Отчёт по лабораторной работе №7

Дискретное логарифмирование в конечном поле

Студент: Гонсалес Ананина Луис Антонио, 1032175329

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать рассмотренный алгоритм программно.

# 2 Теоретические сведения

**Дискретное логарифмирование в конечном поле**

Пусть р — небольшое простое число, п> l,q = р’ GF(q) — конечное поле из q элементов, g — примитивный элемент поля GF(q), h е GF(q) Требуется найти решение уравнения g\* = h относительно х при известных g и h. Решение данной задачи существенно зависит от способа представления элементов поля. В данном параграфе мы познакомимся с алгоритмами логарифмирования в GF(q), использующими изученные в курсе алгебры способы задания конечных полей.

Поле GF(q) может быть задано в виде GF(p)[y]/f(y), где f(y) — неприводимый многочлен над GF(p) степени п (см. [ГЕН2, утверждение 17, с. 181]). Поэтому можно считать, что поле GF(q) состоит из многочленов над GF(p) степени не более п - 1, в частности g = g(y). Операции в этом поле выполняются по модулю многочлена f(y)[1].

**Алгоритм полларда для дискретного логарифмирования**

р-метод Полларда для дискретного логарифмирования (p-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 p, где p — простое число, большее 3[2].

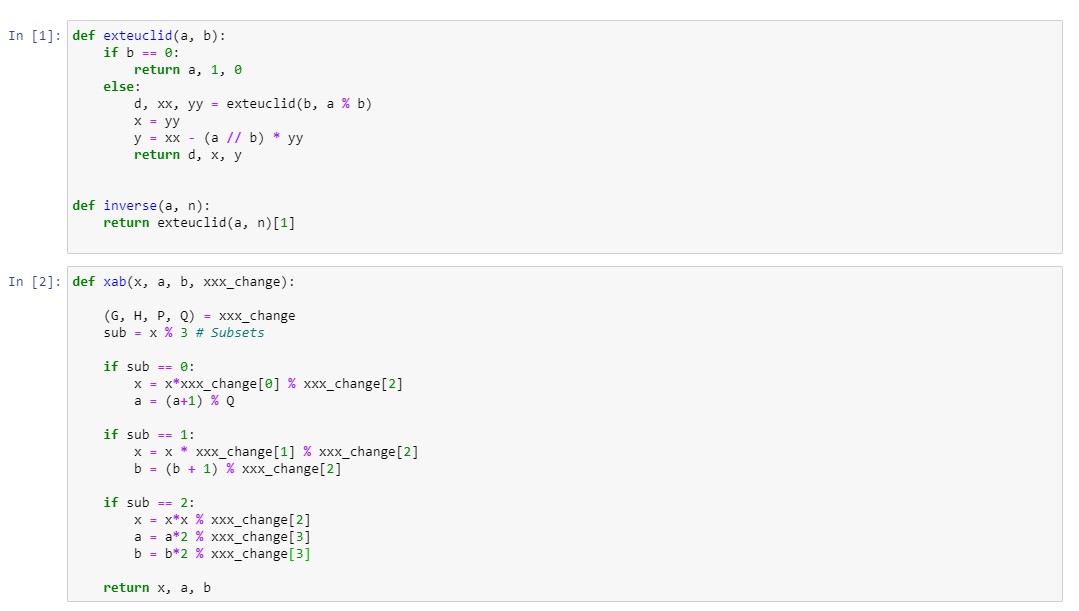
Для заданного простого числа p и двух целых чисел a и b требуется найти целое число x, удовлетворяющее сравнению:

Поллард

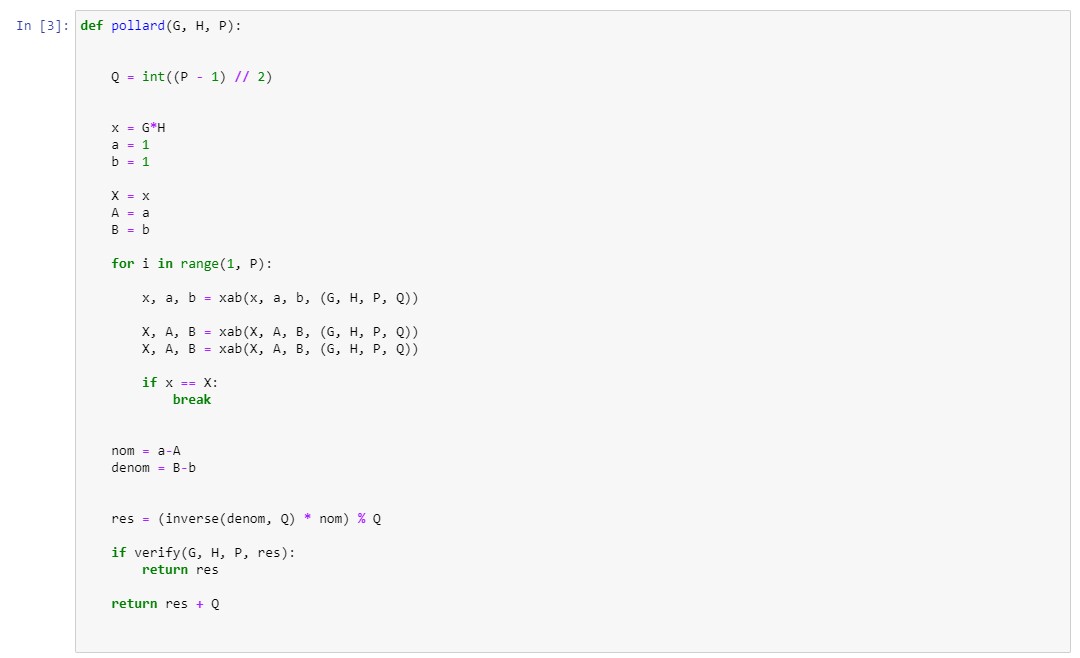
Поллард

где b является элементом циклической группыG, порожденной элементом a.

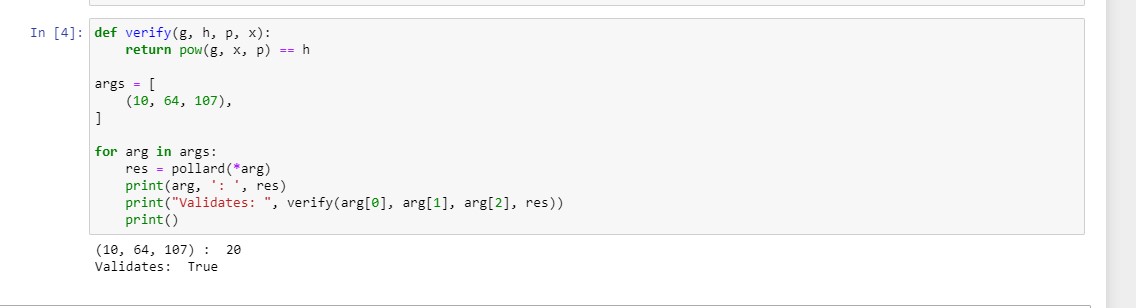
# 3 Выполнение работы



Выполнение1



Выполнение2



Выполнение3

# 4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал рассмотренный алгоритм программно.

# Список литературы

1. Дискретное логарифмирование в конечном поле [Электронный ресурс]. Википедия, 2021. URL: <https://ozlib.com/869476/informatika/algoritmy_diskretnogo_logarifmirovaniya_konechnom_neprostom_pole>.

2. Метод Полларда [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Ро-метод_Полларда_для_дискретного_логарифмирования>.