ЛАБОРАТОРНАЯ РАБОТА №6

Разложение чисел на множители

Задача разложения на множители – одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где p_i – попарно различные простые числа, $\alpha_i \geq 1$.

На практике не обязательно находить каноническое разложение числа n. Достаточно найти его разложение на два *нетривиальных сомножителя*: $n = pq, 1 \leq p \leq q < n$. Далее будем понимать задачу разложения именно в этом смысле.

p–Метод Полларда. Пусть n – нечетное составное число, $S = \{0, 1, \dots, n-1\}$ и $f\colon S \to S$ – случайное отображение, обладающее сжимающими свойствами, например $f(x) \equiv x^2 + 1 \ (mod\ n)$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность $x_0, x_1, x_{2,\dots}$, определяемую рекуррентным соотношением

$$x_{i+1} = f(x_i),$$

где $i \geq 0$, до тех пор, пока не найдем такие числа i, j, что $i < j$ и $x_i = x_j$. Поскольку множество S конечно, такие индексы i, j существуют (последовательность «зацикливается»). Последовательность $\{x_i\}$ будет состоять из «хвоста» $x_0, x_1, \dots, x_{i-1}$ длины $O\left(\sqrt{\frac{\pi n}{8}}\right)$ и цикла $x_i = x_j, x_{i+1}, \dots, x_{j-1}$ той же длины.

Алгоритм, реализующий p-метод Полларда.

Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.

Выход. Нетривиальный делитель числа n.

1. Положить $a \leftarrow c, b \leftarrow c$.
2. Вычислить $a \leftarrow f(a)(mod\ n), b \leftarrow f(b)\ (mod\ n)$
3. Найти $d \leftarrow$ НОД$(a-b, n)$.
4. Если $1 < d < n$, то положить $p \leftarrow d$ и результат: p. При $d = n$ результат: «Делитель не найден»; при $d = 1$ вернуться на шаг 2.

Пример. Найти р-методом Полларда нетривиальный делитель числа $n = 1359331$. Положим $c = 1$ и $f(x) = x^2 + 5\ (mod\ n)$. Работа алгоритма иллюстрируется следующей таблицей:

i	a	b	d = НОД$(a-b, n)$
	1	1	
2	6	41	1
2	41	123939	1
3	1686	391594	1
4	123939	438157	1
5	435426	582738	1
6	391594	1144026	1
7	1090062	885749	1181

Таким образом, 1181 является нетривиальным делителем числа 1359331.

Метод квадратов. (Теорема Ферма о разложении) Для любого положительного нечетного числа n существует взаимно однозначное соответствие между множеством делителей числа n, не меньших, чем $\sqrt{n}$, и множеством пар $\{s, t\}$ таких неотрицательных целых чисел, что $n = s^2 - t^2$.

Пример. У числа 15 два делителя, не меньших, чем $\sqrt{15}$, – это числа 5 и 15. Тогда получаем два представления:

1. $15 = pq = 3 \cdot 5$, откуда $s = 4, t = 1$ и $15 = 4^2 - 1^2$;
2. $15 = pq = 1 \cdot 15$, откуда $s = 8, t = 7$ и $15 = 8^2 - 7^2$.

Задания к лабораторной работе

1. Реализовать рассмотренный алгоритм программно.
2. Разложить на множители данное преподавателем число.