Лабораторная работа 6

Разложение чисел на множители

Климин Никита Денисович

Содержание

1. Цель работы

Изучение и программная реализация вероятностного алгоритма разложения составных чисел на нетривиальные делители --- p-метода Полларда.

2. Задание

Реализовать p-метод Полларда для нахождения нетривиального делителя составного числа, проверить его работу и вывести результат.

3. Теоретическое введение

- **Составное число** - это число, имеющее хотя бы один нетривиальный делитель (кроме 1 и самого числа).

- **Нетривиальный делитель** - любое число (d), такое что (1 < d < n) и

$$n \bmod d = 0.$$

.

P-метод Полларда - вероятностный алгоритм для нахождения нетривиального делителя числа (n).

4. Выполнение лабораторной работы

Программа была написана на Julia.

```
function pollards_rho(n, x0=1, c=5)
    f(x) = (x^2 + c) % n
    a = b = x0
    d = 1
    while d == 1
        a = f(a)
        b = f(f(b))
        d = gcd(abs(a - b), n)
    end
    return d == n ? nothing : d
end

n = 1359331
factor = pollards_rho(n, 1, 5)
println("Нетривиальный делитель числа $n: $factor")
```

Пример работы программы в терминале

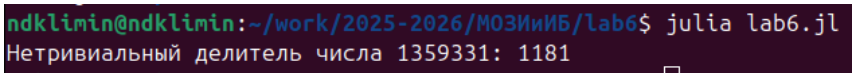

Рис. 4.1.: Пример работы программы

5. Выводы

Реализованный алгоритм корректно находит нетривиальный делитель составного числа.

Список литературы