Лабораторная работа №6

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

Идея метода основана на малой теореме Ферма: если p — простое число, являющееся делителем натурального числа a, то a^(p − 1) == 1 mod p.

Алгоритм состоит из двух стадий: - Определение границы гладкости (B1). Чем больше B1, тем больше времени займёт вычисление, но большое B1 увеличивает шансы найти делитель на первой стадии. - Сбор в виде произведения M как можно большего числа степеней простых сомножителей так, чтобы M делилось на каждый сомножитель, входящий в разложение (p − 1). - Определение искомого делителя p по формуле: p = НОД(n, a^M − 1).

Код

```
using Random
function pollard_rho(n::Integer, c::Integer=1, f::Function=x -> x^2+1)
    a = c
    b = c
    while true
        a = f(a)%n
        b = f(f(b)%n) % n
        d = gcd(abs(a-b),n)
        if 1<d<n
            return d
        elseif d==n
            return 0
        end
    end
```

Результат его работы

```
Тестирование p-метода Полларда
=======================================
Тест: 8051
n = 8051, c = 1
Результат: Найден делитель p = 97
Проверка: 8051 = 97 × 83
Верность: true
---------------------------------------
Тест: 10403
n = 10403, c = 1
Результат: Найден делитель p = 101
Проверка: 10403 = 101 × 103
Верность: true
---------------------------------------
```

Выводы

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