Лабораторная работа №7: отчет.

Дискретное логарифмирование в конечном поле

Евдокимов Максим Михайлович. Группа - НФИмд-01-24.

Содержание

# Цели и задачи работы

## Цель лабораторной работы

Вычисление дискретных логарифмов в конечном поле.

## Задание

Реализовать алгоритм, реализующий р-Метод Полларда для задач дискретного логарифмирования программно.

# Теоретическое введение

## алгоритм р-Метод Полларда для задач дискретного логарифмирования

p-Метод Полларда (Pollard’s rho method for discrete logarithms) — это алгоритм, используемый для решения задачи дискретного логарифмирования в конечных полях. Задача дискретного логарифмирования заключается в нахождении целого числа такого, что:

где , , и — известные целые числа, а — простое число.

### Основные шаги алгоритма

1. **Разделение последовательности**:
   * Последовательность разбивается на три подмножества , , и на основе некоторого правила. Например, можно использовать остаток от деления на 3.
2. **Функция перехода**:
   * Определяется функция перехода , которая перемещает элементы между подмножествами. Обычно используется следующая функция:
3. **Поиск коллизии**:
   * Используем метод “черепахи и зайца” для поиска коллизии.
4. **Решение уравнения**:
   * Пусть найдены и . Тогда:
   * Проверяем:
   * Таким образом, является решением.

### Применение алгоритма

Алгоритм p-Метода Полларда используется для решения задач дискретного логарифмирования в криптографии, где эта задача играет важную роль. Например, в системах шифрования на основе эллиптических кривых и в протоколах обмена ключами Диффи-Хеллмана.

### Преимущества и недостатки

**Преимущества**: - **Эффективность**: Алгоритм работает быстрее, чем полный перебор, особенно для больших . - **Простота реализации**: Алгоритм относительно прост в реализации.

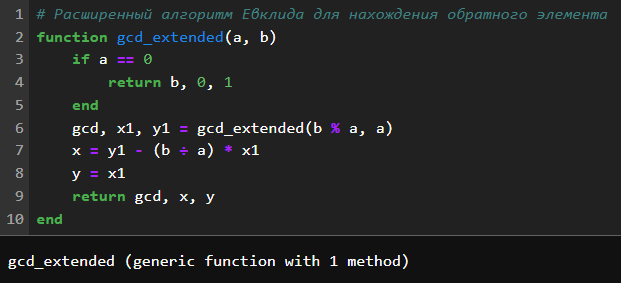
**Недостатки**: - **Не гарантирует успех**: Алгоритм может не найти решение, если не найдена коллизия. - **Зависимость от параметров**: Эффективность алгоритма зависит от выбора параметров , , и .

### Заключение

Алгоритм p-Метода Полларда — это мощный инструмент для решения задач дискретного логарифмирования в конечных полях. Он использует метод “черепахи и зайца” для поиска коллизий и позволяет эффективно находить решения в криптографических задачах.

