Лабораторная работа №5

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

[Цель работы 1](#_Toc182082090)

[Задание 1](#_Toc182082091)

[Теоретическое введение 1](#_Toc182082092)

[Выполнение лабораторной работы 2](#_Toc182082093)

[Выводы 5](#_Toc182082094)

[Список литературы 6](#_Toc182082095)

# Цель работы

Изучить вероятностные алгоритмы проверки чисел на простоту и реализовать их программно на языке Julia.

# Задание

* Изучить теоретическую часть о вероятностных алгоритмах проверки чисел на простоту
* Реализовать вычисление символа Якоби и тесты: Ферма, Соловэя-Штрассена, Миллера-Рабина.

# Теоретическое введение

**Тест Ферма**

При проверке числа на простоту тестом Ферма выбирают несколько чисел a. Чем больше количество a, для которых утверждение истинно, тем больше вероятность, что число n простое. Однако существуют составные числа, для которых данное равенство выполняется для всех a взаимно простых с - это числа Кармайкла. Чисел Кармайкла — бесконечное множество, наименьшее число Кармайкла — 561. Тем не менее, тест Ферма довольно эффективен для обнаружения составных чисел.

**Тест Соловея-Штрассена**

Тест Соловея — Штрассена — вероятностный тест простоты, открытый в 1970-х годах Робертом Мартином Соловеем совместно с Фолькером Штрассеном. Тест всегда корректно определяет, что простое число является простым, но для составных чисел с некоторой вероятностью он может дать неверный ответ. Основное преимущество теста заключается в том, что он, в отличие от теста Ферма, распознает числа Кармайкла как составные.

**Тест Миллера-Рабина**

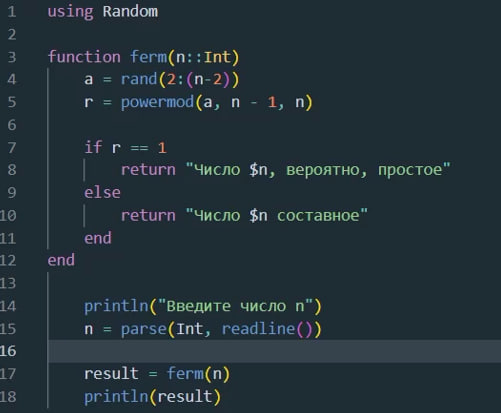
Тест Миллера — Рабина — вероятностный полиномиальный тест простоты. Тест Миллера — Рабина позволяет эффективно определять, является ли данное число составным. Однако, с его помощью нельзя строго доказать простоту числа. Тем не менее тест Миллера — Рабина часто используется в криптографии для получения больших случайных простых чисел. Алгоритм был разработан Гари Миллером в 1976 году и модифицирован Майклом Рабином в 1980 году.

**Символ Якоби**

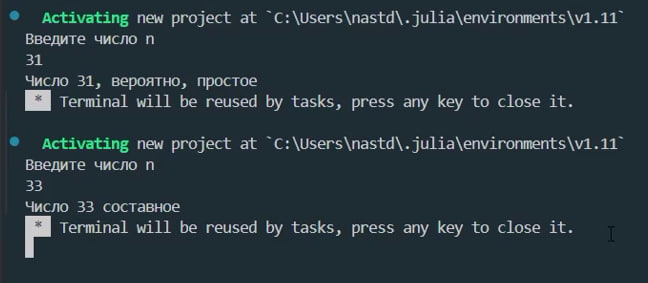
Символ Якоби — теоретико-числовая функция двух аргументов, введённая К. Якоби в 1837 году. Является квадратичным характером в кольце вычетов.

Символ Якоби обобщает символ Лежандра на все нечётные числа, большие единицы. Символ Кронекера — Якоби, в свою очередь, обобщает символ Якоби на все целые числа, но в практических задачах символ Якоби играет гораздо более важную роль, чем символ Кронекера — Якоби.

