Отчёт по лабораторной работе №5  
Математические основы защиты информации и информационной безопасности

Вероятностные алгоритмы проверки чисел на простоту

Выполнил: Махорин Иван Сергеевич,  
НФИмд-02-21, 1032259380

Содержание

# 1 Цель работы

Изучить вероятностные алгоритмы проверки чисел на простоту и научиться их реализовывать.

# 2 Выполнение лабораторной работы

## 2.1 Реализация вычисления символа 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.

Выполним реализацию этого алгоритма на языке Julia (рис. 1) и (рис. 2):

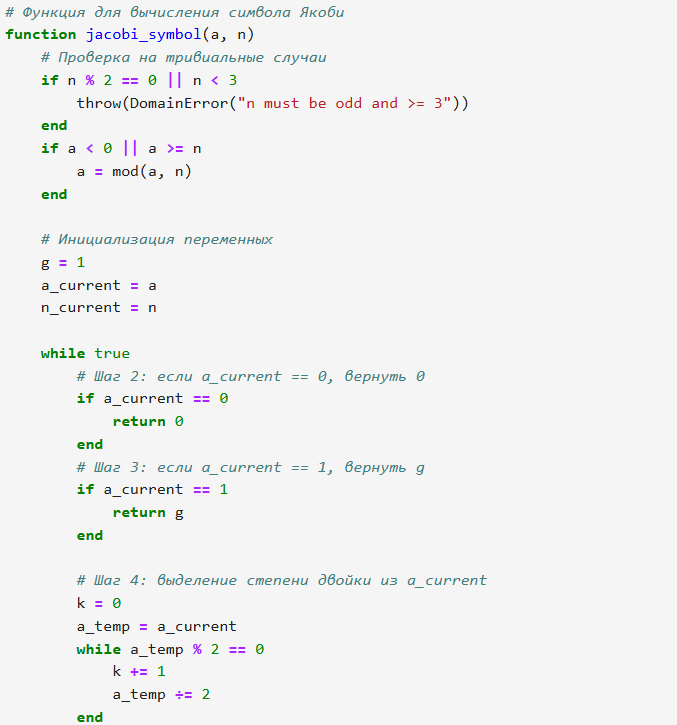


Рис. 1: Реализация вычисления символа Якоби

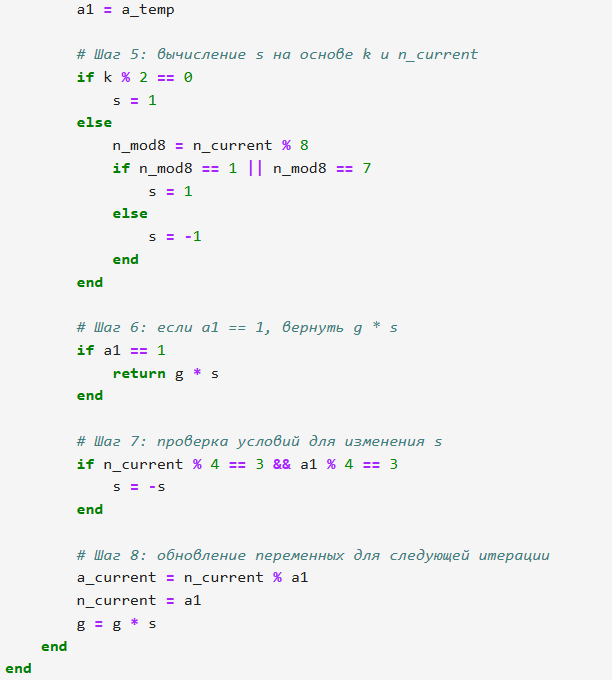


Рис. 2: Реализация вычисления символа Якоби

## 2.2 Реализация алгоритма, реализующего тест Ферма

Тест простоты Ферма в теории чисел — это тест простоты натурального числа , основанный на малой теореме Ферма.

Выполним реализацию этого алгоритма на языке Julia (рис. 3):

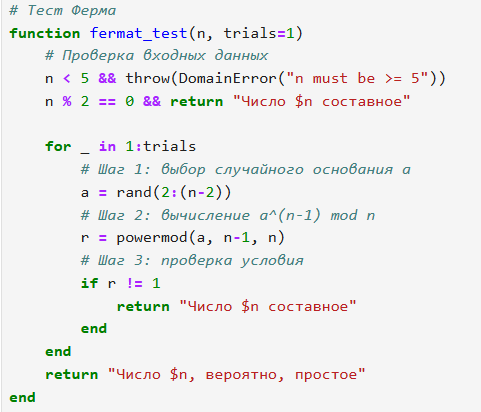


Рис. 3: Реализация алгоритма, реализующего тест Ферма

## 2.3 Реализация алгоритма, реализующего тест Соловэя-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.

Выполним реализацию этого алгоритма на языке Julia (рис. 4):

