Лабораторная работа №5: отчет.

вероятностные алгоритмы проверки чисел на простоту

Евдокимов Максим Михайлович. Группа - НФИмд-01-24.

Содержание

# Цели и задачи работы

## Цель лабораторной работы

Вероятностные алгоритмы проверки чисел на простоту

## Задание

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

# Теоретическое введение

## Тест Ферма

Тест Ферма основан на малой теореме Ферма, которая утверждает, что если n — простое число, то для любого целого такого, что , выполняется:

### Алгоритм действий:

1. Выбрать случайное число такое, что .
2. Вычислить .
3. Если , то — составное.
4. Если $, то вероятно простое.

### Сравнение:

* **Плюсы:** Простой и быстрый.
* **Минусы:** Подвержен “числам Кармайкла” составным числам, которые проходят тест для всех .

## Символ Якоби

**Символ Якоби** — это обобщение символа Лежандра на случай, когда знаменатель является нечетным составным числом. Символ Якоби определяется для целого числа и нечетного натурального числа .

Если — простое число, то символ Якоби совпадает с символом Лежандра. Символ Лежандра определяется для целого числа и простого числа и указывает, является ли квадратичным вычетом по модулю .

### Свойства символа Якоби

1. **Мультипликативность:**
2. **Симметрия:**
3. **Квадратичный закон взаимности:**

* Для нечетных натуральных чисел и :

1. **Свойства для и :**

## Тест Соловея-Штрассена

Тест Соловея-Штрассена использует символ Якоби и малую теорему Ферма для определения вероятности простоты числа.

### Алгоритм действий:

1. Выбрать случайное число такое, что .
2. Вычислить символ Якоби .
3. Вычислить .
4. Если , то — составное.
5. Если , то вероятно простое.

### Сравнение:

* **Плюсы:** Более надежный, чем тест Ферма, так как не подвержен “числам Кармайкла”.
* **Минусы:** Требует вычисления символа Якоби, что может быть сложнее.

## Тест Миллера-Рабина

Тест Миллера-Рабина — это вероятностный тест, основанный на расширении малой теоремы Ферма и использующий свойства квадратичных вычетов.

### Алгоритм действий:

1. Представить как , где — нечетное.
2. Выбрать случайное число такое, что .
3. Вычислить .
4. Если или , то вероятно простое.
5. Иначе, вычислить для .
6. Если для какого-то выполняется , то вероятно простое.
7. Если ни одно из условий не выполняется, то — составное.

### Сравнение:

* **Плюсы:** Один из самых надежных вероятностных тестов, не подвержен “числам Кармайкла”.
* **Минусы:** Требует больше вычислений, чем тест Ферма.

## Вывод:

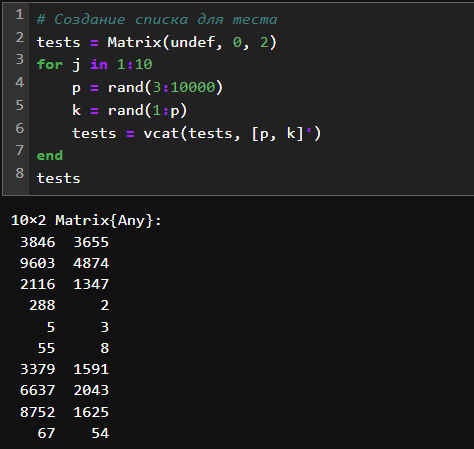
* **Тест Ферма** — простой, но подвержен “числам Кармайкла”.
* **Тест Соловея-Штрассена** — более надежный, чем Ферма, но требует вычисления символа Якоби.
* **Тест Миллера-Рабина** — самый надежный из трех, но требует больше вычислений.

Каждый из этих тестов дает вероятностный результат, и для подтверждения простоты числа обычно используют несколько итераций теста.

# Ход работы

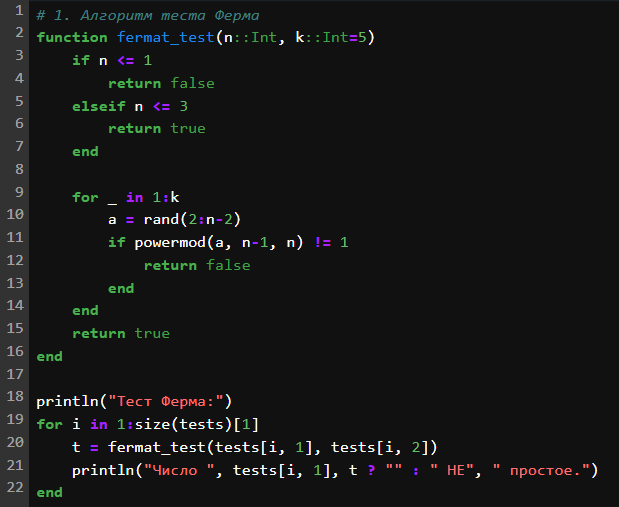
## Подготовка

Так для тестирования работы кода я создал простой шаблон генерирующий наше случайное число для проверки, а также необходимые для каждого алгоритма коэффициент или параметр который гарантированно меньше исходного, но не меньше 1.



