Лабораторная работа №7.  
Дискретное логарифмирование в конечном поле

Студентка: Царитова Нина Аведиковна

Группа: НФИмд-02-23

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Содержание

# 1 Цель работы

Целью данной лабораторной работы является ознакомление с алгоритмом, реализующим Po-метод Полларда для дискретного логарифмирования, а также программное воплощение данного алгоритма.

# 2 Задание

1. Реализовать рассмотренный в инструкции к лабораторной работе алгоритм программно.
2. Подставить численное значение из примера в программный код, проверить правильность полученного ответа.

# 3 Теоретическое введение

В данной лабораторной работе предметом нашего изучения стал Pо-метод Полларда для задач дискретного логарифмирования.

## 3.1 Po-метод Полларда

Ро-метод Полларда для дискретного логарифмирования ( -метод) — алгоритм дискретного логарифмирования в кольце вычетов по простому модулю, имеющий экспоненциальную сложность. Предложен британским математиком Джоном Поллардом 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 p, где p — простое число, большее 3.

## 3.2 Постановка задачи дискретного логарифмирования

Постановка задачи дискретного логарифмирования представлена следующим образом:

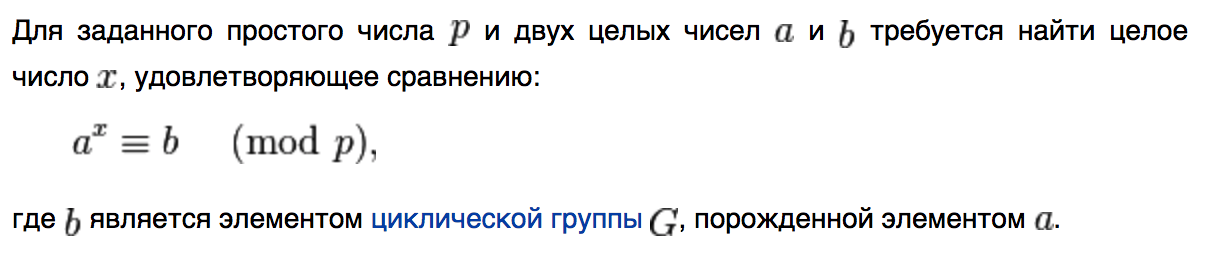


Figure 1: Постановка задачи дискретного логарифмирования

## 3.3 Алгоритм Ро-метода Полларда

Исходя из теоретических сведений, алгоритм Ро-метода Полларда представлен ниже.

