

Лабораторная работа 7

Дискретное логарифмирование в конечном поле

Климин Никита Денисович

Российский университет дружбы народов

Содержание

- › **1 Цель работы**
- › **2 Задание**
- › **3 Теоретическое введение**
- › **4 Выполнение лабораторной работы**
- › **5 Выводы**
- › **Список литературы**

1 Цель работы

Изучить задачу дискретного логарифмирования в конечных полях и программно реализовать вероятностный алгоритм Полларда-р для нахождения дискретного логарифма.

2 Задание

Реализовать алгоритм Полларда-ρ для поиска показателя (x) из сравнения

$$[a^x \ b \ p,]$$

проверить его работу на тестовом примере и вывести найденное значение (x), либо сообщение об отсутствии решения.

3 Теоретическое введение

Задача дискретного логарифмирования состоит в нахождении (x) из сравнения $(a^x \equiv b \pmod{p})$.

Алгоритм Полларда-ρ — вероятностный метод, который строит последовательность значений по правилу $(f(c))$ и использует поиск цикла (черепаха–кролик).

При совпадении элементов последовательности возникает линейное сравнение, из которого вычисляется искомый логарифм (x).

4 Выполнение лабораторной работы

Программа была написана на Julia.

```
1 function powmod(a, e, m)
2     r = 1
3     a %= m
4     while e > 0
5         (e & 1 == 1) && (r = r * a % m)
6         a = a * a % m
7         e >= 1
8     end
9     r
10 end
11
12 function modinv(a, m)
13     t, newt = 0, 1
14     r, newr = m, a
15     while newr != 0
16         q = r ÷ newr
17         t, newt = newt, t - q * newt
18         r, newr = newr, r - q * newr
19     end
20     r == 1 ? mod(t, m) : nothing
21 end
22
23 function pollard_rho(a, b, p, n)
24     function step(c, u, v)
25         if c < p ÷ 2
26             c = (c * a) % p
27             u = (u + 1) % n
28     .
```

Пример работы программы в терминале

```
ndklimin@ndklimin:~/work/2025-2026/МОЗИиИБ/lab7$ julia lab7.jl
x = 20
```

Рисунок 1: Пример работы программы

5 Выводы

В ходе лабораторной работы был изучен алгоритм Полларда-ρ для задачи дискретного логарифмирования. Реализованная программа корректно вычисляет показатель x .

Список литературы

Speaker notes