# Лабораторная работа 7

**Дискретное логарифмирование в конечном поле**

Климин Никита Денисович

# Содержание

# 1. Цель работы

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

# 2. Задание

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

$$a^x \equiv b \pmod{p}$$

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.

```
function powmod(a, e, m)
    r = 1
    a %= m
    while e > 0
        (e & 1 == 1) && (r = r * a % m)
        a = a * a % m
        e >>= 1
    end
    r
end

function modinv(a, m)
    t, newt = 0, 1
    r, newr = m, a
    while newr != 0
        q = r ÷ newr
        t, newt = newt, t - q * newt
        r, newr = newr, r - q * newr
    end
    r == 1 ? mod(t, m) : nothing
end

function pollard_rho(a, b, p, n)
    function step(c, u, v)
```

```
        if c < p ÷ 2
            c = (c * a) % p
            u = (u + 1) % n
        else
            c = (c * b) % p
            v = (v + 1) % n
        end
        return c, u, v
    end

    u = rand(0:n-1)
    v = rand(0:n-1)
    c = powmod(a, u, p) * powmod(b, v, p) % p

    U, V, C = u, v, c

    for _ in 1:10^6
        c, u, v = step(c, u, v)
        C, U, V = step(C, U, V)
        C, U, V = step(C, U, V)

        if c == C
            num = (U - u) % n
            den = (v - V) % n
            inv = modinv(den, n)
            inv === nothing && return nothing
            return (num * inv) % n
        end
    end
    return nothing
end

function test()
```

```
    p = 107
    a = 10
    b = 64
    n = 53

    x = pollard_rho(a, b, p, n)

    println("x = ", x)
end

test()
```

**Пример работы программы в терминале**


Рис. 4.1.: 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