Лабораторная работа №7. Дискретное логарифмирование в конечном поле.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть и реализовать алгоритм, реализующий -метод Полларда для задач дискретного логарифмирования.

# 2 Задание

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

# 3 Теоретическое введение

**p-Метод Полларда:**

-Метод Полларда для дискретного логарифмирования (-метод) — алгоритм дискретного логарифмирования в кольце вычетов по простому модулю, имеющий экспоненциальную сложность. Предложен британским математиком Джоном Поллардом (англ. John Pollard) в 1978 году, основные идеи алгоритма очень похожи на идеи ро-алгоритма Полларда для факторизации чисел. Данный метод рассматривается для группы ненулевых вычетов по модулю , где — простое число, большее . # Выполнение лабораторной работы

## 3.1 -Метод Полларда

### 3.1.1 Задача

Реализовать -Метод Полларда для задач дискретного логарифмирования.

#### 3.1.1.1 Решение

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

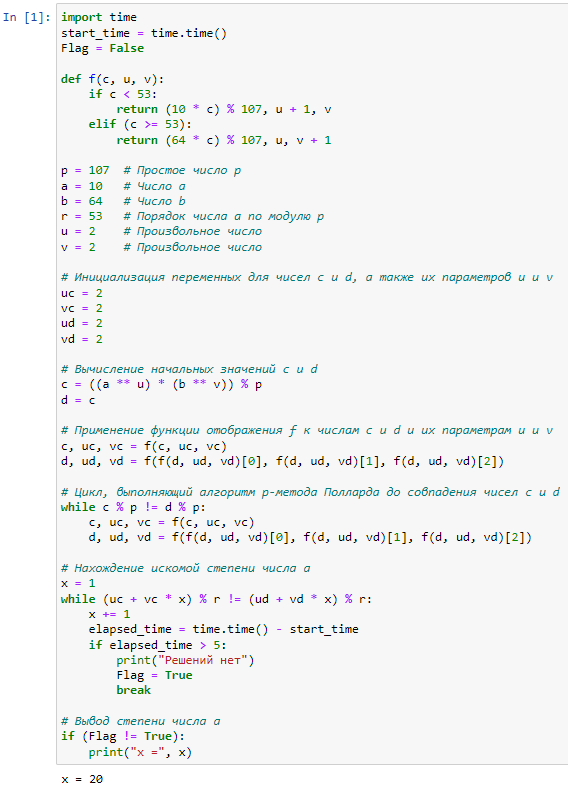


Figure 1: p-Метод Полларда

# 4 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал алгоритм, реализующий -метод Полларда для задач дискретного логарифмирования.

# 5 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 №7. Дискретное логарифмирование в конечном поле. - 4 с. [Электронный ресурс]. М. URL: [Лабораторная работа №7. Дискретное логарифмирование в конечном поле.](https://esystem.rudn.ru/pluginfile.php/2089825/mod_folder/content/0/lab07.pdf) (Дата обращения: 30.11.2023).