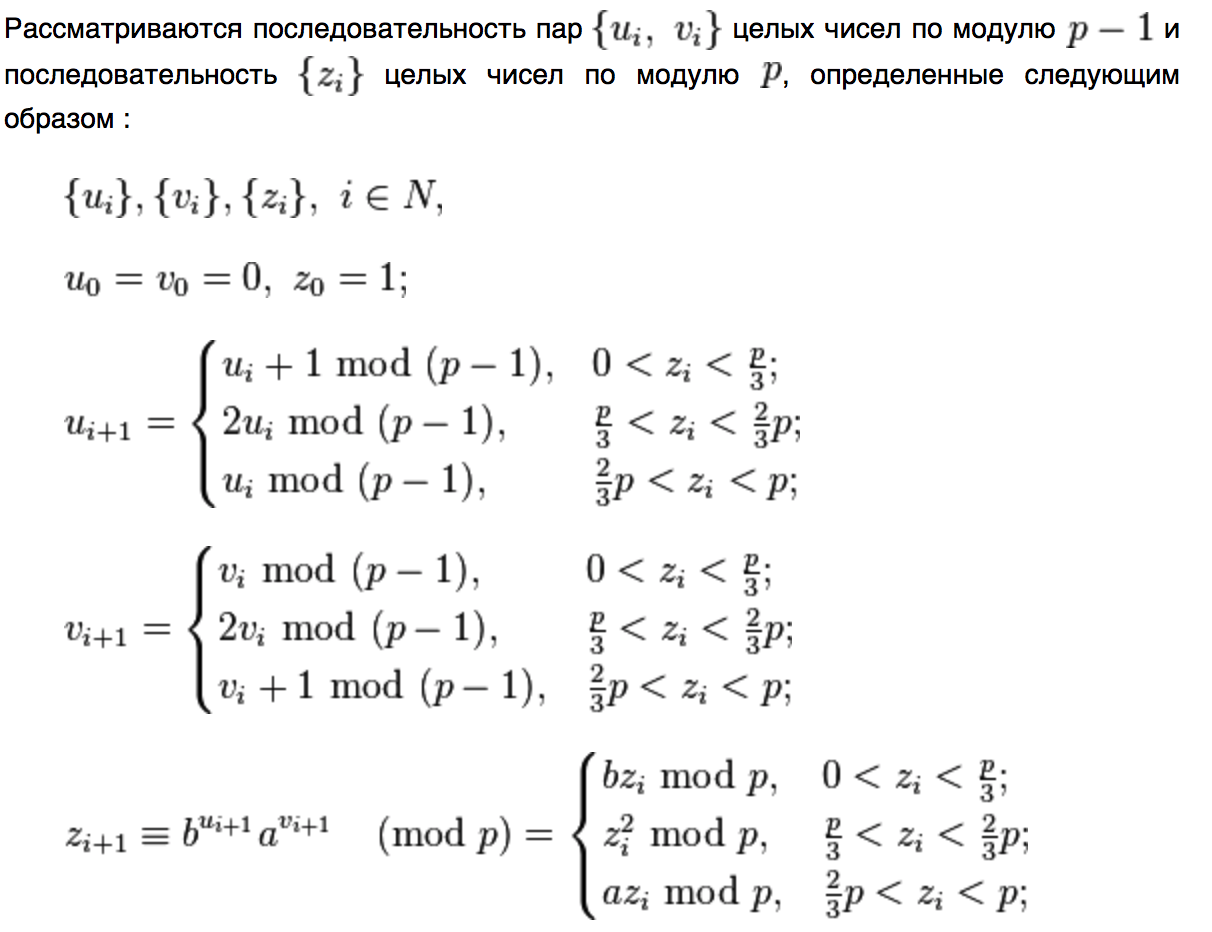


Figure 2: Алгоритм Ро-метода Полларда. 1.

При этом, важно учесть следующие замечания [**mind:pol?**]:

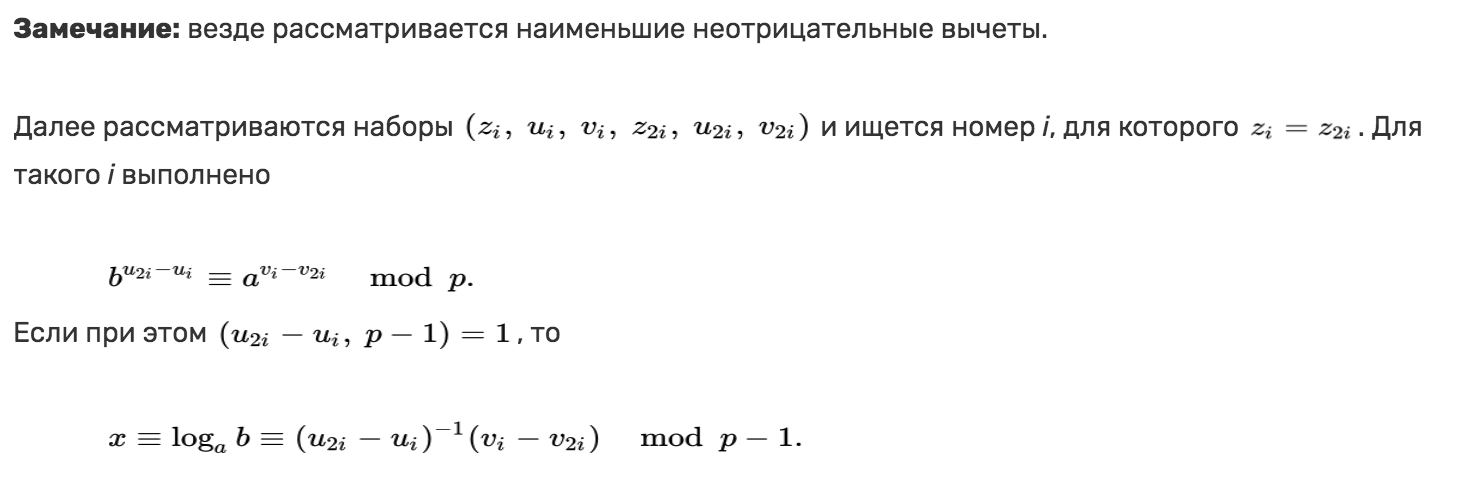


Figure 3: Алгоритм Ро-метода Полларда. 2.

