Лабораторная работа №5. Вероятностные алгоритмы проверки чисел на простоту.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть и реализовать алгоритмы проверки чисел на простоту.

# 2 Задание

Реализовать следующие алгоритмы:

* Тест Ферма;
* Нахождение символа Якоби;
* Тест Соловэя-Штрассена;
* Тест Миллера-Рабина.

# 3 Теоретическое введение

Тест Ферма:

Теория: Основан на малой теореме Ферма, которая утверждает, что если p - простое число, то для любого целого a, не кратного p, справедливо . Если обратное также верно, то p - простое. Тест Ферма использует эту теорему, проверяя условие для случайно выбранных a.

Нахождение символа Якоби:

Теория: Символ Якоби обобщает символ Лежандра и предоставляет метод определения квадратичной вычетности для нечетных простых чисел. Символ Якоби для числа a и простого нечетного числа p определяется как произведение символов Лежандра для простых множителей a по модулю p. Используется для проверки квадратичной вычетности.

Тест Соловэя-Штрассена:

Теория: Основан на том, что простые числа обладают свойством квадратичной вычетности. Если n - простое, то для любого целого числа a существует квадратный корень по модулю n. Тест Соловэя-Штрассена проверяет это свойство для случайно выбранных a, используя символ Якоби.

Тест Миллера-Рабина:

Теория: Основан на том, что большинство составных чисел обладают свойством “псевдопростоты” по отношению к определенному базису. Тест Миллера-Рабина проверяет это свойство для случайно выбранных базисов. Если число n не проходит тест, то оно с большой вероятностью составное.

Эти тесты предоставляют методы проверки простоты чисел, но важно отметить, что они не гарантируют абсолютную простоту и могут давать ошибочные результаты. В практике их часто комбинируют или применяют с дополнительными проверками для повышения надежности.

# 4 Выполнение лабораторной работы

## 4.1 Тест Ферма

### 4.1.1 Задача

Реализовать тест Ферма

#### 4.1.1.1 Решение

Реализуем тест Ферма (рис. [1](#fig:001))

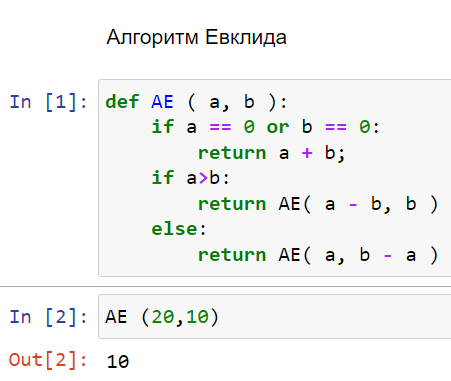


Figure 1: Тест Ферма

## 4.2 Нахождение символа Якоби

### 4.2.1 Задача

Реализовать алгоритм нахождения символа Якоби

#### 4.2.1.1 Решение

Найдём символ Якоби (рис. [2](#fig:002))



Figure 2: Символ Якоби

## 4.3 Тест Соловэя-Штрассена

### 4.3.1 Задача

Реализовать тест Соловэя-Штрассена

### 4.3.2 Решение

Реализуем тест Соловэя-Штрассена (рис. [3](#fig:003))

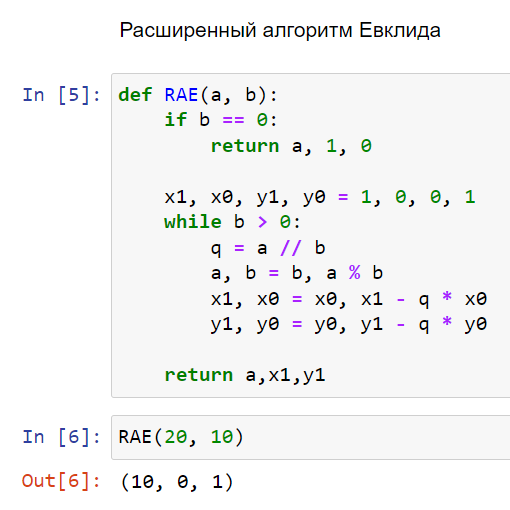


Figure 3: Тест Соловэя-Штрассена

## 4.4 Тест Соловэя-Штрассена

### 4.4.1 Задача

Реализовать тест Соловэя-Штрассена

### 4.4.2 Решение

Реализуем тест Соловэя-Штрассена (рис. [4](#fig:004))

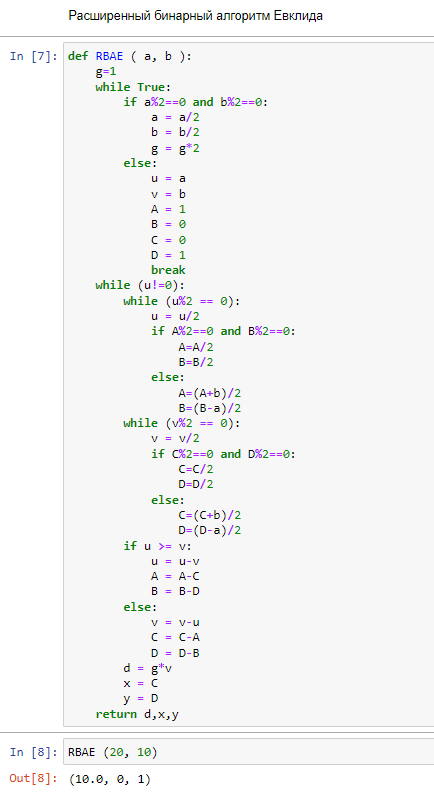


Figure 4: Тест Соловэя-Штрассена

# 5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал следующие алгоритмы:

* Тест Ферма;
* Нахождение символа Якоби;
* Тест Соловэя-Штрассена;
* Тест Миллера-Рабина.

# 6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: [Python documentation](https://docs.python.org/3/index.html) (Дата обращения: 28.09.2023).
2. Лабораторная работа №5. Вероятностные алгоритмы проверки чисел на простоту. - 5 с. [Электронный ресурс]. М. URL: [Лабораторная работа №5. Вероятностные алгоритмы проверки чисел на простоту.](https://esystem.rudn.ru/pluginfile.php/2089811/mod_folder/content/0/lab05.pdf) (Дата обращения: 10.11.2023).