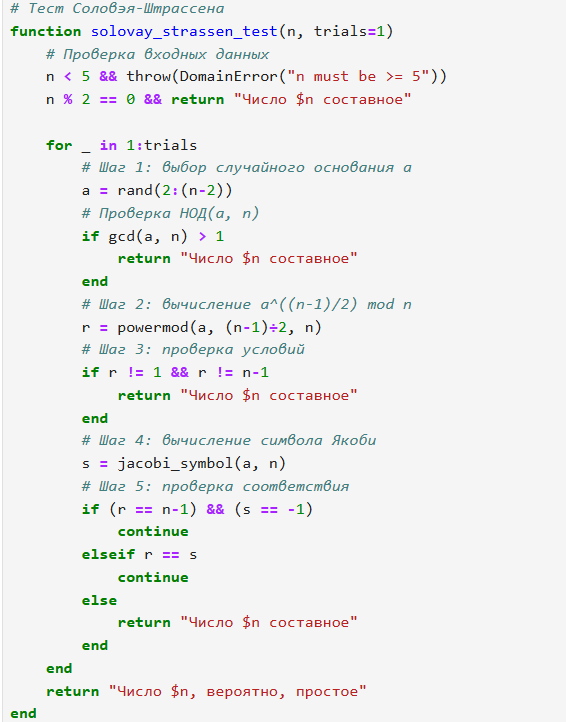


Рис. 4: Реализация алгоритма, реализующего тест Соловэя-Штрассена

## 2.4 Реализация алгоритма, реализующего тест Миллера-Рабина

Тест Миллера—Рабина — вероятностный полиномиальный тест простоты. Тест Миллера—Рабина, наряду с тестом Ферма и тестом Соловея—Штрассена, позволяет эффективно определить, 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.

Выполним реализацию этого алгоритма на языке Julia (рис. 5) и (рис. 6):

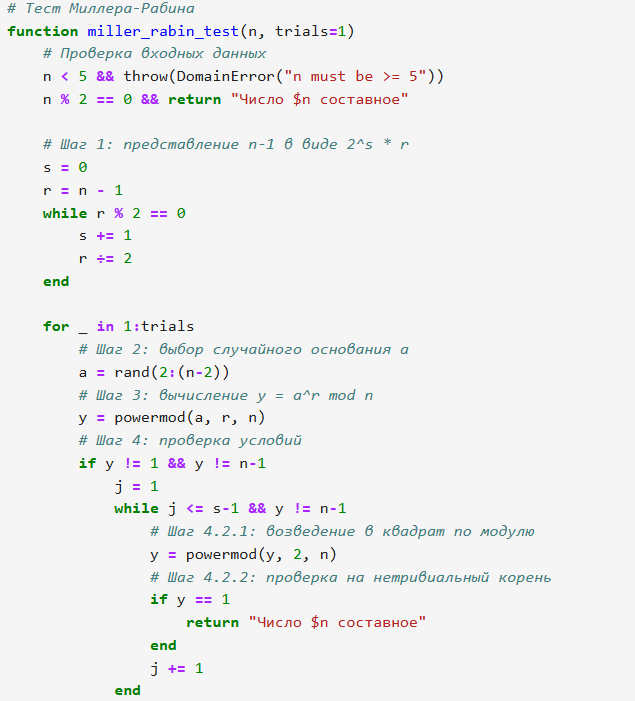


Рис. 5: Реализация алгоритма, реализующего тест Миллера-Рабина

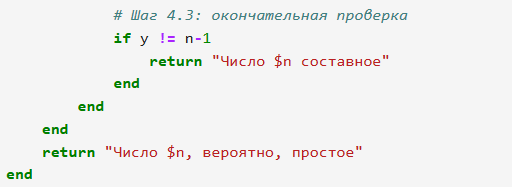


Рис. 6: Реализация алгоритма, реализующего тест Миллера-Рабина

Проверим работу алгоритмов (рис. 7):

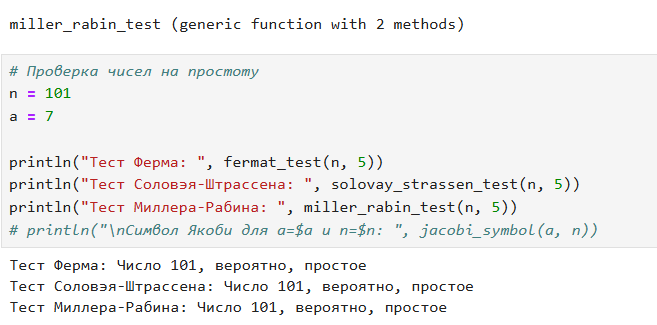


Рис. 7: Проверка

# 3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/