Лабораторная работа 7

Дискретное логарифмирование в конечном поле

Пологов Владислав Александрович

Содержание

# Цель работы

## Цель работы

Реализовать алгоритм, реализующий р-метод Полларда для задач дискретного логарифмирования

# Описание реализации

## Описание реализации

Для реализации алгоритмов использовались средства языка Python.

# Реализация

## Алгоритм, реализующий р-метод Полларда для задач дискретного логарифмирования

На вход будет подаваться простое число р, число а порядка r по модулю p, целое число b, 1 < b < p; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма. На выходе должны получить показатель x, для которого a ^ x = b (mod p), если такой показатель существует. Алгоритм представлен на рисунке 1. (рис. -fig. 1)

## Алгоритм, реализующий р-метод Полларда

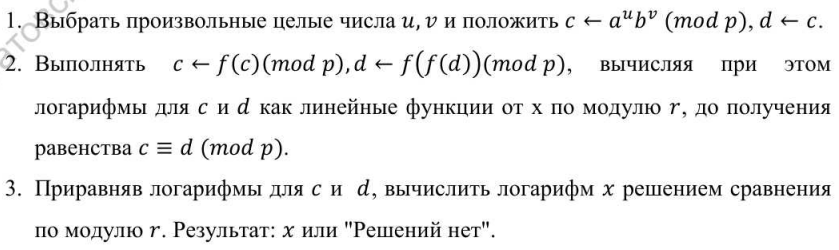


Figure 1: Алгоритм, реализующий р-метод Полларда для дискретного логарифмирования

## Код, реализующий алгоритм

В начале использовалась функция, реазлизующая расширенный алгоритм Евклида, представленный на рисунке 2.(рис. -fig. 2) Также применена функция, для нахождения логарифма методом перебора, испульзуема для проверки.(рис. -fig. 3) Код, реализующий р-метод Полларда для задач дискретного логарифмирования представлен на рисунках 2, 3, 4. (рис. -fig. 4)

## Код, реализующий алгоритм ч.1

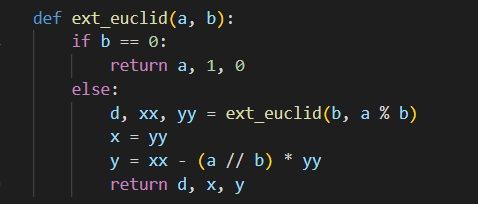


Figure 2: Код, реализующий р-метод Полларда

## Код, реализующий алгоритм ч.2

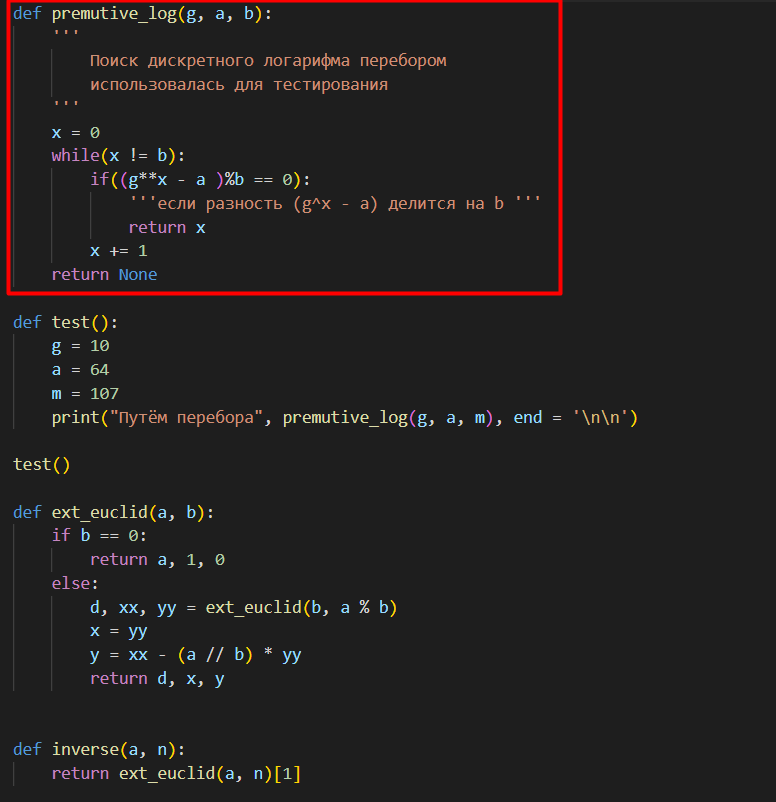


Figure 3: Код, реализующий р-метод Полларда

## Код, реализующий алгоритм ч.3

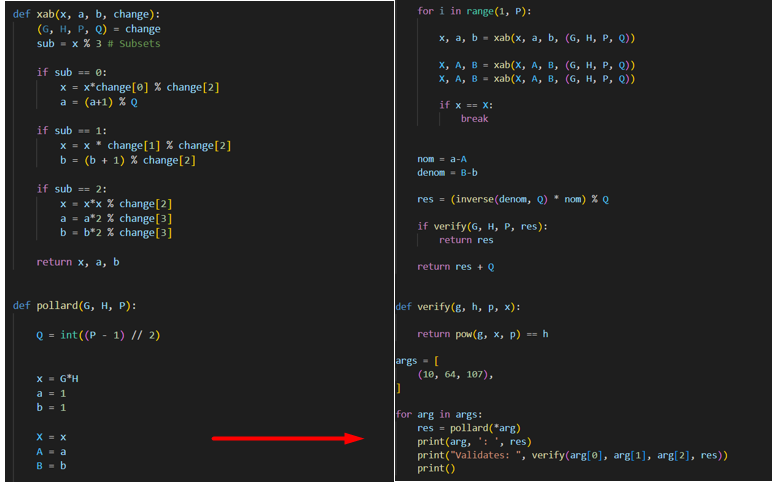


Figure 4: Код, реализующий р-метод Полларда

# Вывод

* Реализован программно р-метод Полларда для задач дискретного логарифмирования. Проведена проверка методом перебора.