

Презентация к лабораторной работе 5

Математические основы защиты информации и информационной безопасности

Аристова Арина Олеговна

24 октября 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 алгоритмы проверки чисел на простоту, реализовать их на языке Julia.

Задание

Реализовать несколько алгоритмов:

- алгоритм Ферма
- алгоритм Миллера-Рабина
- алгоритм Соловэя-Штрассена

Выполнение лабораторной работы

Основной блок кода

Выбор алгоритма, проверяемое число и число итераций программа получает из вводимых аргументов.

```
method = lowercase(ARGS[1])
n = parse(Int, ARGS[2])
count = length(ARGS) > 2 ? parse(Int, ARGS[3]) : 25

println("Проверяется число $n методом $(uppercase(method)) (количество итераций: $count)")

result = method == "f" ? Ferma(n, count) :
        method == "s" ? SoloveiStrassen(n, count) :
        method == "m" ? MillerRabin(n) :
        error("Неизвестный метод")
```

Проверка работы кода

Проверяю работу кода. Алгоритм Ферма

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl f 102 15
Проверяется число 102 методом F (кол-во итераций: 15)
Complex
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl f 103 15
Проверяется число 103 методом F (кол-во итераций: 15)
Simple
```

Рис. 1: Проверка работы кода для алгоритма Ферма.

Проверка работы кода

Проверяю работу кода. Алгоритм Миллера-Рабина

```
Complex
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl m 101 15
Проверяется число 101 методом M (кол-во итераций: 15)
Simple
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl m 102 15
Проверяется число 102 методом M (кол-во итераций: 15)
Complex
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> -
```

Рис. 2: Проверка работы кода для алгоритма Миллера-Рабина.

Проверка работы кода

Проверяю работу кода. Алгоритм Соловэя-Штрассена

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl s 102 15
Проверяется число 102 методом S (кол-во итераций: 15)
Complex
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05> julia .\lab05.jl s 101 15
Проверяется число 101 методом S (кол-во итераций: 15)
Simple
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab05>
```

Рис. 3: Проверка работы кода для алгоритма Соловэя-Штрассена.

Вывод

В ходе выполнения лабораторной работы мною были реализованы программные решения алгоритмы проверки чисел на простоту: алгоритма Ферма, алгоритма Соловэя-Штассена, алгоритма Миллера-Рабина.