Отчёт по лабораторной работе №7.  
Дискретное логарифмирование в конечном поле

Студент: Лапшенкова Любовь Олеговна, 10322127633

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

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 [1].

## 3.2 Постановка задачи дискретного логарифмирования

Постановка задачи дискретного логарифмирования представлена следующим образом:

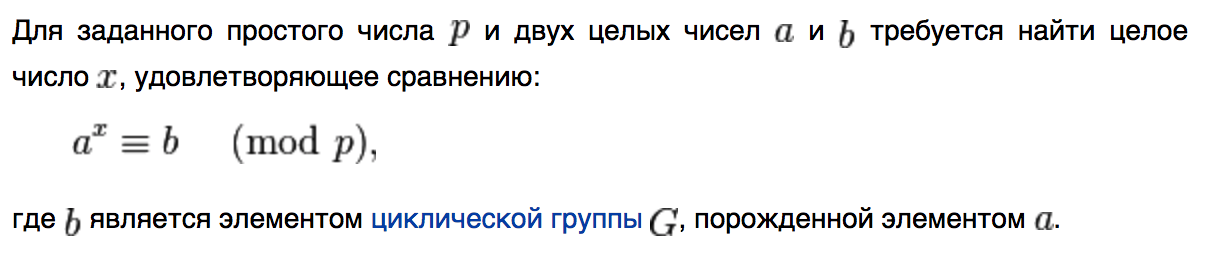


Figure 1: Постановка задачи дискретного логарифмирования

## 3.3 Алгоритм Ро-метода Полларда

Исходя из теоретических сведений, алгоритм Ро-метода Полларда представлен ниже [2].

