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 G задано уравнение

$$g^x = a$$

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, 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 g. 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 Полларда

- Вход. Простое число p, число a порядка r по модулю p, целое число b $1 < b < p$; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
- Выход. показатель x, для которого $a^x = b(modp)$, если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v (modp), d = c$
2. Выполнять $c = f(c)(modp), d = f\big(f(d)\big)(modp)$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c = d(modp)$
3. Приняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат x или РЕШЕНИЯ НЕТ.

Выполнение лабораторной работы

1. Написал функцию ext_euclid и inverse (рис. -@fig:001)

Функция для расширенного алгоритма Евклида и обратного значнения

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

Функция xab

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

Функция для алгоритма pollard

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

Функция verify и блок работы программы

5. Получил результат (рис. -@fig:005)

```
(10, 64, 107) :  20
Validates:  True
```

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