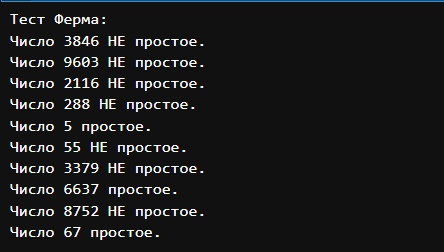
Случайная тестовая группа

## Алгоритм теста Ферма



Код теста Ферма

## Результат 1



Результат шифра Цезаря

## Алгоритм вычисления символа Якоби

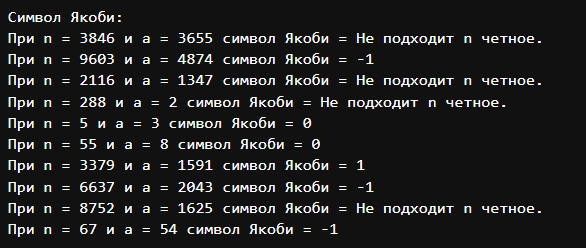
Если посмотреть на полученный результаты может показаться что при данных значениях нет ни одного число которое при использовании теста Соловэя-Штрассена. Для проверки рассмотрим случай номер 5 при значениях n = 5 (число для проверки) и a = 3 (случайное число) оба при этом оказались простыми.

1. Начнём с символа Якоби: 3/5; 5 - простое и совпадает с символом Лежандра который вычисляем как 5/3 => 2/3 а, так как 2 = mod(3) и не является квадратом по модулю 3 то 2/3 = -1 => 3/5 => -1
2. Теперь вычислим => =>
3. Сравним: -1 и 4 не ровны значит чисто по тесту Соловея-Штрассена при a = 3 и n = 5, n не простое. При других значениях возможно он даст правильный ответ, но не здесь.



Код вычисления символа Якоби

## Результат 2



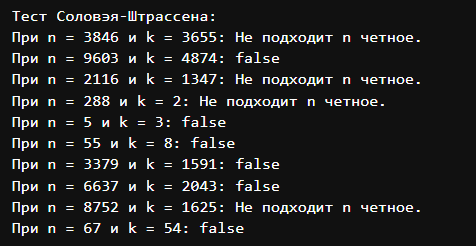
Результат вычисления символа Якоби

## Алгоритм теста Соловэя-Штрассена



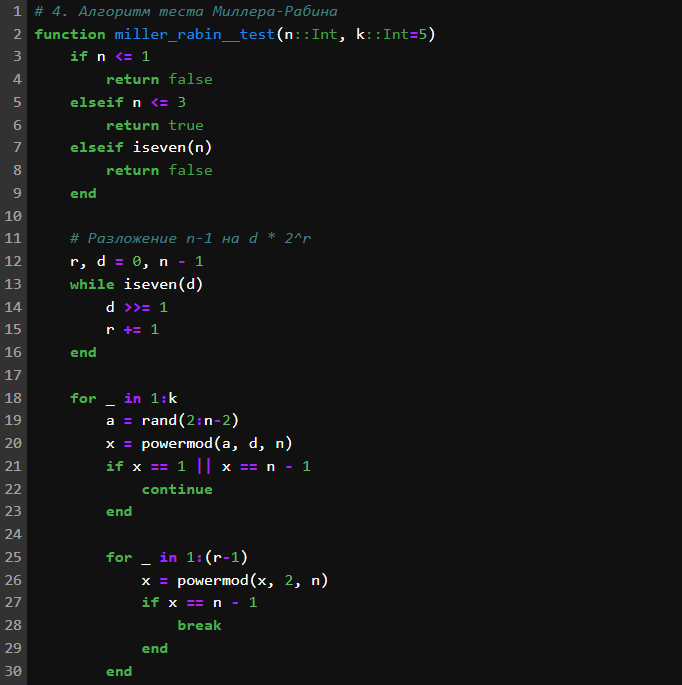
Код теста Соловэя-Штрассена

## Результат 3

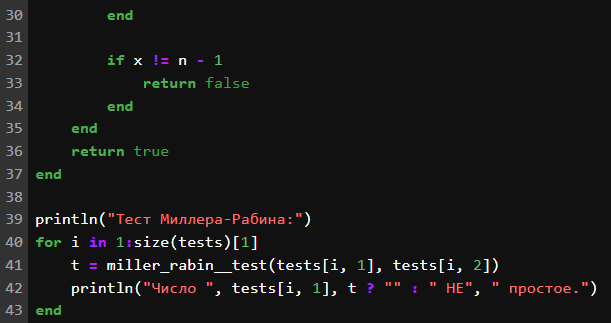


Результат теста Соловэя-Штрассена

## Алгоритм теста Миллера-Рабина

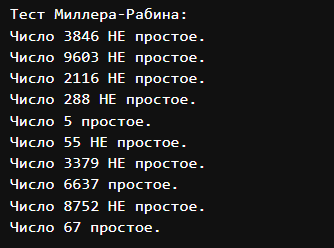


Код теста Миллера-Рабина 1



Код теста Миллера-Рабина 2

## Результат 4



Результат теста Миллера-Рабина

# Выводы по проделанной работе

## Вывод

В ходе выполнения лабораторной работе выли изучены такие способы определение простоты числа как алгоритм теста Ферма, алгоритм теста Миллера-Рабина и алгоритм теста Соловэя-Штрассена, и алгоритм вычисления символа Якоби.

# Список литературы

1. [Свойства символа Якоби и Тест на простоту Соловея-Штрассена](https://studfile.net/preview/6268704/page:17/)
2. [Метод Соловея -Штрассена для проверки на простоту](https://www.geeksforgeeks.org/solovay-strassen-method-of-primality-test/)
3. [Primality Test | Set 3 (Miller–Rabin)](https://www.geeksforgeeks.org/primality-test-set-3-miller-rabin/)
4. [Тесты Ферма и Миллера-Рабина на простоту](https://habr.com/ru/companies/otus/articles/486116/)
5. [Алгоритм Соловея-Штрассена](https://habr.com/ru/articles/127544/)