Лабораторная работа 6

Разложение чисел на множители

Пологов Владислав Александрович

Содержание

# Цель работы

Реализовать алгоритм, реализующий р-метод Полларда

# Описание реализации

Для реализации алгоритмов использовались средства языка Python.

# Реализация

## Алгоритм, реализующий р-метод Полларда

Итак, мы хотим факторизовать число n. Предположим, что n = pq и p ≈ q. Понятно, что труднее случая, наверное, нет. Алгоритм итеративно ищет наименьший делитель и таким образом сводит задачу к как минимум в два раза меньшей. Алгоиртм, реализующий р-метод Полларда приведён на рисунке 1. (рис. -fig. 1)

## Алгоритм, реализующий р-метод Полларда

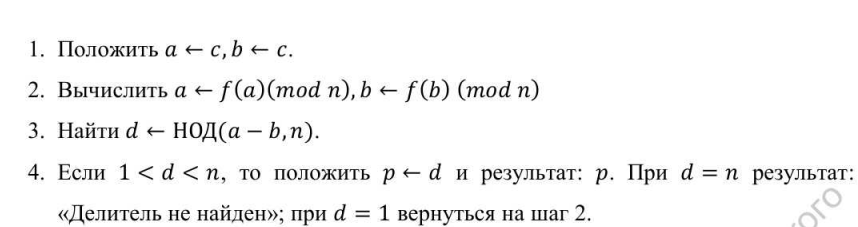


Figure 1: Алгоритм, реализующий р-метод Полларда

## Алгоритм, реализующий р-метод Полларда

Возьмём произвольную «достаточно случайную» с точки зрения теории чисел функцию. Например f(x) = (x + 1) ^2 mod n.

Граф, в котором из каждой вершины есть единственное ребро , называется функциональным. Если в нём нарисовать «траекторию» произвольного элемента — какой-то путь, превращающийся в цикл — то получится что-то похожее на букву (ро). Алгоритм из-за этого так и назван. Траектория произвольного элемента представлена на рисунке 2. (рис. -fig. 2)

## Траектория произвольного элемента

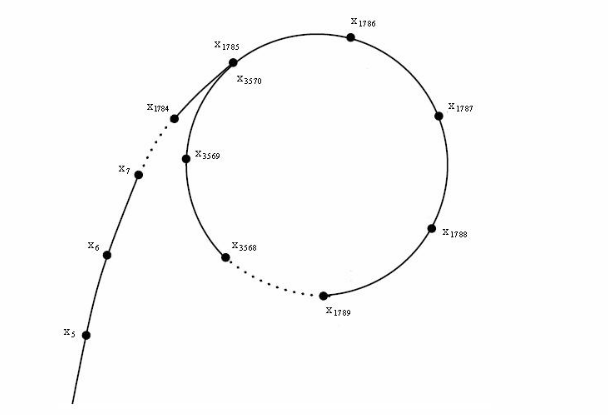


Figure 2: Траектория произвольного элемента

## Код, реализующий алгоритм

Использовались библиотеки math для вычисления НОД и randint для получения целого рандомного числа. Код, реализующий р-метод Полларда представлен на рисунке 3. (рис. -fig. 3)

## Код, реализующий алгоритм

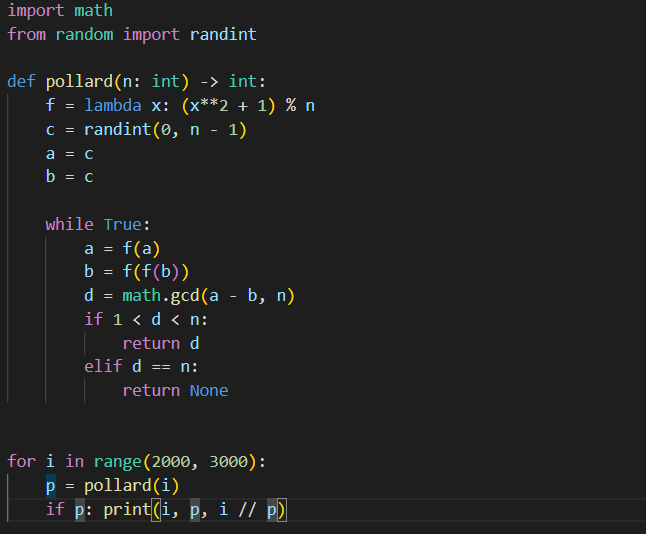


Figure 3: Код, реализующий р-метод Полларда

# Вывод

* Реализован программно р-метод Полларда. Проведена проверка методом квадратов.