Лабораторная работа №7

Морозова Ульяна

Российский университет дружбы народов, Москва, Россия

Цель работы

Целью работы является изучение алгоритм разложение чисел на множителей и реализация его на языке Julia.

Алгоритм p-метода Полларда для задачи дискретного логарифмирования

Алгоритм ρ-Полларда (Pollard's rho) — это вероятностный алгоритм для вычисления дискретного логарифма. Он особенно эффективен, когда порядок циклической группы является составным числом с небольшими простыми делителями, но работает и в общем случае быстрее, чем алгоритм перебора (Baby-step Giant-step), потребляя при этом значительно меньше памяти.

```
function extended_gcd(a::BigInt, b::BigInt)
    if a == 0
        return b, 0, 1
    else
        g, y, x = extended_gcd(b % a, a)
        return g, x - (b ÷ a) * y, y
    end
end

function pollard_rho_dlp(alpha::Union{Int, BigInt}, beta::Union{Int, BigInt},
    alpha, beta, p = BigInt(alpha), BigInt(beta), BigInt(p)
    n = p - 1
    function step(x, a, b)
        mode = x % 3
```

Результат его работы

```
Задача: 2^x = 22 (mod 29)
Дискретный логарифм x: 26
Проверка: 22 == 22
```

Выводы

Мы изучили работу алгоритма, а также реализовали его на языке Julia.