Отчет по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Выполнила Дяченко Злата Константиновна, НПМмд-02-22

Содержание

# 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 найти его каноническое разложение , где – попарно различные простые числа, . На практике не обязательно находить каноническое разложение числа . Достаточно найти его разложение на два нетривиальных сомножителя: . *p–Метод Полларда*. Пусть – нечетное составное число, S = {0, 1, … , n − 1} и – случайное отображение, обладающее сжимающими свойствами, например . ݀Основная идея метода состоит в следующем. Выбираем случайный элемент и строим последовательность , определяемую рекуррентным соотношением

, где i ≥ 0, до тех пор, пока не найдем такие числа , что и . Поскольку множество конечно, такие индексы существуют (последовательность «зацикливается»). Последовательность будет состоять из «хвоста» длины и цикла той же длины.

Алгоритм, реализующий p-метод Полларда. *Вход*. Число , начальное значение , функция , обладающая сжимающими свойствами. *Выход*. Нетривиальный делитель числа . 1. Положить . 2. Вычислить . 3. Найти . 4. Если , то положить и результат: . При результат: «Делитель не найден»; при 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. 1). Функция принимает на вход число и число . Фукнцию 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.

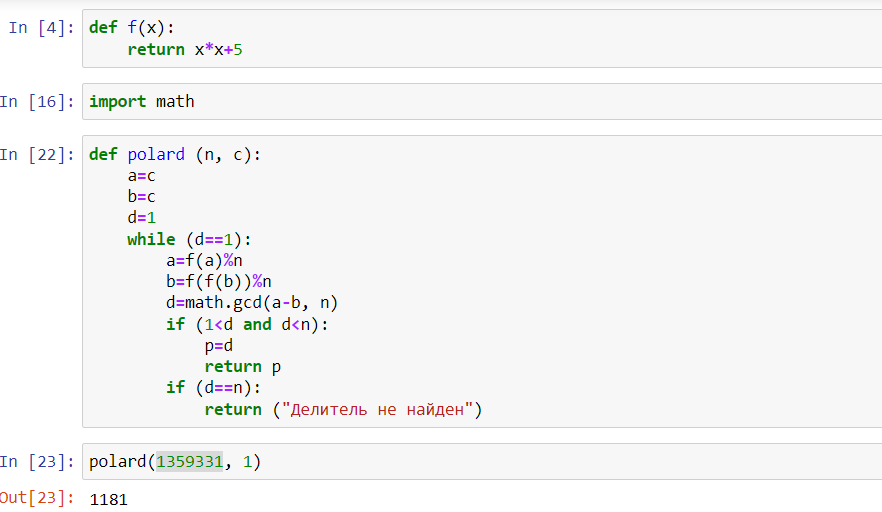


Figure 1: Реализация алгоритма, реализующего p-метод Полларда

## 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. 2).

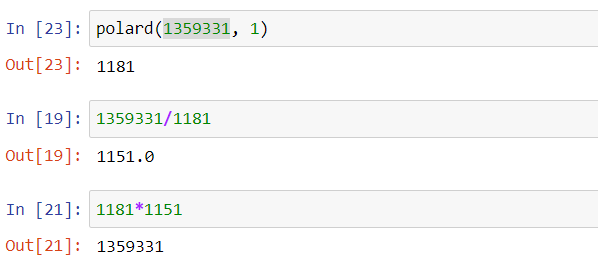


Figure 2: Разложение на множители

# 5 Выводы

Я ознакомилась с алгоритмом, реализующем p-метод Полларда, и реализовала его программно. Результаты работы находятся в [репозитории на GitHub](https://github.com/ZlataDyachenko/workD), а также есть [скринкаст выполнения лабораторной работы](https://youtu.be/1mD8BJZiB4w).