Лабораторная работа №6. Разложение чисел на множители.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть и реализовать алгоритм, реализующий p-метод Полларда и реализовать метод квадратов.

# 2 Задание

Реализовать следующие алгоритмы:

* p-метод Полларда;
* Метод квадратов.

# 3 Теоретическое введение

**p-Метод Полларда:**

p-Метод Полларда — это один из методов факторизации составных чисел, который был разработан Джоном Поллардом. Метод основан на свойствах мультипликативной группы вычетов по модулю простого числа p.

Метод Полларда работает основываясь на том, что при достаточном количестве итераций два значения в последовательности будут находиться в одном цикле и могут быть использованы для вычисления делителя.

Применение параметра в функции позволяет разнообразить последовательность значений и улучшить эффективность метода в некоторых случаях.

Метод Полларда является одним из алгоритмов факторизации, используемых для разложения больших составных чисел на их простые множители.

**Метод квадратов:**

Метод квадратов (Quadratic Sieve) — это алгоритм факторизации целых чисел, разработанный Карлом Померанцем и Джоном Поллелем. Этот метод основан на поиске целых чисел, которые представляют собой разность двух квадратов. Метод квадратов является одним из эффективных методов для факторизации больших составных чисел и часто применяется в криптографии. Вместе с методом факторизации ро (алгоритмом Полларда), он используется для атаки на криптографические системы, основанные на сложности факторизации больших чисел.

# 4 Выполнение лабораторной работы

## 4.1 p-Метод Полларда

### 4.1.1 Задача

Реализовать p-Метод Полларда

#### 4.1.1.1 Решение

Реализуем p-Метод Полларда (рис. [1](#fig:001))

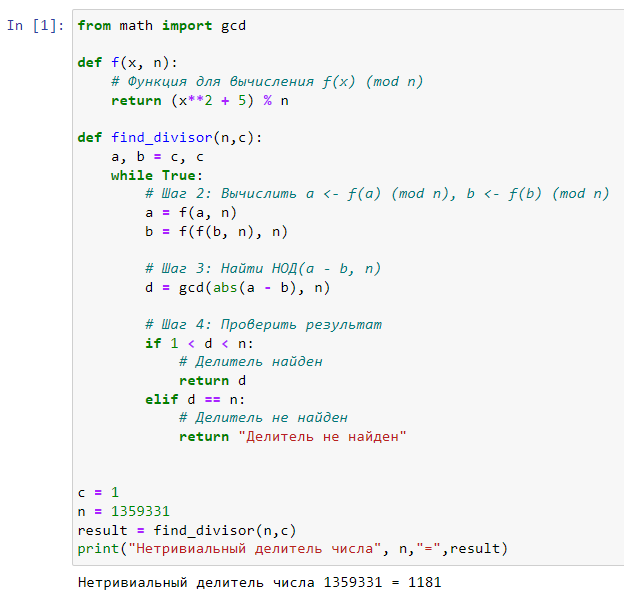


Figure 1: p-Метод Полларда

## 4.2 Метод квадратов

### 4.2.1 Задача

Реализовать метод квадратов

#### 4.2.1.1 Решение

Реализуем метод квадратов (рис. [2](#fig:002))

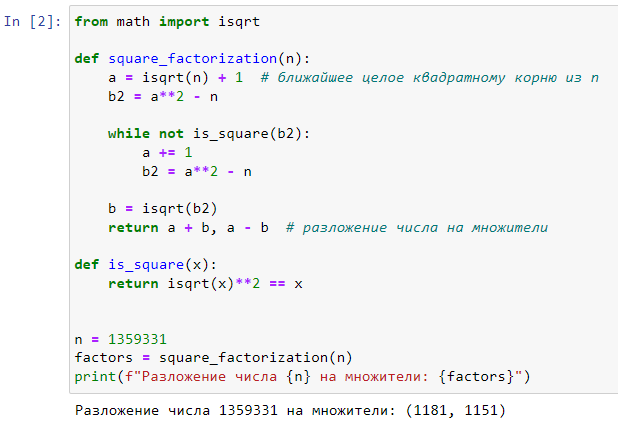


Figure 2: Метод квадратов

# 5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал следующие алгоритмы:

* p-метод Полларда;
* Метод квадратов.

# 6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: [Python documentation](https://docs.python.org/3/index.html) (Дата обращения: 28.09.2023).
2. Лабораторная работа №6. Разложение чисел на множители. - 3 с. [Электронный ресурс]. М. URL: [Лабораторная работа №6. Разложение чисел на множители.](https://esystem.rudn.ru/pluginfile.php/2089818/mod_folder/content/0/lab06.pdf) (Дата обращения: 22.11.2023).