

# Дискретное логарифмирование в конечном поле

Лабораторная работа №7

---

Шутенко Виктория

17 сентября 2023

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Шутенко Виктория михайловна
- студентка Магистратуры
- группы НФИмд-02-23
- Российский университет дружбы народов

## Задание лабораторной работы

---

1. Реализовать алгоритм, реализующий р-Метод Полларда для задач дискретного логарифмирования.

Реализация алгоритма,  
реализующего р-метод Полларда  
для задач дискретного  
логарифмирования

---

# Реализация алгоритма, реализующего р-метод Полларда для задач дискретного логарифмирования

```
def po_method(a: int, b: int, p: int):
    print(f"\n{a}^{x} = {b} mod {p}")
    print("-----")
    print('|\\t{c}\\t\\tlog c\\t\\td\\t\\tlog d\\t|')
    print("-----")

    u = np.random.randint(4)
    v = np.random.randint(4)
    r = order(a, p)

    c = mod(np.power(a, u) * np.power(b, v), p)
    d = c

    u_c, u_d = u, u
    v_c, v_d = v, v

    print(f'|\\t{c}\\t\\t{u_c}+{v_c}x\\t\\t{d}\\t\\t{u_d}+{v_d}x\\t|')

    def f(x, u_x, v_x):
        if x < r:
            return mod(a*x, p), u_x + 1, v_x
        else:
            return mod(b*x, p), u_x, v_x + 1

    c, u_c, v_c = f(c, u_c, v_c)
    tmp_d = f(d, u_d, v_d)
    d, u_d, v_d = f(tmp_d[0], tmp_d[1], tmp_d[2])

    while mod(c, p) != mod(d, p):
        print(f'|\\t{c}\\t\\t{u_c}+{v_c}x\\t\\t{d}\\t\\t{u_d}+{v_d}x\\t|')
        c, u_c, v_c = f(c, u_c, v_c)
        tmp_d = f(d, u_d, v_d)
        d, u_d, v_d = f(tmp_d[0], tmp_d[1], tmp_d[2])

    print(f'|\\t{c}\\t\\t{u_c}+{v_c}x\\t\\t{d}\\t\\t{u_d}+{v_d}x\\t|')
    print("-----")

    x = 1
    # print(v_c - v_d, u_d - u_c)
    while mod((v_c - v_d)*x, r) != mod(u_d - u_c, r):
        x += 1
```

## Результаты

---



```
if __name__ == "__main__":  
    main()
```

$$10^x \equiv 64 \pmod{107}$$

c	log c	d	log d
100	2+0x	100	2+0x
87	2+1x	4	2+2x
4	2+2x	79	4+2x
40	3+2x	56	5+3x
79	4+2x	75	5+5x
27	4+3x	3	5+7x
56	5+3x	86	7+7x
53	5+4x	42	8+8x
75	5+5x	23	9+9x
92	5+6x	53	11+9x
3	5+7x	92	11+11x
30	6+7x	30	12+12x

$$x = 20$$

$$10^{(20)} \equiv 64 \pmod{107}$$

$$2^x \equiv 1 \pmod{15}$$

c	log c	d	log d
1	0+3x	1	0+3x
2	1+3x	4	2+3x
4	2+3x	4	2+5x

$$x = 2$$

$$2^2 \equiv 1 \pmod{15}$$

## Выводы

---

1. Реализован алгоритм, реализующий  $p$ -метод Полларда для задач дискретного логарифмирования.