

# Дискретное логарифмирование

---

Драммех Мариама

9 декабря, 2024, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

# Цель лабораторной работы

Изучение задачи дискретного логарифмирования.

# **Выполнение лабораторной работы**

---

# 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 Поллрада

- 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.
  - Выход. показатель  $x$ , для которого  $a^x = b \pmod{p}$ , если такой показатель существует.
1. Выбрать произвольные целые числа  $u, v$  и положить  $c = a^u b^v \pmod{p}$ ,  $d = c$
  2. Выполнять  $c = f(c) \pmod{p}$ ,  $d = f(f(d)) \pmod{p}$ , 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.

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

# Пример работы алгоритма

```
57     return res
58     return res + Q
59
60 def verify(g, h, p, x):
61     return pow(g, x, p) == h
62
63 args = [(10, 64, 107)]
64
65 for arg in args:
66     res = pollrad(*arg)
67     print(arg, ' : ', res)
68     print("Validates: ", verify(arg[0], arg[1], arg[2], res))

```

(10, 64, 107) : 20  
Validates: True

[ 1: 1

**Figure 1:** Работа алгоритма



## **Выводы**

---

Изучили задачу дискретного логарифмирования.