Отчёт по лабораторной работе №6  
Разложение чисел на множители

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

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 -алгоритм Полларда

**-алгоритм (-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 .

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

### 3.1.1 Современная версия

Пусть составное целое положительное число, которое требуется разложить на множители. Алгоритм выглядит следующим образом: Случайным образом выбирается небольшое число и строится последовательность , определяя каждое следующее как .

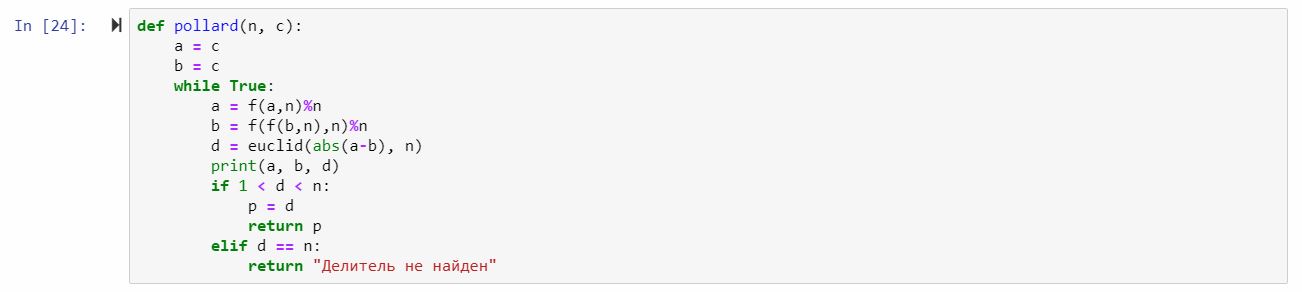
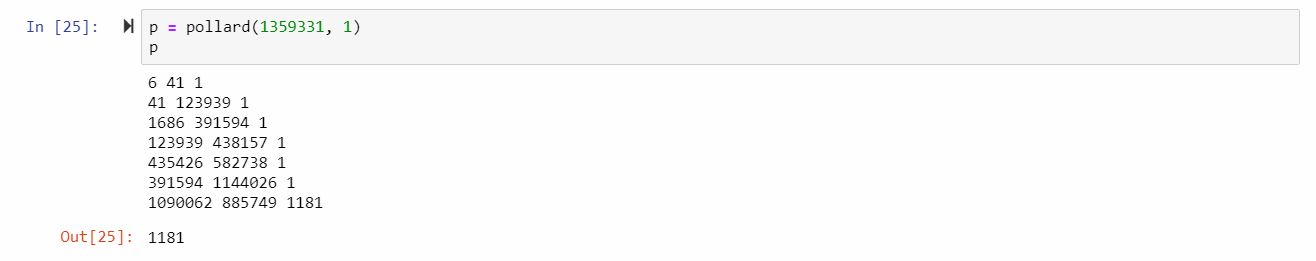
Одновременно на каждом i-ом шаге вычисляется для каких-либо , таких, что , например, . Если , то вычисление заканчивается, и найденное на предыдущем шаге число является делителем . Если не является простым числом, то процедуру поиска делителей продолжается, взяв в качестве число .

На практике функция 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 выбираются функции или . Однако функции и не подходят.

Если известно, что для делителя числа справедливо при некотором , то имеет смысл использовать .

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

# 4 Выполнение лабораторной работы

1. **Реализация p-метода Полларда**
   1. Задам функцию , обладающую сжимающими свойствами, в которую буду передавать числа и .
   * 
   * Figure 1: Сжимающая функция f
   1. Задам функцию , в которую буду передавать число , разлагаемое на множители, и начальное значение . По алгоритму, реализующему p-метода Полларда, осуществляется нахождение нетривиального делителя числа . В качестве результата возвращается делитель или строка, сообщающая, что он не найден.
   * 
   * Figure 2: Результаты p-метода Полларда
   1. Вызову функцию для чисел и . Алгоритм верно находит нетривиальный делитель числа .
   * 
   * Figure 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>.