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

Вероятностные алгоритмы проверки чисел на простоту

Лубышева Ярослава Михайловна

Содержание

[1 Цель работы 1](#_Toc150631316)

[2 Задание 1](#_Toc150631317)

[3 Выполнение лабораторной работы 1](#_Toc150631318)

[4 Выводы 5](#_Toc150631319)

[5 Список литературы 5](#_Toc150631320)

# 1 Цель работы

Выполнить задание к лабораторной работе № 5 [1].

# 2 Задание

1. Ознакомиться с алгоритами проверки чисел на простоту: тест Ферма, тест Соловэя-Штрассена, тест Миллера-Рабина, также алгоритм вычисления символа Якоби.
2. Реализовать все алгоритмы программно.

# 3 Выполнение лабораторной работы

Для реализации алгоритмов вычисления наибольшего общего делителя была написана программа на языке программирования Python ([1](#fig:1) - [5](#fig:5)).

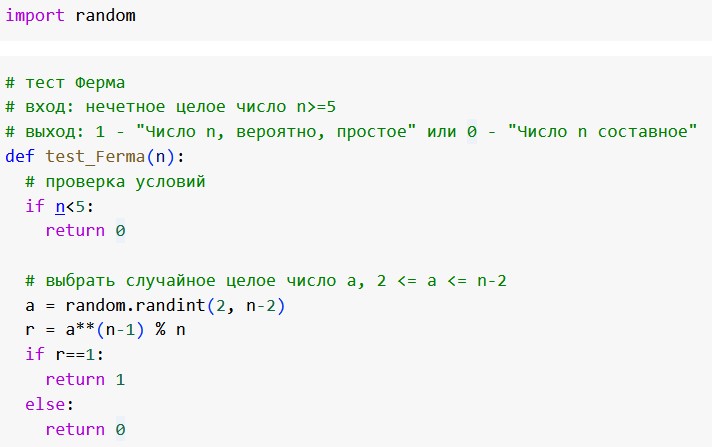


Figure 1: Программная реализация теста Ферма

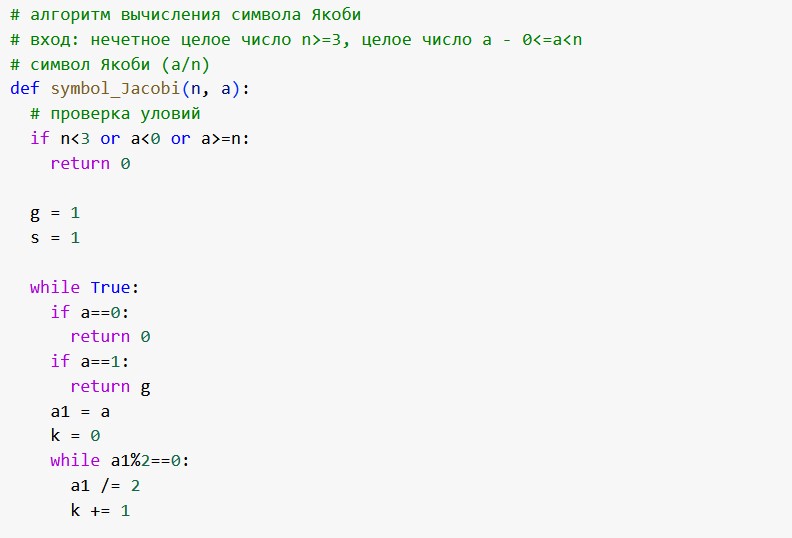


Figure 2: Программная реализация алгоритма вычисления символа Якоби (часть 1)

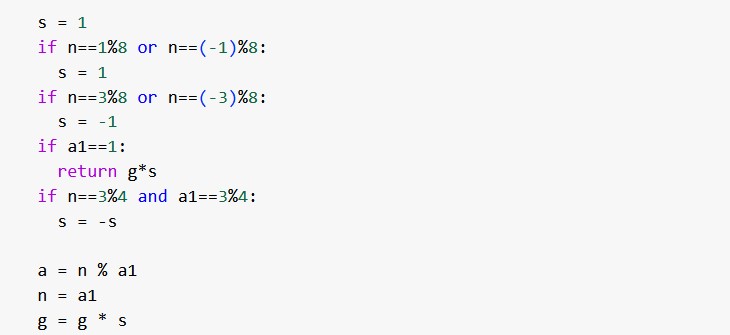


Figure 3: Программная реализация алгоритма вычисления символа Якоби (часть 2)

