Отчёт по лабораторной работе 5

Вероятностные алгоритмы проверки чисел на простоту

Гаджиев Нурсултан Тофик оглы НФИ-01-22

Содержание

# Цель работы

Реализация алгоритмов Ферма,Соловэя-Штрассена, Миллера-Рабина и вычисления Якоби.

# Теоретические сведения

Тестом простоты (или проверкой простоты) называется алгоритм, который, приняв на входе число N, позволяет либо не подтвердить предположение о составности числа, либо точно утверждать его простоту. Во втором случае он называется истинным тестом простоты. Таким образом, тест простоты представляет собой только гипотезу о том, что если алгоритм не подтвердил предположение о составности числа N, то это число может являться простым с определённой вероятностью. Это определение подразумевает меньшую уверенность в соответствии результата проверки истинному положению вещей, нежели истинное испытание на простоту, которое даёт математически подтверждённый результат[1].

## Тест Ферма

* Вход. Нечетное целое число .
* Выход. «Число n, вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число .
2. Вычислить
3. При результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное» [2].

## Тест Соловэя-Штрассена

* Вход. Нечетное целое число .
* Выход. «Число n, вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число .
2. Вычислить
3. При и результат: «Число n составное».
4. Вычислить символ Якоби
5. При результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное» [3].

## Тест Миллера-Рабина.

* Вход. Нечетное целое число .
* Выход. «Число n, вероятно, простое» или «Число n составное».

1. Представить в виде , где r - нечетное число
2. Выбрать случайное целое число .
3. Вычислить
4. При и выполнить действия
   * Положить
   * Если и то
     + Положить
     + При результат: «Число n составное».
     + Положить
   * При результат: «Число n составное».
5. Результат: «Число n, вероятно, простое» [4].

# Выполнение лабораторной работы

1. Написал функцию ferma для алгоритма ферма. (рис. 1)

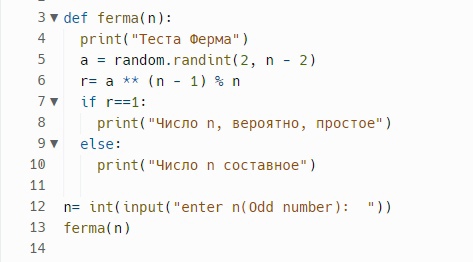


Figure 1: Функция для алгоритма ферма

1. Написал функцию modul для вычисления бинарного эксп. (рис. 2)

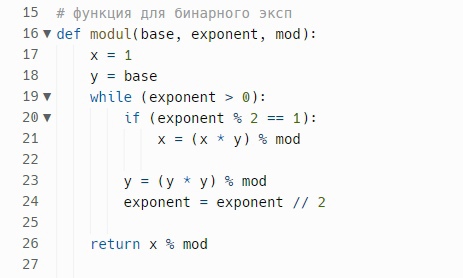


Figure 2: Функция для вычисления бинарного эксп

1. Написал функцию jacobian для вычисления Якоби. (рис. 3)

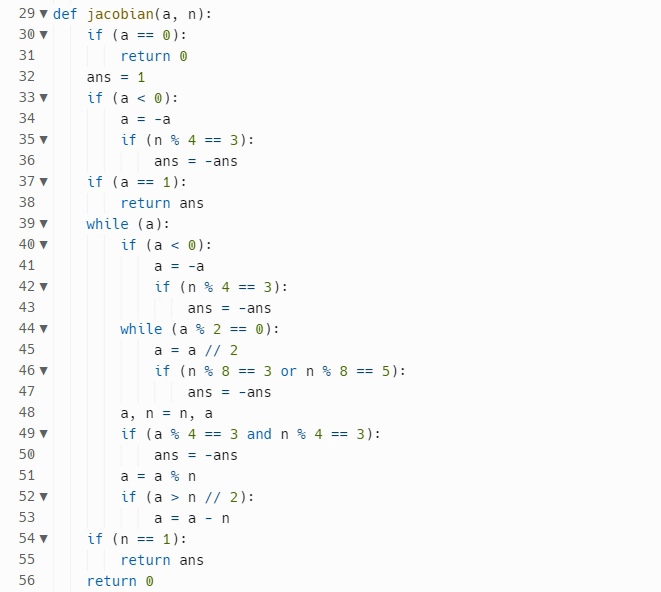


Figure 3: Функция для вычисления Якоби

1. Написал функцию solovoy для алгоритма Соловэя-Штрассена. (рис. 4)