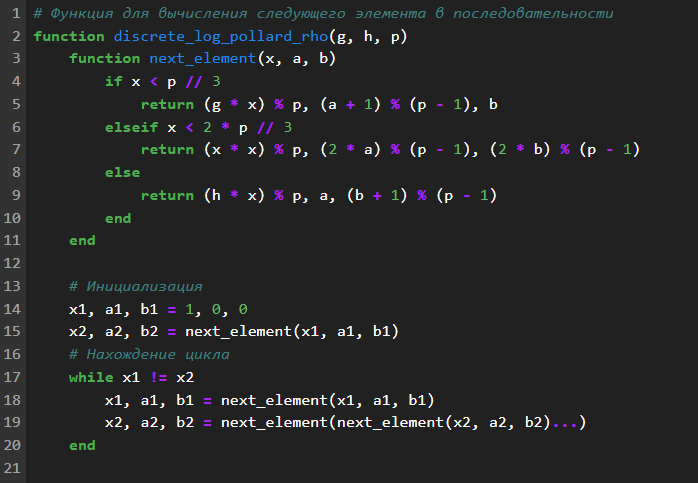
# Ход работы

## Расширенный алгоритм Евклида для нахождения обратного элемента

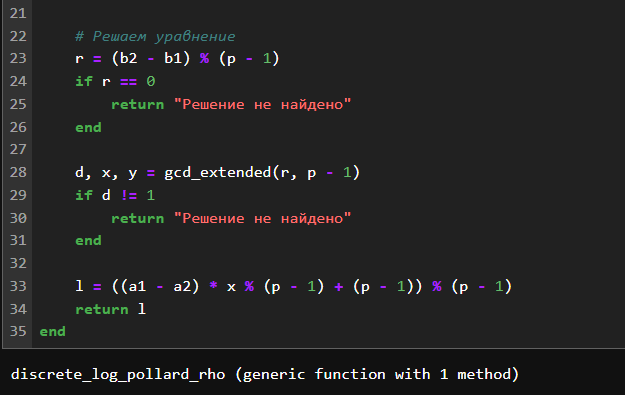


Расширенный алгоритм Евклида

## Функция для вычисления следующего элемента в последовательности

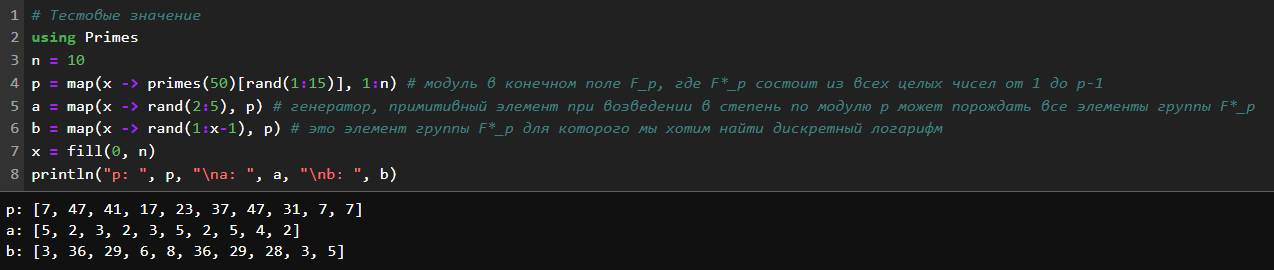


Функция для вычисления часть 1



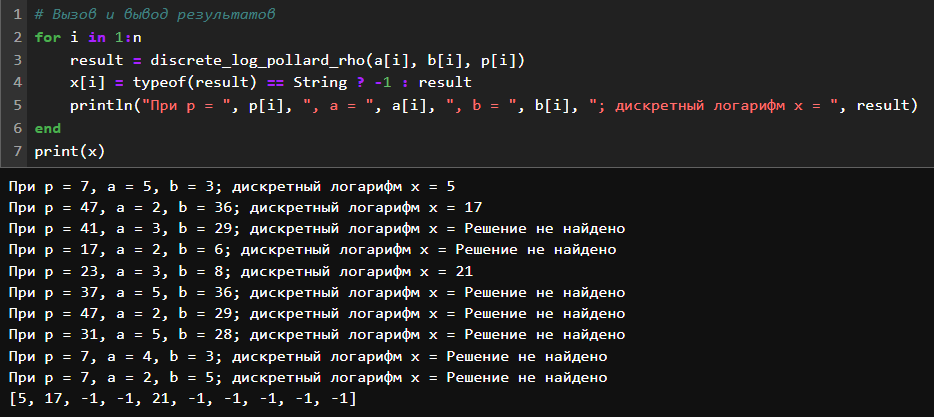
Функция для вычисления часть 2

## Тестовые значение

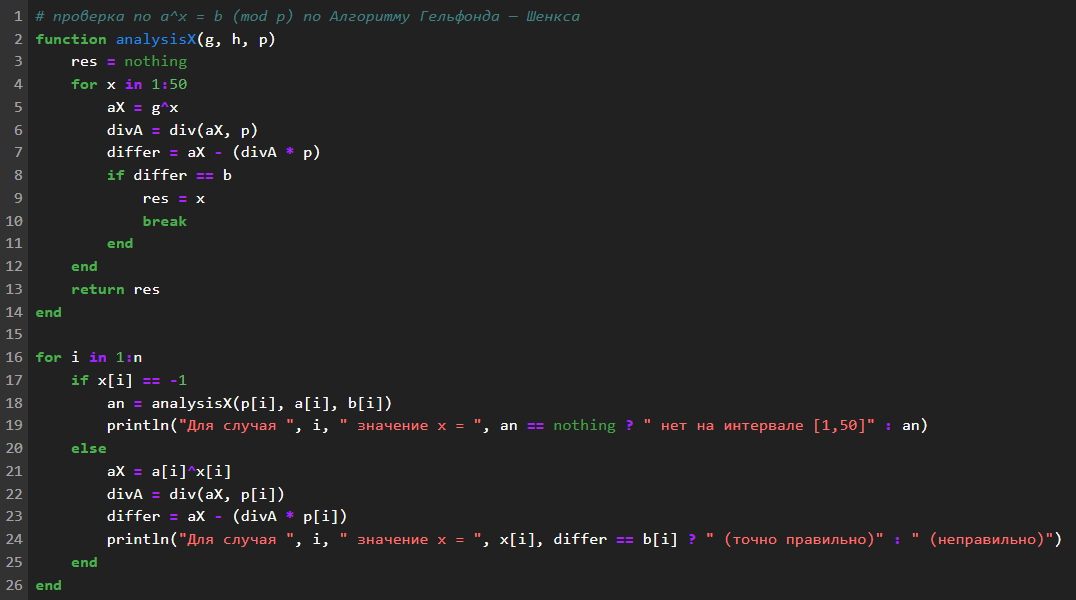


Стартовые значения и переменные

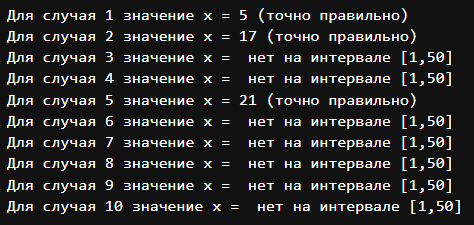
## Результаты и тесты



Вызов и вывод результатов



Проверка по a^x = b (mod p)



Результаты проверки

# Выводы по проделанной работе

## Вывод

В ходе выполнение лабораторной работы был изучен и реализован способ определения дискретного логарифма для дискретного логарифмирования в конечном поле с использованием алгоритм, реализующий р-Метод Полларда для задач дискретного логарифмирования.

# Список литературы

1. [Параллельный метод Полларда решения задачи дискретного логарифмирования с использованием детерминированной функции разбиения на множества](http://omega.sp.susu.ru/books/conference/PaVT2013/talks/Pogrebnyak.pdf)
2. [Поиск дискретного логарифма 2015 Сергей Николенко](https://logic.pdmi.ras.ru/~sergey/teaching/cryptoclub15/08-discretelog.pdf)
3. [Доступно о криптографии на эллиптических кривых](https://habr.com/ru/articles/335906/)