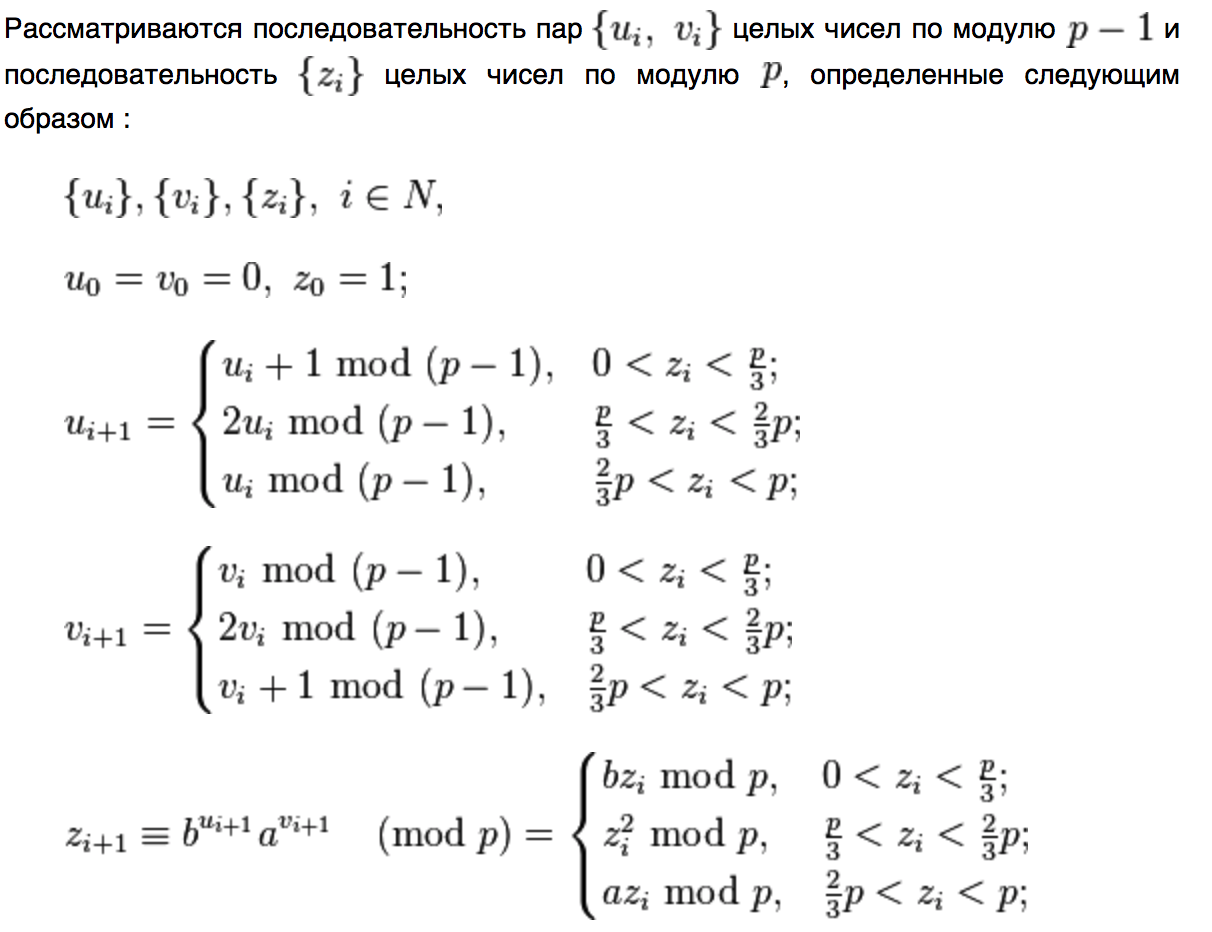


Figure 2: Алгоритм Ро-метода Полларда. 1.

При этом, важно учесть следующие замечания [3]:

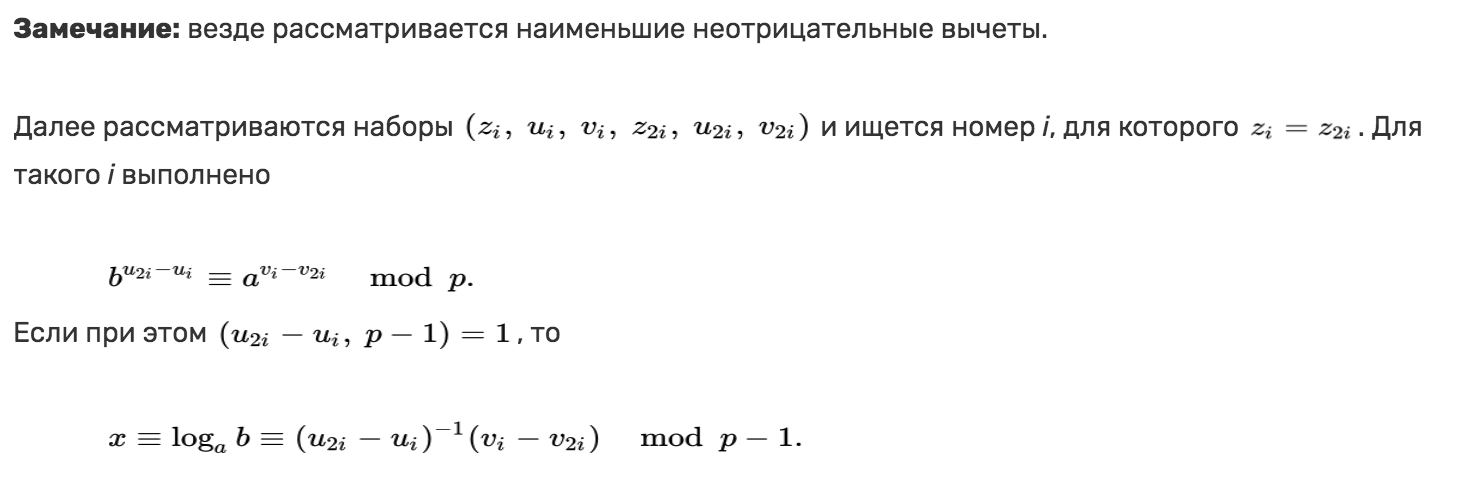


Figure 3: Алгоритм Ро-метода Полларда. 2.

## 3.4 Сложность алгоритма

Эвристическая оценка сложности составляет .

