
Дискретное логарифмирование в конечном поле

Милёхин Александр НПМмд-02-21



Цель лабораторной работы

Изучение задачи дискретного логарифмирования.

Задача дискретного логарифмирования

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.


р-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.
-
1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v \pmod{p}$, $d = c$
 2. Выполнять $s = f(c) \pmod{p}$, $d = f(f(d)) \pmod{p}$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r до получения равенства $c = d \pmod{p}$
 3. Приняв логарифмы для c и d , вычислить логарифм x решением сравнения по модулю r . Результат x или “Решения нет”.

Оценка сложности

Алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Пример работы алгоритма



The screenshot displays the JupyterLab interface. At the top, there is a menu bar with options: File, Edit, View, Insert, Cell, Kernel, Widgets, and Help. Below the menu bar is a toolbar containing icons for file operations (save, add, delete, copy, paste), cell navigation (up, down, run), and a dropdown menu currently set to 'Code'. The main area is a code editor with a light blue background. It contains the following Python code:

```
return res
return res + Q

def verify(g, h, p, x):
    return pow(g, x, p) == h

args = [(10, 64, 107)]

for arg in args:
    res = pollard(*arg)
    print(arg, ':   x =', res)
    print("Верификация: ", verify(arg[0], arg[1], arg[2], res))
    print()
```

Below the code editor, the output of the code execution is shown:

```
(10, 64, 107) :   x = 20
Верификация: True
```

Figure 1: Пример работы алгоритма
Получаем $x = 20$ для значений в данном примере.

Результаты выполнения лабораторной работы

Я изучил задачу дискретного логарифмирования, повторить р-алгоритм Полларда, а также реализовал алгоритм программно на языке Python.

Спасибо за внимание

A solid orange horizontal bar at the bottom of the slide.