Отчёт по лабораторной работе 7

Дискретное логарифмирование в конечном поле

Воробьев А.О.

Содержание

# Цель работы

Реализация алгоритма, реализующий p-метод Полларда для задач дискретного логарифмирования.

# Теоретические сведения

Пусть в некоторой конечной мультипликативной абелевой группе задано уравнение

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа , удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Это сразу даёт грубую оценку сложности алгоритма поиска решений сверху — алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Чаще всего рассматривается случай, когда группа является циклической, порождённой элементом . В этом случае уравнение всегда имеет решение. В случае же произвольной группы вопрос о разрешимости задачи дискретного логарифмирования, то есть вопрос о существовании решений уравнения , требует отдельного рассмотрения.

**p-алгоритм Поллрада**

* Вход. Простое число , число порядка по модулю , целое число ; отображение , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
* Выход. показатель , для которого , если такой показатель существует.

1. Выбрать произвольные целые числа и положить
2. Выполнять , вычисляя при этом логарифмы для и как линейные функции от по модулю , до получения равенства
3. Приняв логарифмы для и , вычислить логарифм решением сравнения по модулю . Результат или РЕШЕНИЯ НЕТ.

# Выполнение лабораторной работы

1. Написал функцию ext\_euclid и inverse (рис. -@fig:001)

Функция для расширенного алгоритма Евклида и обратного значнения

1. Написал функцию xab (рис. -@fig:002)

Функция xab

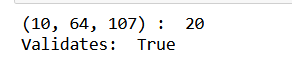
1. Написал функцию pollard (рис. -@fig:003)

Функция для алгоритма pollard

1. Написал функцию verify и блок работы программы(рис. -@fig:004)

Функция verify и блок работы программы

1. Получил результат (рис. -@fig:005)



Результат алгоритма

# Выводы

Реализовал реализующий p-метод Полларда для задач дискретного логарифмирования.

# Список литературы

1. Дискретное логарифмирование [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Дискретное\_логарифмирование