Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

[Цель работы 1](#_Toc184506255)

[Задание 1](#_Toc184506256)

[Теоретическое введение 1](#_Toc184506257)

[Выполнение лабораторной работы 2](#_Toc184506258)

[Выводы 2](#_Toc184506259)

[Список литературы 2](#_Toc184506260)

# Цель работы

Изучить дискретное логарифмирование в конечном поле и реализовать алгоритм программно на языке программмирования Julia.

# Задание

* Изучить теоретическую часть о дискретном логарифмировании;
* Реализовать алгоритм программно.

# Теоретическое введение

**P-метод Полларда**

Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

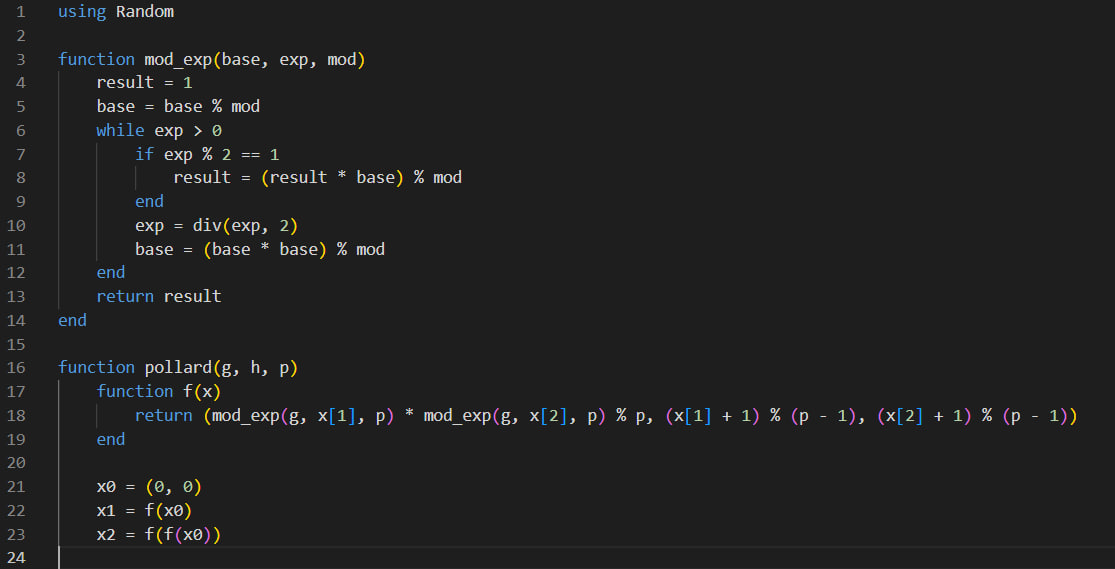
**Дискретное логарифмирование**

Дискретное логарифмирование (DLOG) — задача обращения функции g^x в некоторой конечной мультипликативной группе G.

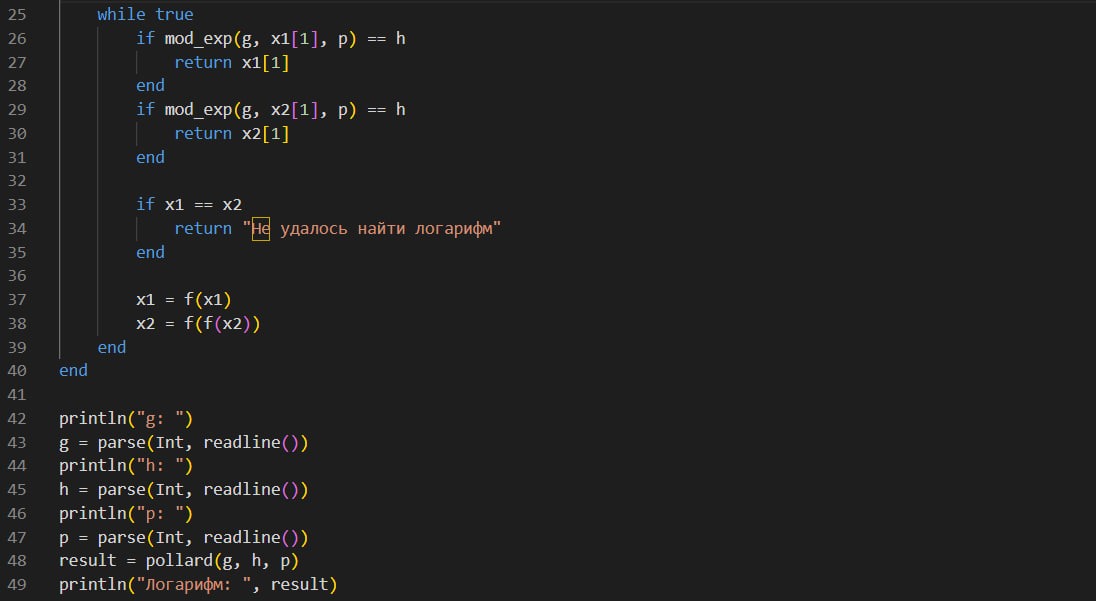
Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Для заданных g и a решение x уравнения g^x = a называется дискретным логарифмом элемента a по основанию g. В случае, когда G является мультипликативной группой кольца вычетов по модулю m, решение называют также индексом числа a по основанию g. Индекс числа a по основанию g гарантированно существует, если g является первообразным корнем по модулю m.

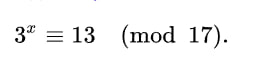
# Выполнение лабораторной работы



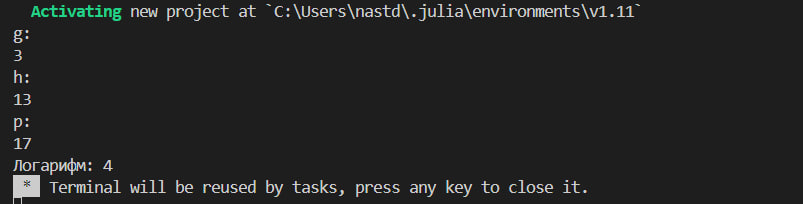
Код



Код2



Пример задачи



Результат

# Выводы

Мы изучили теоретическую часть о дискретном логарифмировании в конечном поле и реализовали алгоритм на языке программмирования Julia.

# Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/