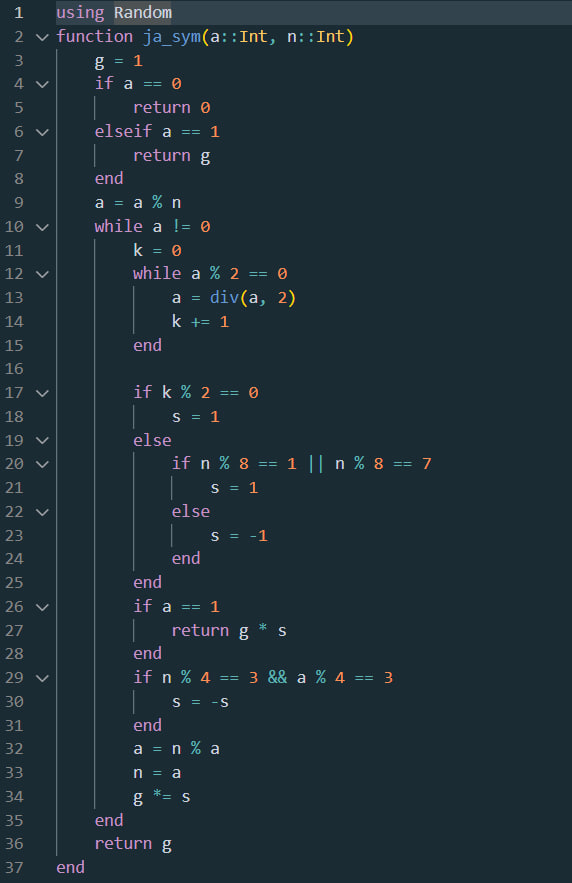
# Выполнение лабораторной работы



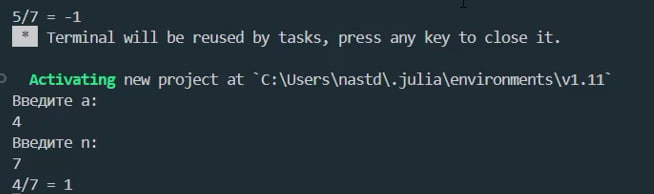
Тест Ферма



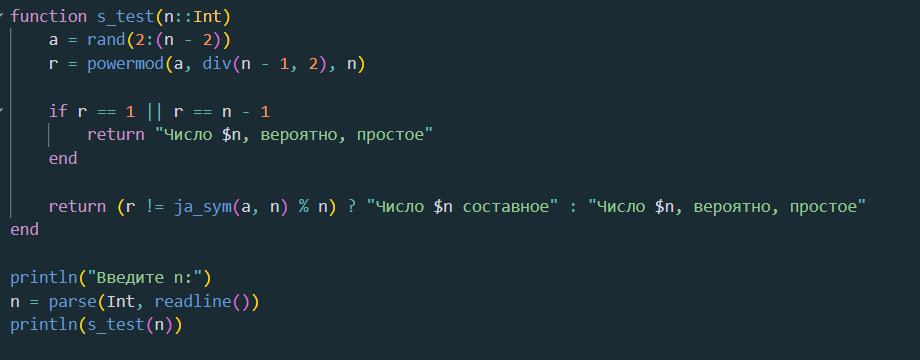
Результаты



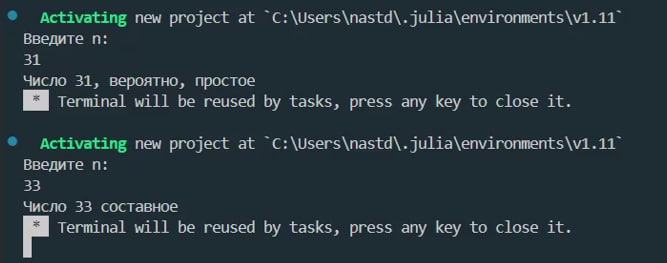
Символ Якоби



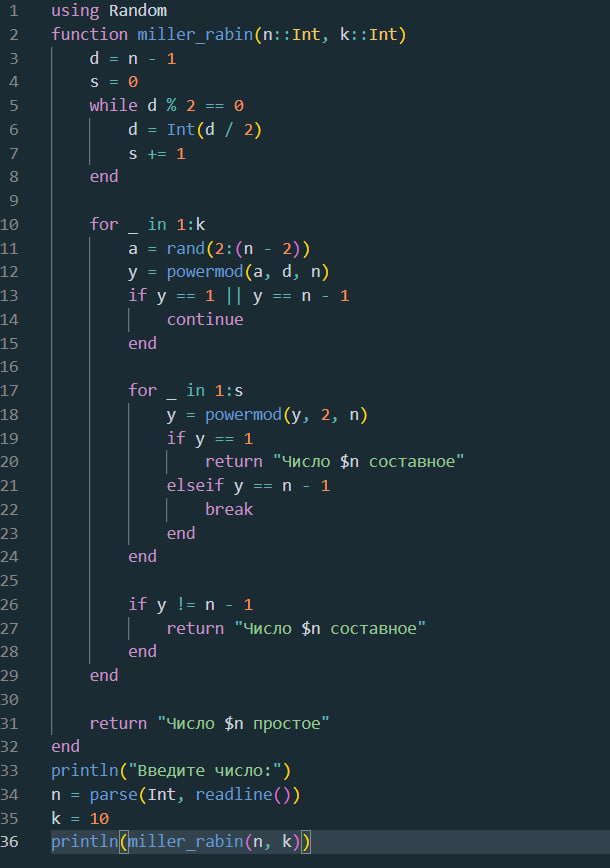
Результаты



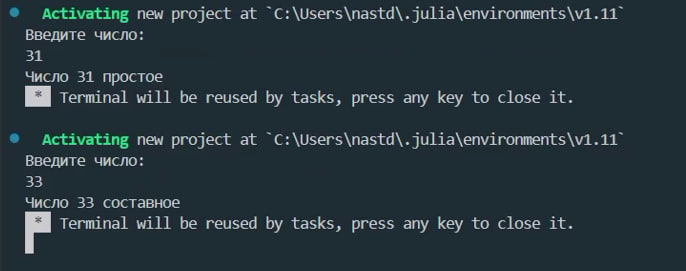
Тест Соловея-Штрассена



Результаты



Тест Миллера-Рабина



Результаты

# Выводы

Мы изучили вероятностные алгоритмы проверки чисел на простоту и реализовали их программно на языке Julia.

# Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/