Лабораторна работа № 7 - Дисректное логарифмирование в конечном поле

Покрас Илья Михайлович НФИмд-01-24

4 ноября, 2024, Москва, Россия

Российский Университет Дружбы Народов Имени Патриса Лумумбы

Цель работы

Реализовать алгоритм дискретного логарифмирования программно

Задания

Реализовать ρ-метод Полларда для задач дискретного логарифмирования.

ρ-метод Полларда - основная функция

```
function pollards_rho_log(p, a, b, u1, v1, u2, v2)


    c = (a^u1 % p) * (b^v1 % p) % p
    d = c

    println("c: $c - $u1 + $v1 x")
    println("d: $d - $u2 + $v2 x")

    u1, v1 = calc_func_uv(c, p, u1, v1)
    c = calc_func_x(c, p, a, b)

    u2, v2 = calc_func_uv(d, p, u2, v2)
    d = calc_func_x(d, p, a, b)

    u2, v2 = calc_func_uv(d, p, u2, v2)
    d = calc_func_x(d, p, a, b)

    println("c: $c - $u1 + $v1 x")
    println("d: $d - $u2 + $v2 x")

    while c != d

        u1, v1 = calc_func_uv(c, p, u1, v1)
        c = calc_func_x(c, p, a, b)

        u2, v2 = calc_func_uv(d, p, u2, v2)
        d = calc_func_x(d, p, a, b)

        u2, v2 = calc_func_uv(d, p, u2, v2)
        d = calc_func_x(d, p, a, b)
        println("c: $c - $u1 + $v1 x")
        println("d: $d - $u2 + $v2 x")
    end

    x = 1

    while mod((v1-v2)*x, p ÷ 2) != mod((u2-u1), p ÷ 2)
        x+=1
    end

    println("x = $x(mod$(p÷ 2))")
end
```

Рис. 1: Функция ρ-метода для дискретного логарифмирования

ρ-метод Полларда - функции расчета

```
function calc_func_x(x, p, a, b)
    if x < p ÷ 2
        return mod(a*x, p)
    else
        return mod(b*x, p)
    end
end

function calc_func_uv(c, p, u, v)
    if c < p ÷ 2
        u=u+1
    else
        v=v+1
    end
    return u, v
end
```

Рис. 2: Функции расчета

ρ-метод Полларда - переменные и вызов функции

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

pollards_rho_log(p, a, b, 2, 2, 2, 2)
```

Рис. 3: Инициализация переменных и вызов функции

ρ-метод Полларда - результат

```
c: 3 - 5 + 7 x
d: 53 - 11 + 9 x
c: 30 - 6 + 7 x
d: 92 - 11 + 11 x
c: 86 - 7 + 7 x
d: 30 - 12 + 12 x
c: 47 - 7 + 8 x
d: 47 - 13 + 13 x
x = 20(mod53)
```

Рис. 4: Результат выполнения кода

Вывод

Я реализовал ρ-метод Полларда для задач дискретного логарифмирования.

Спасибо за внимание