## 3.4 Сложность алгоритма

Эвристическая оценка сложности составляет .

# 4 Выполнение лабораторной работы

В соответствии с заданием, была написана программа по воплощению алгоритма Ро-метода Полларда для задач дискретного логарифмирования.

Программный код и результаты выполнения программ представлен ниже.

## 4.1 Pо-метод Полларда

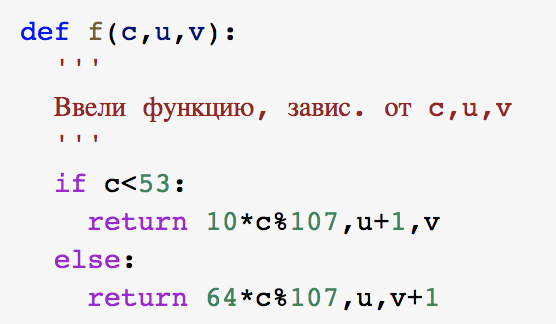


Figure 4: Вспомогательная функция, зависящая от c,u,v

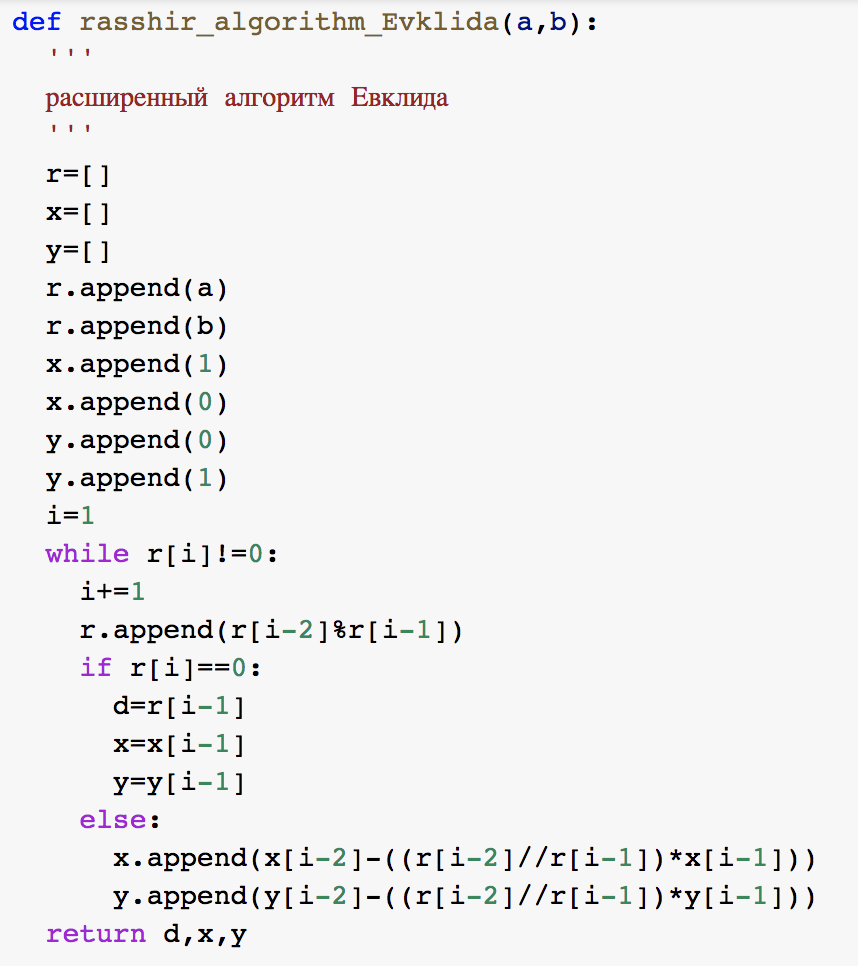


Figure 5: Вспомогательная функция. Расширенный алгоритм Евклида

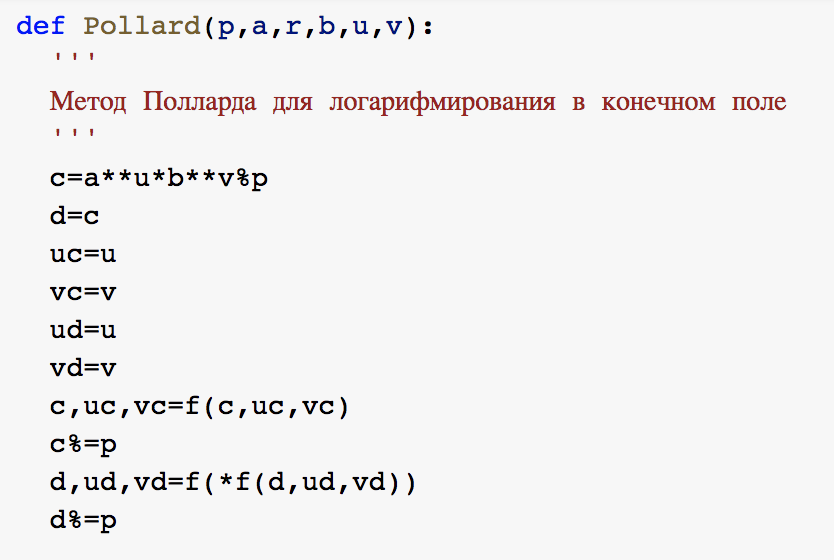


Figure 6: Реализация алгоритма Po-метода Полларда для логарифмирования

