РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Отчёт по лабораторной работе №6
Разложение чисел на множители

Дисциплина: *Математические основы защиты информации и информационной безопасности*

Студент: Агеева Анастасия Сергеевна, 1032212304
Группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

1 Цель работы **4**

2 Задание **5**

3 Теоретическое введение **6**
3.1 ρ-алгоритм Полларда 6
3.1.1 Современная версия 6

4 Выполнение лабораторной работы **8**

5 Выводы **10**

Список литературы **11**

List of Figures

4.1 Сжимающая функция f 8
4.2 Результаты p-метода Полларда 8
4.3 Результаты p-метода Полларда 9

1 Цель работы

Цель данной лабораторной работы изучение алгоритмов разложения чисел на множители.

2 Задание

1. Реализовать программно алгоритм, реализующий p-метод Полларда.

3 Теоретическое введение

3.1 ρ-алгоритм Полларда

ρ-алгоритм (ρ-алгоритм) — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении [1].

Сложность алгоритма оценивается как $O(N^{1/4})$.

ρ-алгоритм Полларда строит числовую последовательность, элементы которой образуют цикл, начиная с некоторого номера n, что может быть проиллюстрировано, расположением чисел в виде греческой буквы ρ, что послужило названием семейству алгоритмов.

3.1.1 Современная версия

Пусть N составное целое положительное число, которое требуется разложить на множители. Алгоритм выглядит следующим образом: Случайным образом выбирается небольшое число x_0 и строится последовательность $\{x_n\}, n = 0, 1, 2, ...$, определяя каждое следующее как $x_{n+1} = F(x_n) \pmod N$.

Одновременно на каждом i-ом шаге вычисляется $d = \text{GCD}(N, |x_i - x_j|)$ для каких-либо i, j таких, что $j < i$, например, $i = 2j$. Если $d > 1$, то вычисление заканчивается, и найденное на предыдущем шаге число d является делителем

N. Если N/d не является простым числом, то процедуру поиска делителей продолжается, взяв в качестве N число $N' = N/d$.

На практике функция $F(x)$ выбирается не слишком сложной для вычисления (но в то же время не линейным многочленом), при условии того, что она не должна порождать взаимно однозначное отображение. Обычно в качестве $F(x)$ выбираются функции $F(x) = x^2 \pm 1 (\mathrm{mod}\, N)$ или $F(x) = x^2 \pm a (\mathrm{mod}\, N)$. Однако функции $x^2 - 2$ и x^2 не подходят.

Если известно, что для делителя p числа N справедливо $p \equiv 1 \,(\mathrm{mod}\, k)$ при некотором $k > 2$, то имеет смысл использовать $F(x) = x^k + b$.

Существенным недостатком алгоритма в такой реализации является необходимость хранить большое число предыдущих значений x_j.

4 Выполнение лабораторной работы

1. **Реализация p-метода Полларда**

    1. Задам функцию $f()$, обладающую сжимающими свойствами, в которую буду передавать числа n и x.

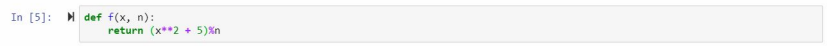

Figure 4.1: Сжимающая функция f

    2. Задам функцию $pollard()$, в которую буду передавать число n, разлагаемое на множители, и начальное значение c. По алгоритму, реализующему p-метода Полларда, осуществляется нахождение нетривиального делителя числа n. В качестве результата возвращается делитель или строка, сообщающая, что он не найден.

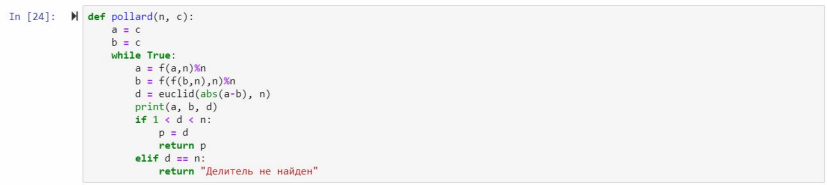

Figure 4.2: Результаты p-метода Полларда

    3. Вызову функцию для чисел $n = 1359331$ и $c = 1$. Алгоритм верно находит нетривиальный делитель числа $n = 1359331$.

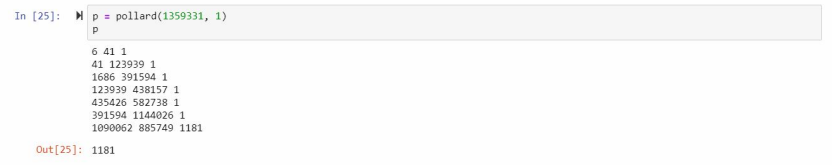

Figure 4.3: Результаты p-метода Полларда

5 Выводы

В ходе данной лабораторной работы я реализовала программно p-метода Полларда нахождения нетривиального делителя.

Список литературы

1. Ро-алгоритм Полларда [Электронный ресурс]. Википедия, 2019. URL: https://ru.wikipedia.org/wiki/Ро-алгоритм_Полларда.