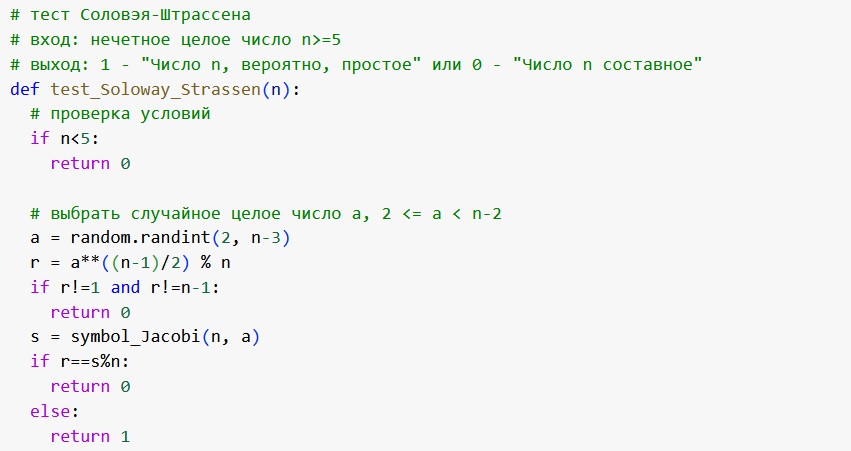


Figure 4: Программная реализация теста Соловэя-Штрассена

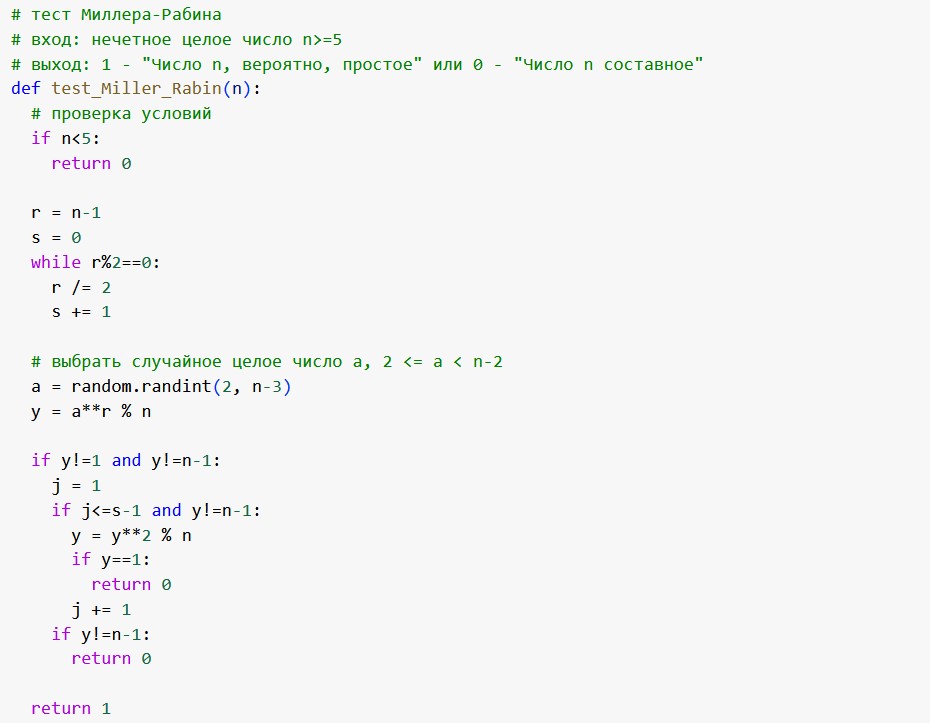


Figure 5: Программная реализация теста Миллера-Рабина

Результаты работы алгоритмов представлены на рисунке ниже ([6](#fig:6)).

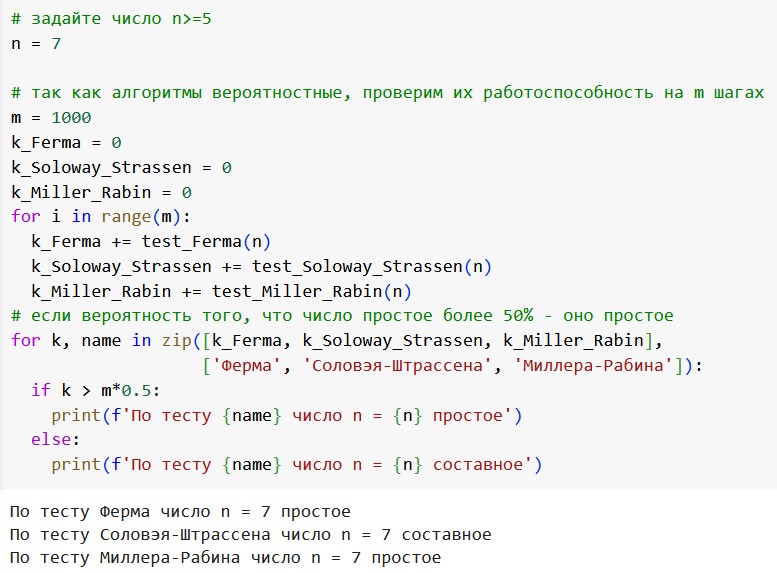


Figure 6: Результаты работы алгоритмов проверки чисел на простоту

# 4 Выводы

Выполнено задание к лабораторной работе № 5.

# 5 Список литературы

1. Методические материалы курса