# Дискретное логарифмирование в конечном поле

Кейела Патачона

25 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

# Цель и задание работы

# Цель и задание работы

***Цель***

Научиться дискретному логарифмированию в конечном поле

***Задания к лабораторной работе***

1. Реализовать алгоритм программно.
2. Получить у преподавателя задание, содержащее числа $p, a, b$ и вычислить логарифм.

# Выполнение лабораторной работы

# Алгоритм, реализующий $p$—Метод Полларда для задач дискретного логарифмирования.

*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 $a^x \equiv b$*(mod p)*, если такой показатель существует. 1. Выбрать произвольные целые числа $u, v$ положить $c \leftarrow a^u b^v$*(mod p)*, $d \leftarrow c$ 2. Выполнять $c \leftarrow f(c)$*(mod p)*, $d \leftarrow f(f(c))$*(mod p)*, вычисляя при этом логарифмы для $c$ и $d$ как линейные функции от $x$ по модулю $r$, до получения равенства $c \equiv d$*(mod p)*. 3. Приравняв логарифмы для $c$ и $d$, вычислить логарифм $x$ решением сравнения по модулю $r$. Результат: $x$ или “Решений нет”.

# Пример реализа

Пример. Решим задачу дискретного логарифмирования $10^x \equiv 64$*(mod 107)*, используя $p$—Метод Полларда. Порядок числа $10$ по модулю $107$ равен $53$.

Выберем отображение $f(c) \equiv 10c$*(mod 107)* при $c < 53$, $f(c) \equiv 64c$*(mod 107)* при $c \geq 53$. Пусть $u = 2, v = 2$. Результаты вычислений запишем в таблицу:

| Номер шага | $c$ | $\log_a c$ | $d$ | $\log_a d$ |
|---|---|---|---|---|
| 0 | 4 | 2+2 $x$ | 4 | 2+2 $x$ |
| 1 | 40 | 3+2 $x$ | 76 | 4+2 $x$ |
| 2 | 79 | 4+2 $x$ | 56 | 5+3 $x$ |
| 3 | 27 | 4+3 $x$ | 75 | 5+5 $x$ |
| 4 | 56 | 5+3 $x$ | 3 | 5+7 $x$ |
| 5 | 53 | 5+4 $x$ | 86 | 7+7 $x$ |
| 6 | 75 | 5+5 $x$ | 42 | 8+8 $x$ |
| 7 | 92 | 5+6 $x$ | 23 | 9+9 $x$ |
| 8 | 3 | 5+7 $x$ | 53 | 11+9 $x$ |
| 9 | 30 | 6+7 $x$ | 92 | 11+11 $x$ |
| 10 | 86 | 7+7 $x$ | 30 | 12+12 $x$ |
| 11 | 47 | 7+8 $x$ | 47 | 13+13 $x$ |

**Figure 1:** Пример дискретного логарифмирования

Приравниваем логарифмы, полученные на $11$—м шаге: $7 + 8x \equiv 13 + 13x$*(mod 107)*. Решая сравнение первой степени, получаем: $x = 20$*(mod 53)*.

# Алгоритм $p$—Полларда

```
a = 10
b = 64
p = 107
u_0 = 2
v_0 = 2


def f(c, a, b, p):
    if c < (p // 2):
        return a * c
    else:
        return b * c


c = (a ** u_0 * b ** v_0) % p
d = c
i = 1
while True:
    print(f"Iteration {i} : c = {c} d = {d}")
    c = f(c, a, b, p) % p
    d = f(f(d, a, b, p) % p, a, b, p) % p

    if c == d % p:
        break
    i += 1
print(f"Iteration {i} : c = {c} d = {d}")
```

# Результат реализации алгоритма

```
Iteration 1 : c = 4 d = 4
Iteration 2 : c = 40 d = 79
Iteration 3 : c = 79 d = 56
Iteration 4 : c = 27 d = 75
Iteration 5 : c = 56 d = 3
Iteration 6 : c = 53 d = 86
Iteration 7 : c = 75 d = 42
Iteration 8 : c = 92 d = 23
Iteration 9 : c = 3 d = 53
Iteration 10 : c = 30 d = 92
Iteration 11 : c = 86 d = 30
Iteration 11 : c = 47 d = 47
```

**Figure 3:** Результат алгоритма $p$—Полларда

# Выводы

# Выводы

Мной была узчена тема дискретного логарифмирования в конечном поле.