Лабораторна работа № 7

Дисректное логарифмирование в конечном поле

Покрас Илья Михайлович

Содержание

# 1 Цель работы

Реализовать алгоритм дискретного логарифмирования программно

# 2 Задание

Реализовать -метод Полларда для задач дискретного логарифмирования.

# 3 Теоретическое введение

-Метод Полларда для дискретного логарифмирования — 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 -алгоритма Полларда для факторизации чисел. Данный метод рассматривается для группы ненулевых вычетов по модулю p.

Постановка задачи:

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

# 4 Выполнение лабораторной работы

Я создал функцию -метод Полларда с входными параметрами a, b, p, v1, v2, u1, u2 (u, v могут быть как определнными числами, так и случайными значениями). Данная функция рассчитывает c и d, а так же их логарифмы. Далее вычисляется x, удовлетворяющее условия сравнения, что и является результатом (рис. 1).

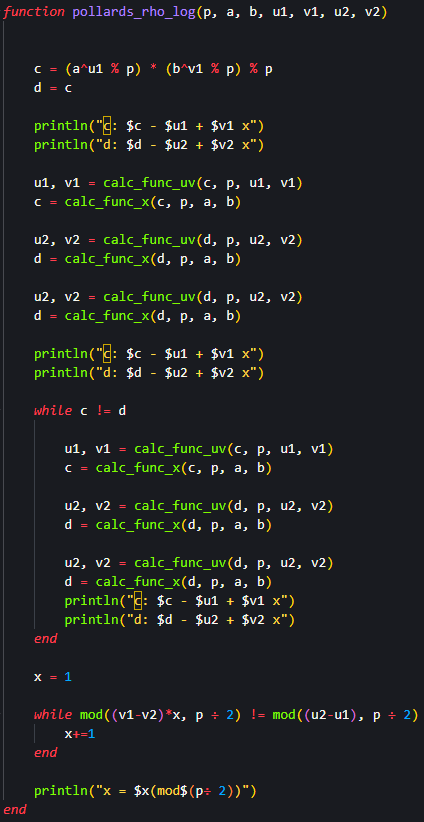


Рис. 1: Функция -метода для дискретного логарифмирования

Мною были созданы функции для расчета функции c и d, а также u и v в зависимости от того, к какому множеству относится проверяемое значение (рис. 2).

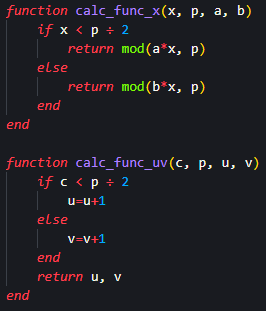


Рис. 2: Функции расчета

Далее были инциализированы переменные и вызвана функция с данными, взятыми из примера для большей наглядности (рис. 3).

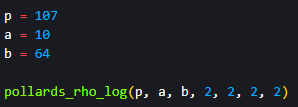


Рис. 3: Инициализация переменных и вызов функции

И получил следующие значения (рис. 4):

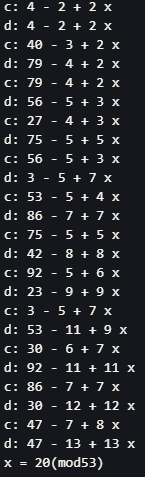


Рис. 4: Результат выполнения кода

# 5 Выводы

Я реализовал -метод Полларда для задач дискретного логарифмирования.

# Список Литературы

1. [Julia - Control Flow](https://docs.julialang.org/en/v1/manual/control-flow/)
2. [Julia - Mathematical Operations](https://docs.julialang.org/en/v1/manual/mathematical-operations/)
3. [Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone - Handbook of Applied Cryptography](https://cacr.uwaterloo.ca/hac/)