# 4 Выполнение лабораторной работы

**Примечание:** комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

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

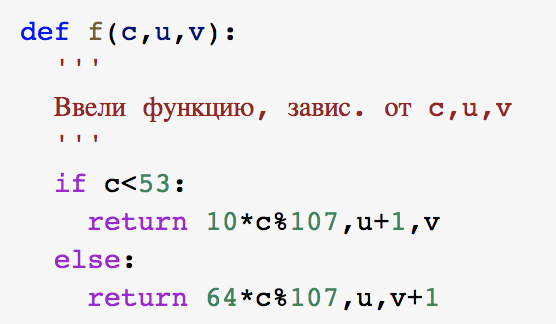


Figure 4: Вспомогательная функция, зависящая от c,u,v

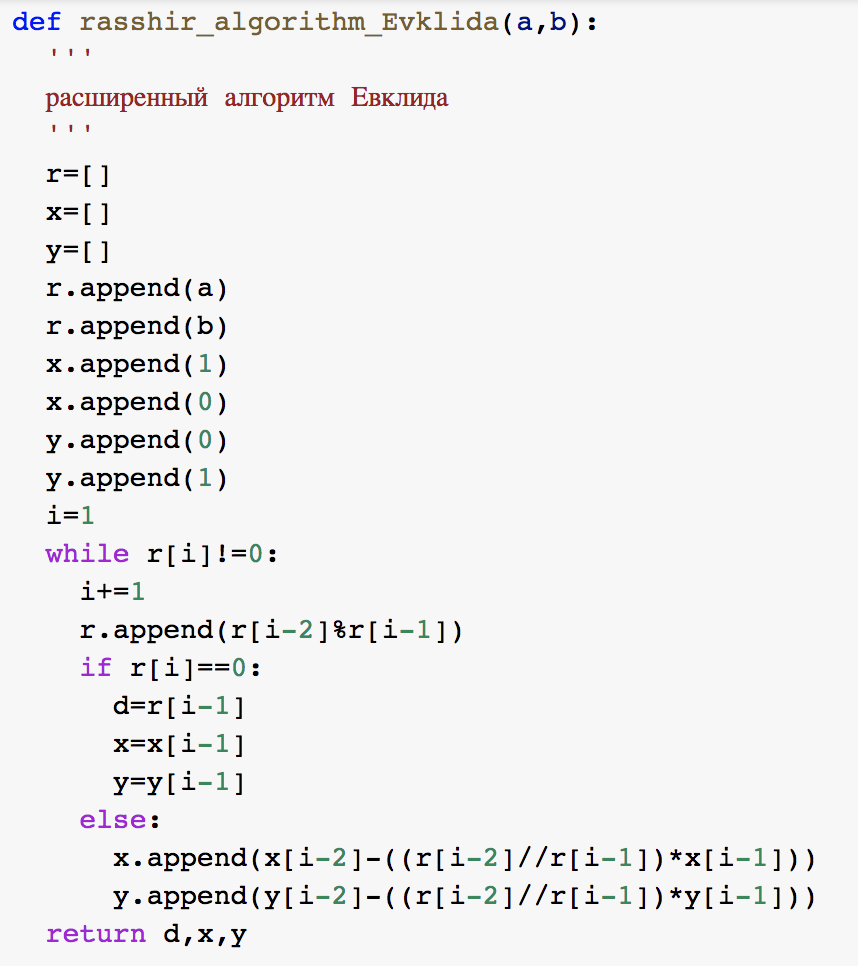


Figure 5: Вспомогательная функция. Расширенный алгоритм Евклида

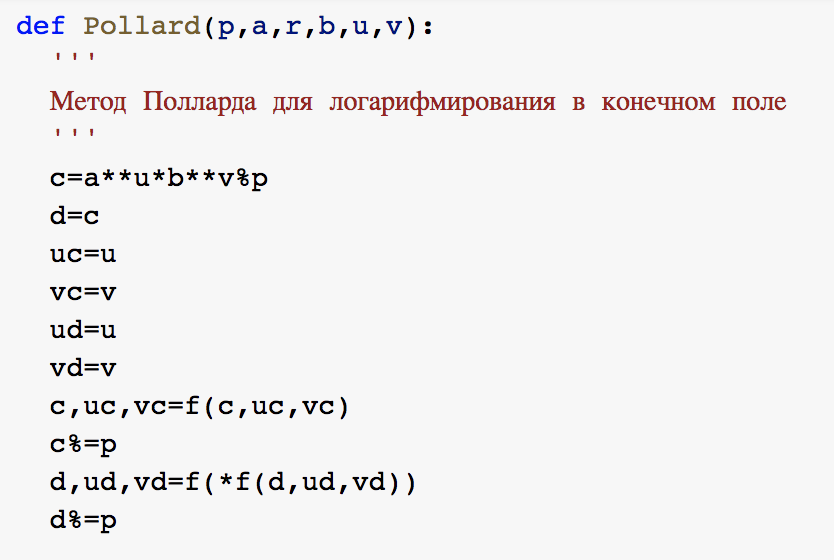


Figure 6: Реализация алгоритма Po-метода Полларда для логарифмирования

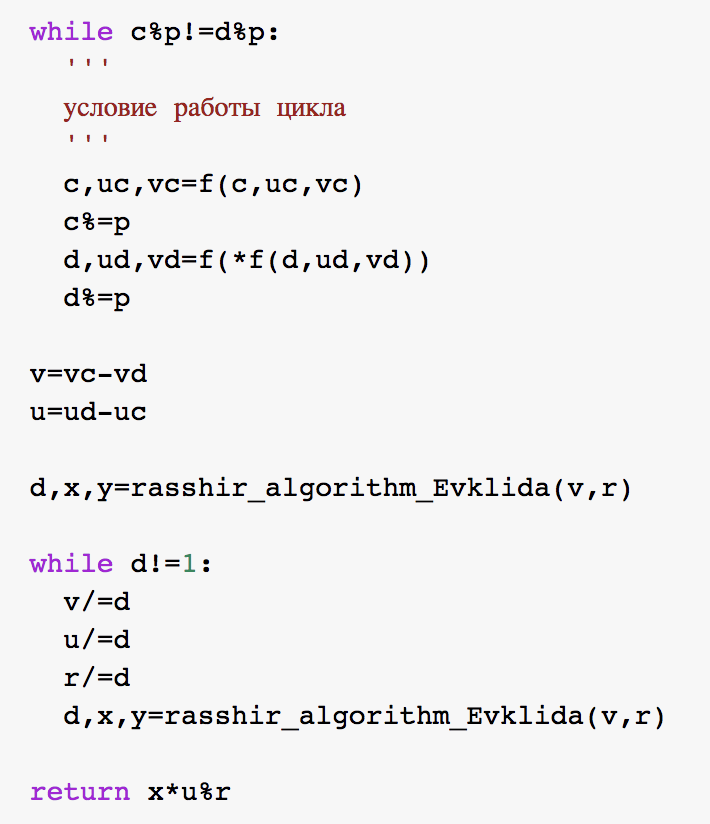


Figure 7: Реализация алгоритма Po-метода Полларда для логарифмирования

Были взяты данные из пояснения к лабораторной работе. Они были подставлены в программу. Получен следующий результат (см. рис. [-fig. 8).

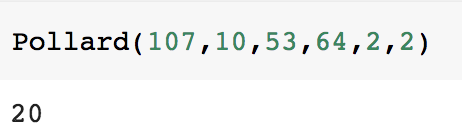


Figure 8: Результат реализации Po-метода Полларда на примере

# 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. Википедия. ро-метод Полларда для дискретного логарифмирования [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://ru.wikipedia.org/wiki/%D0%A0%D0%BE-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D0%9F%D0%BE%D0%BB%D0%BB%D0%B0%D1%80%D0%B4%D0%B0_%D0%B4%D0%BB%D1%8F_%D0%B4%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F> (дата обращения: 25.12.2021).

2. Wikiznanie. ро-метод Полларда для дискретного логарифмирования [Электронный ресурс]. Википедия, 2021. URL: <https://www.wikiznanie.ru/wp/index.php/%D0%A0%D0%BE-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D0%9F%D0%BE%D0%BB%D0%BB%D0%B0%D1%80%D0%B4%D0%B0_%D0%B4%D0%BB%D1%8F_%D0%B4%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F> (дата обращения: 25.12.2021).

3. Wikiznanie. Ρ-метод Полларда дискретного логарифмирования [Электронный ресурс]. Википедия, 2021. URL: <https://mind-control.fandom.com/wiki/%CE%A1-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D0%9F%D0%BE%D0%BB%D0%BB%D0%B0%D1%80%D0%B4%D0%B0_%D0%B4%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F> (дата обращения: 25.12.2021).