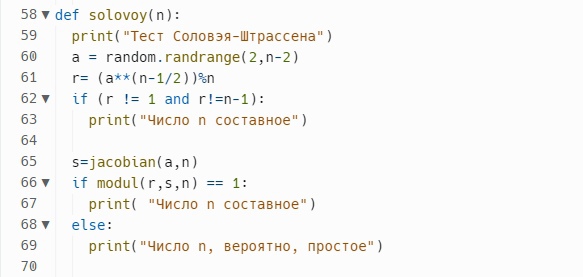


Figure 4: Функция для алгоритма Соловэя-Штрассена

1. Написал функцию MillerRabin для алгоритма Миллера-Рабина. (рис. 5)

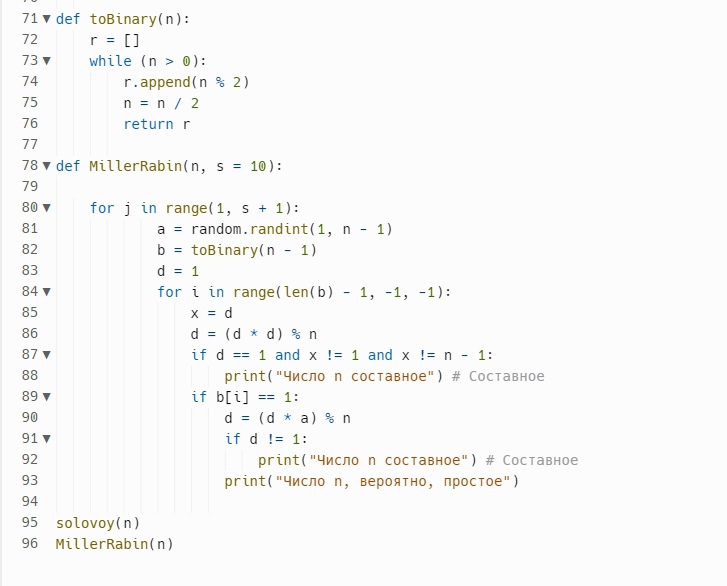


Figure 5: Функция для алгоритма Миллера-Рабина

1. Получил результат (рис. 6)

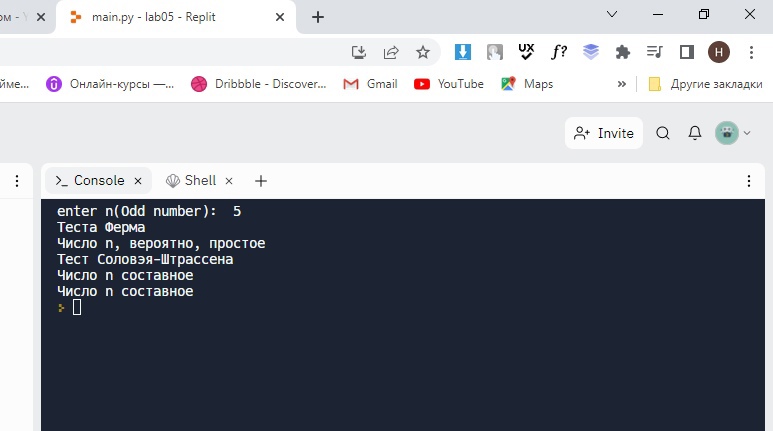


Figure 6: Результат алгоритмов

# Выводы

Реализовал алгоритмы Ферма,Соловэя-Штрассена, Миллера-Рабина и вычисления Якоби.

# Список литературы

1. Тест простоты [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Тест\_простоты
2. Тест Ферма [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Тест\_Ферма
3. Тест Соловея — Штрассена [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Тест\_Соловея\_—\_Штрассена
4. Тест Миллера — Рабина [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Тест\_Миллера\_—\_Рабина