Отчет по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Выполнила Дяченко Злата Константиновна, НПМмд-02-22

Содержание

List of Figures

List of Tables

1 Цель работы

Ознакомится и реализовать алгоритм разложения чисел на множители.

2 Задание

Реализовать программно алгоритм, реализующий p-метод Полларда.

3 Теоретическое введение

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, 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: $n = pq, 1 \leq p \leq q < n$. *p–Метод Полларда*. Пусть n – нечетное составное число, S = {0, 1, ... , n − 1} и $f : S \to S$– 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 $x_0, x_1, x_2, ...$, определяемую рекуррентным соотношением

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

, где i ⩾ 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» $x_0, x_1, ..., x_{i-1}$ длины $O(\sqrt{\frac{\pi n}{8}})$ и цикла $x_i = x_j, x_{i+1}, ..., x_{j-1}$ той же длины.

Алгоритм, реализующий р-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 $a \leftarrow f(a)(mod n), b \leftarrow f(f(b))(mod n)$. 3. Найти $d \leftarrow (a - b, n)$. 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.

4 Выполнение лабораторной работы

4.1 Шаг 1

Ознакомилась с предоставленными теоретическими данными. Для выполнения задания решила использовать язык Python. Подключила библиотеку math. Написала функцию, реализующую поиск нетривиального делителя с помощью p-метода Полларда. Код функции и результат ее использования представлен на Рисунке 1 (рис. - fig. 4.1). Функция принимает на вход число n и число c. Фукнцию f реализовала как отдельную функцию и не передавала ее функции алгоритма. Пример работы алгоритма для числа из представленых для лабораторной работы материалов также представлен на рисунке.

```
In [4]: def f(x):
            return x*x+5

In [16]: import math

In [22]: def polard (n, c):
             a=c
             b=c
             d=1
             while (d==1):
                 a=f(a)%n
                 b=f(f(b))%n
                 d=math.gcd(a-b, n)
                 if (1<d and d<n):
                     p=d
                     return p
                 if (d==n):
                     return ("Делитель не найден")

In [23]: polard(1359331, 1)
Out[23]: 1181
```

Figure 4.1: Реализация алгоритма, реализующего p-метод Полларда

4.2 Шаг 2

Так как результатом выполнения функции является нетривиальный делитель, для разложения числа 1359331 на множители разделила его на найденный делитель для нахождения второго множителя. Так, 1359331=1181*1151 (рис. - fig. 4.2).

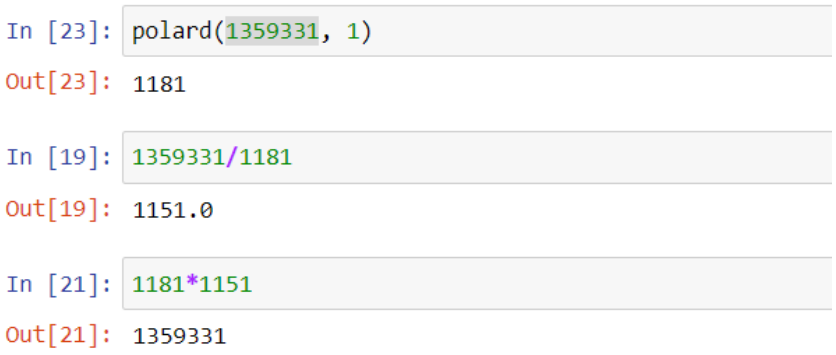

Figure 4.2: Разложение на множители

5 Выводы

Я ознакомилась с алгоритмом, реализующем p-метод Полларда, и реализовала его программно. Результаты работы находятся в репозитории на GitHub, а также есть скринкаст выполнения лабораторной работы.