Математические основы защиты информации и информационной безопасности

Лабораторная работа №7 - Дискретное логарифмирование в конечном поле

Кейела Патачона, группа НПМмд-02-21

Содержание

# Цель и задание работы

***Цель***

Научиться дискретному логарифмированию в конечном поле

***Задания к лабораторной работе***

1. Реализовать алгоритм программно.
2. Получить у преподавателя задание, содержащее числа и вычислить логарифм.

# Выполнение работы

## Теоретическая часть

Задача дискретного логарифмирования, как и задача разложения на множители, применяется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Диффи и М.Хеллманом для установления сеансового ключа, та задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулсным разглашением и других криптографических протоколов.

Пусть над некоторым множеством Ω произвольной природы определены операции сложения и умножения . Множество Ω называется кольцом если выполняются следующие условия: 1. Сложение коммутативно: для любых ; 2. Сложение ассоциативно: для любых ; 3. Существует нулевой элемент такой, что для любого ; 4. Для каждого элемента существует противоположный элемент такой, что ; 5. Умножение дистрибутивно относительно сложения:

для любых .

Если в кольце Ω умножение коммутативно: для любых , то кольцо называется *коммунтативным*.

Если в колые Ω умножение ассоциативно: для любых , то кольцо называется *ассоциативным*.

Если в кольце Ω существует единичный элемент такой, что для любого , то кольцо называется кольцом с единицей.

Если в ассоциативном, коммутативном кольце с единицей для каждого ненулевого элемента существует обратный элемент такой, что , то кольцо называется *полем*.

Пусть . Целые числа и называются *сравнимыми по модулю* (обозначается (*mod m*)), если разность делится на Некоторые свойства отношения сравнимости:

1. *Рефлексивность:* (*mod m*).
2. *Симметричность:* если (*mod m*), то (*mod m*).
3. *Транзитивность:* если (*mod m*) и (*mod m*), (*mod m*).

Отношение, обладающее свойством рефлексивности, симметричности и транитимности, называется *отношением эквивалентности*. Отношение сравнимости является отношением эквивалентности на множестве целых чисел.

Отношение эквивалентности разбивает множество, на котором оно определено, на *классы эквивалентности*. Любые два класса эквивалентности либо не пересекаются, либо совпадают.

Классы эквивалентности, определяемые отношением сравнимости, называются *классами вычетов по модулю m*. Класс вычетов, содержащий число , обозначается *(mod m)* и представляет собой множество чисел вида , где : число называется представителем этого класса вычетов.

Множество классов вычетов по модулю обозначается , состоит ровно из элементов и относительно операций сложения и умножения является *кольцом классов вычетов по модулю т*.

Пример. Если , то  *= {0 (mod 2), 1 (mod 2))*, где *0 (mod 2) =*  множество всех четных чисел, *1 (mod 2)*  множество всех нечетных чисел.

Обозначим простое целое число и назовем конечным полем и элементов. Задача дискретного логарифмирования в конечном поле формулируется так: для данных целых чисел и , , найти логарифм - такое целое число , что (*mod m*) (если такое число существует). По аналогии с вещественными числами используется обозначение .

Безопасность соответствующих криптосистем основана на том, что зная числа , вычислить *(mod p)* легко, а решит задачу дискретного логарифмирования трудно. Рассмотрим р-Метод Полларда, который можно применить и для задач дискретного логарифмирования. При этом случайное отображение должно обладать не только сжимающими свойствами, но и вычислимостью логарифма (логарифм числа можно выразить через неизвестный логарифм и ). Для дискретного логарифмирования в качестве случайного отображения чаще всего используются ветвящиеся отображения, например:

При имеем , при

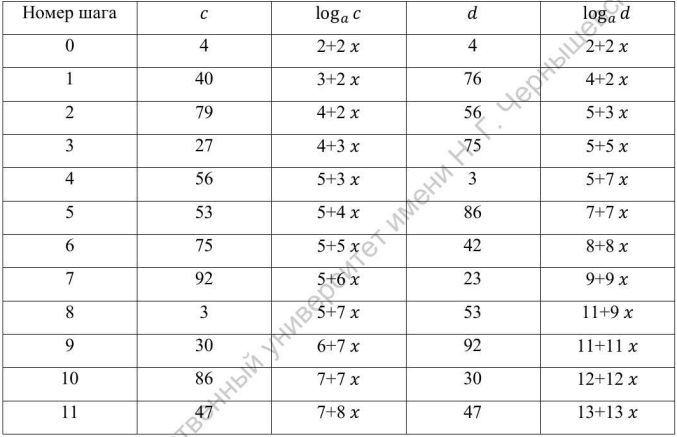
## Алгоритм, реализующий Метод Полларда для задач дискретного логарифмирования.

*Вход.* Простое число , число порядка по модулю , целое число , ; отображение , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

*Выход.* Показатель , для которого *(mod p)*, если такой показатель существует. 1. Выбрать произвольные целые числа положить *(mod p)*, 2. Выполнять *(mod p)*, *(mod p)*, вычисляя при этом логарифмы для и как линейные функции от по модулю , до получения равенства *(mod p)*. 3. Приравняв логарифмы для и , вычислить логарифм решением сравнения по модулю . Результат: или “Решений нет”.

Пример. Решим задачу дискретного логарифмирования *(mod 107)*, используя Метод Полларда. Порядок числа по модулю равен .

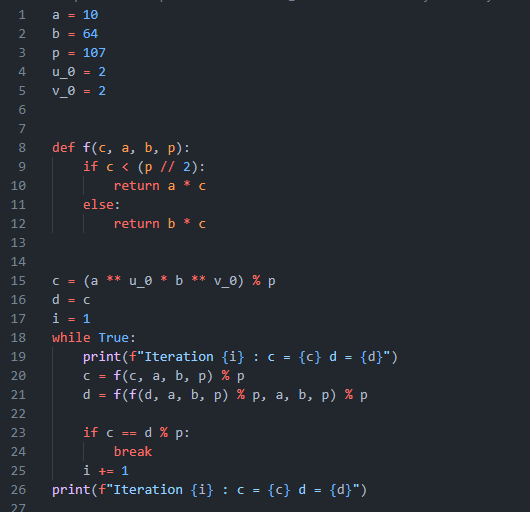
Выберем отображение *(mod 107)* при , *(mod 107)* при . Пусть . Результаты вычислений запишем в таблицу:



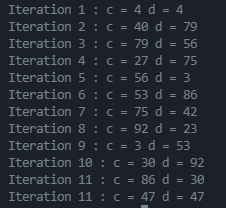
Пример дискретного логарифмирования

Приравниваем логарифмы, полученные на м шаге: *(mod 107)*. Решая сравнение первой степени, получаем: *(mod 53)*.

Проверка: *(mod 107)*.



Алгоритм Полларда



Результат алгоритма Полларда

# Выводы

Мной была узчена тема дискретного логарифмирования в конечном поле.

# Список литературы

1. [Инструкция к лабораторной работе №7](https://esystem.rudn.ru/pluginfile.php/1283466/mod_folder/content/0/lab07.pdf?forcedownload=1)