаг 3. $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ и возврат (d, x, y).

Кроме того, расширенный алгоритм Евклида позволяет находить обратные элементы в кольце классов вычетов по модулю n.

Вход: $n > a > 0$, $a, n \in \mathbb{Z}$.

Выход: $a^{-1} \pmod n$.

Шаг 1. Используя расширенный алгоритм Евклида, найти целые числа x, y, такие, что $xn + ya = d = \text{НОД}(n, a)$.

Шаг 2. Если $d > 1$, то $a^{-1} \pmod n$ не существует.

Шаг 3. Если $d = 1$, то возврат (y).

Пример.

Найти целочисленную линейную комбинацию чисел 3931 и 1148.

Решение.

Работу итерационных алгоритмов, к которым в том числе относится расширенный алгоритм Евклида, удобно демонстрировать с помощью таблицы.

Каждая строка данной таблицы отражает полученные на очередной итерации значения переменных, которыми оперирует расширенный алгоритм Евклида. Первая строка содержит входные данные, поэтому значения переменных q, r, x, y в первой строке не определены.

q	r	x	y	a	b	x_2	x_1	y_2	y_1
—	—	—	—	3931	1148	1	0	0	1
3	487	1	–3	1148	487	0	1	1	–3
2	174	–2	7	487	174	1	–2	–3	7
2	139	5	–17	174	139	–2	5	7	–17
1	35	–7	24	139	35	5	–7	–17	24
3	34	26	–89	35	34	–7	26	24	–89
1	1	–33	113	34	1	26	–33	–89	113
34	0	1148	–3931	1	0	–33	1148	113	–3931

Расчеты велись в течение семи итераций. На седьмой итерации очередное значение a было нацело разделено на очередное значение b. Это является условием завершения алгоритма.

После этого произошел выход из алгоритма с возвратом трех значений, содержащихся в ячейках, выделенных цветом.

Можно увидеть, что полученная целочисленная линейная комбинация имеет следующий вид:

$$-33 \cdot 3931 + 113 \cdot 1148 = 1.$$

Проверка показывает, что данное равенство является верным. Следовательно, числа 3931 и 1148 являются взаимно простыми. Если бы в данной задаче необходимо было найти значение $1148^{-1} \bmod 3931$, то можно было бы сказать, что, во-первых, данное значение существует, а, во-вторых, оно равно 113.