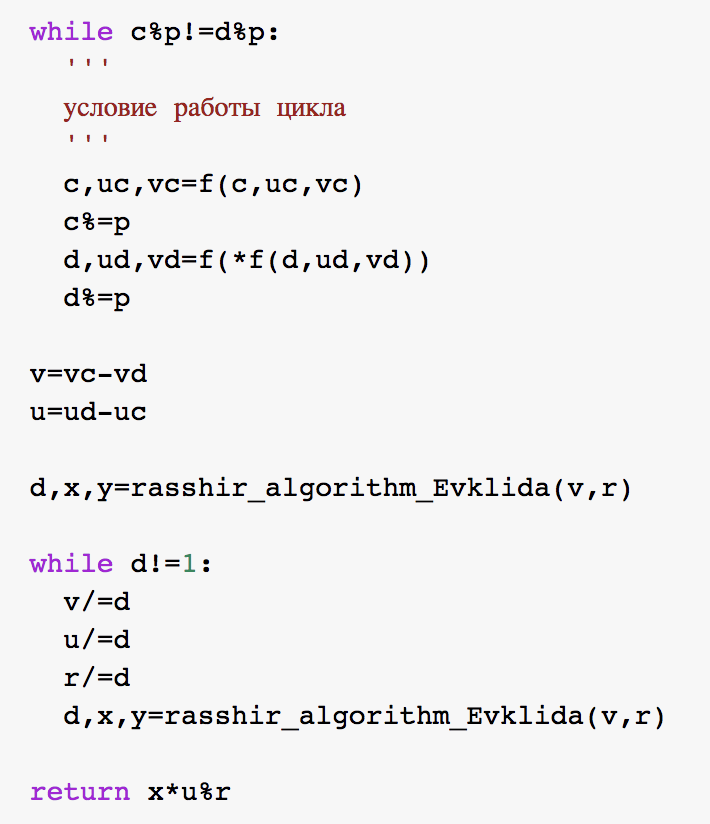


Figure 7: Реализация алгоритма Po-метода Полларда для логарифмирования

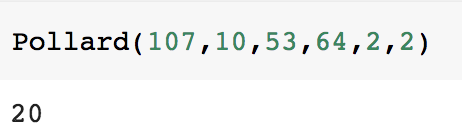


Figure 8: Результат реализации Po-метода Полларда на примере

# 5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: в результате выполнения данной лабораторной работы нам удалось изучить алгоритм Po-Полларда осуществить программно алгоритм, рассмотренный в описании к лабораторной работе на языке Python 3. А также получить ответ, совпадающий с ответом из инструкции.

# Список литературы

1. https://ru.wikipedia.org/wiki/Ро-метод\_Полларда\_для\_дискретного\_логарифмирования