Лабораторная работа №7

Дисциплина: Математические основы защиты информации и информационной безопасности

Аветисян Давид Артурович

Содержание

# 1 Цель работы

Познакомиться с дискретным логарифмированием в конечном поле.

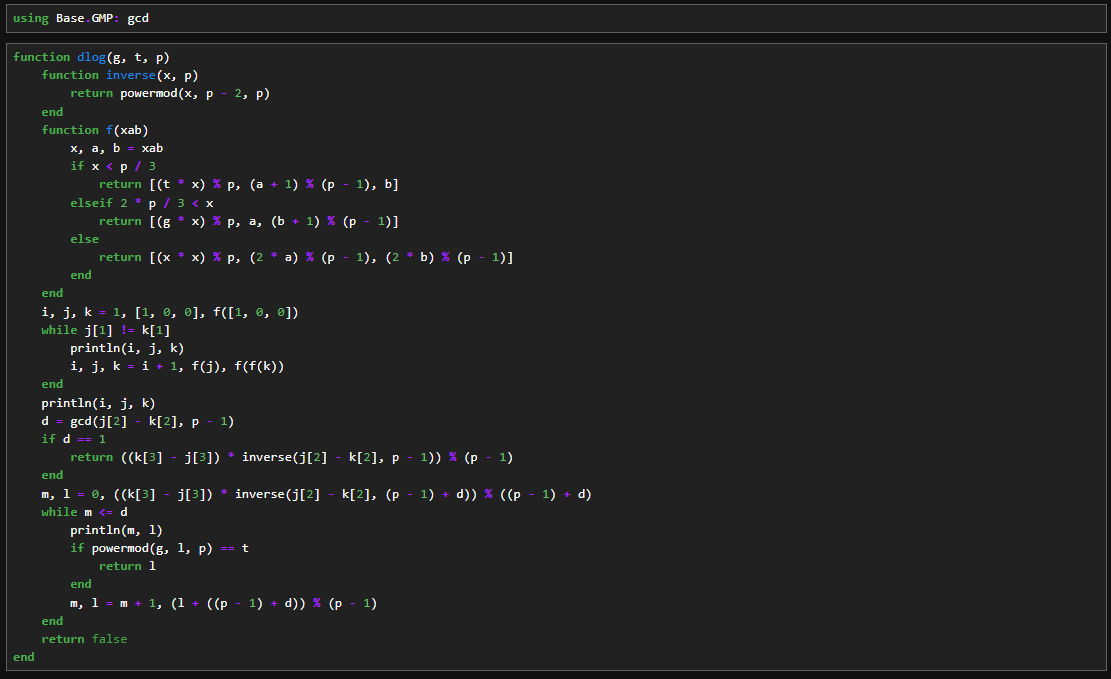
# 2 Задание

Реализовать алгоритм, реализующий p-метод Полларда.

# 3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

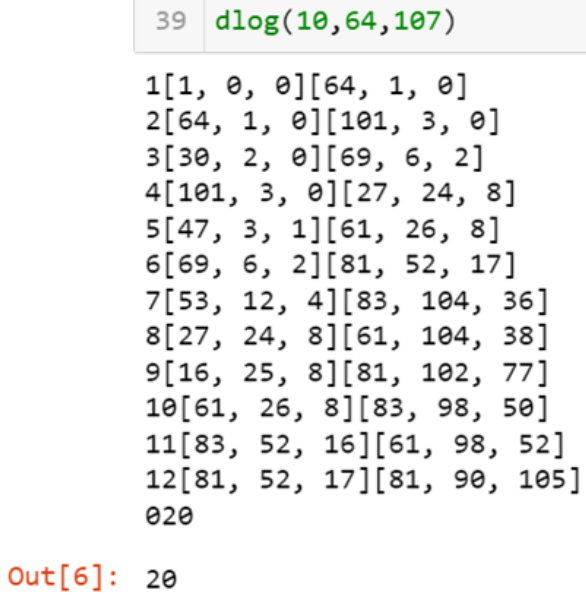
Для реализации p-метода Полларда была написана следующая программа.



p-метод Полларда

В данной программе: - 1 строка: подключение библиотеки для нахождения НОД. - 3 строка: задание функции. - 4-16 строки: задание внутренней функции для вывода результатов. - 17 строка: задание начальных значений. - 18 строка: начало вычисления, пока не получим равенство. - 19-36 строки: запуск основного алгоритма, который с помощью вычисления остатков от деления и формул, представленных в теории лабораторной работы, формирует таблицу ответов. - 39 строка: запуск функции

Мы можем видеть результат на рисунке ниже. Программа работае верно.



Результат p-метода Полларда

# 4 Выводы

Я познакомился с дискретным логарифмированием в конечном поле и реализовал p-метод Полларда.