Математические основы защиты информации и информационной безопасности.

Лабораторная работа №5.

Сапёров Максим Александрович.

Содержание

# 1 Цель работы

Освоить на практике вероятностные алгоримты проверки чисел на простоту

# 2 Задание

1. Реализовать алгоритм теста Ферма
2. Реализовать вычисления символа Якоби
3. Реализовать алгоритм теста Соловэя-Штрассена
4. Реализовать алгоритм теста Миллера-Рабина

# 3 Выполнение лабораторной работы

Написал код для вычисления теста Ферма. Все функции реализованы шаблонами:



Figure 1: Функция теста Ферма

Написал код для вычисления теста Соловэя-Штрассена.



Figure 2: Функция теста Соловэя-Штрассена

Реализовал вычисление теста Миллера-Рабина



Figure 3: тест Миллера-Рабина

Написал вспомогательную функцию вычисления символа Якоби

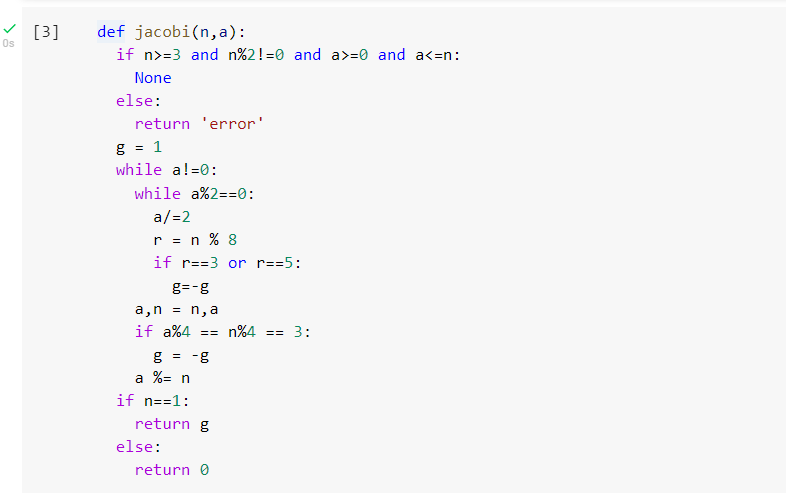


Figure 4: Вспомогательная функция вычисления символа Якоби

Результаты тестов.

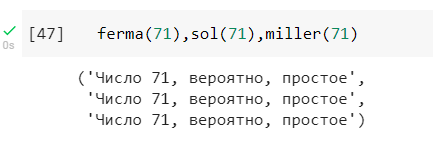


Figure 5: Результаты тестов

# 4 Выводы

Освоил на практике вероятностные алгоримты проверки чисел на простоту