

Презентация к лабораторной работе 6

Математические основы защиты информации и информационной безопасности

Аристова Арина Олеговна

01 ноября 2025

Российский университет дружбы народов, Москва, Россия

- Аристова Арина Олеговна
- студентка группы НФИмд-01-25
- Российский университет дружбы народов
- 1032259382@rudn.ru
- <https://github.com/aoaristova>



Цель работы

Изучить алгоритм Полларда для разложения составного числа на множители, реализовать его на языке Julia.

Задание

- Реализовать программно алгоритм Полларда
- Найти наименьший делитель числа с помощью реализованного алгоритма (или сделать вывод об отсутствии нетривиальных делителей)

Выполнение лабораторной работы

Основной блок кода

Код, реализующий алгоритм Полларда выглядит следующим образом.

Функция `main()` “вытаскивает” из запроса командной строки число, которое будем проверять, поданное в качестве аргумента, в противном случае (если на вход не подано число) проверяем какое-то число по умолчанию.

Основной блок кода

```
function main()
    if length(ARGS) > 0
        n = parse(Int, ARGS[1])
    else
        n = 1234537
    end
    println("Факторизация числа $n методом Полларда")
    println("Используется функция f(x) = x**2 + 5 mod n")
    result = pollard_rho(n)
    if result !== nothing
        println("Результат: $n = $result × $(n ÷ result)")
        println("Проверка: $result × $(n ÷ result) = $(result * (n ÷ result)))")
    else
        println("Делитель не найден для числа $n")
    end
end
```

Проверка работы кода

Проверяю работу кода. Рассматриваем разные числа: простое число, не имеющее делителей, и составное число

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
факторизация числа 1234537 методом Полларда
Используется функция f(x) = x**2 + 5 mod n
делитель не найден.
делитель не найден для числа 1234537
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
факторизация числа 123453 методом Полларда
Используется функция f(x) = x**2 + 5 mod n

Найден нетривиальный делитель: 9
Результат: 123453 = 9 x 13717
Проверка: 9 x 13717 = 123453
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
```

Рис. 1: Проверка работы кода для простого и составного чисел.

Вывод

В ходе выполнения лабораторной работы мною было реализовано программное решение алгоритма поиска нетривиального делителя составного числа методом Полларда.