II. Разложение чисел на множители. Факторизация составных чисел.

Задача разложения составного числа на множители:

Для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, где p_i – попарно различные простые числа, $\alpha_i \geq 1$.

Прежде чем раскладывать число на множители, его необходимо проверить одним из тестов на простоту.

На практике не обязательно находить каноническое разложение числа n. Достаточно найти его разложение на два нетривиальных сомножителя: $n = p \cdot q, 1 < p \leq q < n$. Данная задача носит название задачи факторизации числа n.

1. Метод пробного деления.

Пусть n – нечетное составное число. Перебирая по очереди простые числа $p_i = 3, 5, 7, \ldots$ необходимо разделить n нацело на p_i. Если попытка удалась, то $n \leftarrow \frac{n}{p_i}$ и повторяем процедуру до тех пор, пока не получим каноническое разложение числа n.

Процесс можно немного ускорить, если заранее вычислить произведения простых чисел. Тогда вместо целочисленного деления нужно вычислить алгоритмом Евклида наибольший общий делитель d числа n и этих произведений и положить $n \leftarrow \frac{n}{d}$, повторяя процедуру до тех пор, пока не получится каноническое разложения числа n.

Пример. Разложить на множители число $n = 84\,257\,901$ методом пробного деления.

Решение.

Составим базу данных из произведений простых чисел по три:

$q_1 = 3 \cdot 5 \cdot 7 = 105; \quad q_2 = 11 \cdot 13 \cdot 17 = 2\,431; \quad q_3 = 19 \cdot 23 \cdot 29 = 12\,673.$

I)

1) Вычисляем $d_{11} = \text{НОД}(n, q_1) = \text{НОД}(84\,257\,901,\ 105) = 21 \implies$ n делится на $\boxed{3}$ и на $\boxed{7}$.

Полагаем $n \leftarrow \frac{n}{d_{11}} = \frac{84\,257\,901}{21} = 4\,012\,281.$

2) Вычисляем $d_{12} = \text{НОД}(n, q_1) = \text{НОД}(4\,012\,281,\ 105) = 21 \implies n$ делится на $\boxed{3}$ и на $\boxed{7}$.

Полагаем $n \leftarrow \frac{n}{d_{12}} = \frac{4\,012\,281}{21} = 191\,061.$

3) Вычисляем $d_{13} = \text{НОД}(n, q_1) = \text{НОД}(191\,061,\ 105) = 3 \implies n$ делится на $\boxed{3}$.

Полагаем $n \leftarrow \frac{n}{d_{13}} = \frac{191\,061}{3} = 63\,687.$

4) Вычисляем $d_{14} = \text{НОД}(n, q_1) = \text{НОД}(63\,687,\ 105) = 3 \implies n$ делится на $\boxed{3}$.

Полагаем $n \leftarrow \frac{n}{d_{14}} = \frac{63\,687}{3} = 21\,229.$

5) Вычисляем $d_{15} = \text{НОД}(n, q_1) = \text{НОД}(21\,229,\ 105) = 1.$

II)

1) $d_{21} = \text{НОД}(n, q_2) = \text{НОД}(21\,229,\ 2\,431) = 13 \implies n$ делится на $\boxed{13}$.

Полагаем $n \leftarrow \frac{n}{d_{21}} = \frac{21\,229}{13} = 1\,633.$

2) $d_{22} = \text{НОД}(n, q_2) = \text{НОД}(1\,633,\ 2\,431) = 1.$

III)

1) $d_{31} = \text{НОД}(n, q_3) = \text{НОД}(1\,633,\ 12\,673) = 23 \implies n$ делится на $\boxed{23}$.

Полагаем $n \leftarrow \frac{n}{d_{31}} = \frac{1\,633}{23} = 71.$ Так как 71 – простое число, то разложение на простые множители окончено.

Итак, $84\,257\,901 = 3 \cdot 7 \cdot 3 \cdot 7 \cdot 3 \cdot 3 \cdot 13 \cdot 23 \cdot 71 = 3^4 \cdot 7^2 \cdot 13 \cdot 23 \cdot 71.$

Ответ. $84\,257\,901 = 3^4 \cdot 7^2 \cdot 13 \cdot 23 \cdot 71.$

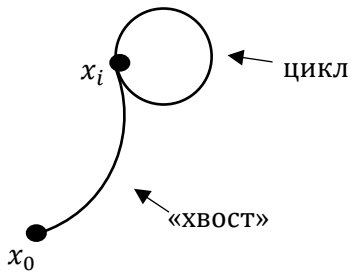
Замечание. Перебрав все простые числа, меньше $\sqrt{n}$, получается каноническое разложение числа n. В наихудшем случае, т.е. когда n представляет собой произведение двух простых чисел примерно одинакового размера, для этого потребуется примерно $\sqrt{n}$ делений. В общем случае, делители, получаемые на каждом шаге, проверяют на простоту.

2. ρ – метод Полларда.

Это наиболее популярный метод факторизации, предложенный в 1975 году.

Пусть n – нечетное составное число, $S = \{0, 1, \dots, n-1\}$ и f – некоторый многочлен с целыми коэффициентами, степени больше единицы. В своей работе Полларда предложил многочлен $f(x) = x^2 + 1$.

Основная идея ρ – метода Полларда:



Выбирается случайный элемент $x_0 \in S$ и строится последовательность $x_0, x_1, x_2, \dots$, определяемая рекуррентным соотношением (уравнение, которое выражает каждый элемент последовательности как функцию предыдущих элементов): $x_{i+1} = f(x_i), i \geq 0$, до тех пор, пока не найдутся такие числа i и j, что $i < j$ и $x_i = x_j$. Так как множество S конечно, то такие индексы i и j существуют (последовательность с некоторого момента «зацикливается»). Таким образом, последовательность $\{x_i\}$ будет состоять из «хвоста» $x_0, x_1, \dots, x_{i-1}$ и цикла $x_i(= x_j), x_{i+1}, \dots, x_{j-1}$. Графически последовательность $\{x_i\}$ образовывает греческую букву «ρ». Отсюда и название метода.

Если p – простой делитель числа n и $x_i \equiv x_j \pmod p$, то разность $x_i - x_j$ делится на p и НОД$(x_i - x_j, n) > 1$. Число p необходимо найти, поэтому

все вычисления в алгоритме проводятся по модулю n и на каждом шаге вычисляется $d = \text{НОД}(x_i - x_j, n)$. Нетривиальный ($\neq 1$ и $\neq n$) наибольший общий делитель $1 < d < n$ как раз и будет искомым делителем p числа n. Случай $d = n$ имеет место с пренебрежимо малой вероятностью.

Алгоритм. ρ – метод Полларда.

Вход. Число n, начальное значение c, функция f.

Выход. Нетривиальный делитель p числа n.

1. Положить $a \leftarrow c, b \leftarrow c$.
2. Вычислить $a \leftarrow f(a) \pmod n, b \leftarrow f(b) \pmod n, b \leftarrow f(b) \pmod n$ (понимать, как $f(f(b))$ – суперпозиция функций).
3. Найти $d \leftarrow$ НОД $(a - b, n)$.
4. Если $1 < d < n$, то положить $p \leftarrow d$ и результат: «p – нетривиальный делитель числа n». При $d = n$ результат: «Делитель не найден», при $d = 1$ вернуться на шаг 2.

Замечание. Существенным недостатком алгоритма является необходимость хранить большое число предыдущих значений x_i. В настоящий момент существует несколько подходов к улучшению оригинального алгоритма, например, Брентом или Флойдом.