Отчёт по лабораторной работе №5.  
Вероятностные алгоритмы проверки чисел на простоту

Студент: Лапшенкова Любовь Олеговна, 10322127633

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

[1 Цель работы 1](#_Toc90072351)

[2 Задание 2](#_Toc90072352)

[3 Теоретическое введение 2](#_Toc90072353)

[3.1 Тест Ферма 2](#_Toc90072354)

[3.2 Символ Якоби 3](#_Toc90072355)

[3.3 Тест Соловэя-Штрассена 3](#_Toc90072356)

[3.4 Тест Миллера-Рабина 4](#_Toc90072357)

[4 Выполнение лабораторной работы 5](#_Toc90072358)

[4.1 Тест Ферма 5](#_Toc90072359)

[4.2 Символ Якоби 6](#_Toc90072360)

[4.3 Тест Соловэя-Штрассена 8](#_Toc90072361)

[4.4 Тест Миллера-Рабина 9](#_Toc90072362)

[5 Выводы 9](#_Toc90072363)

[Список литературы 9](#_Toc90072364)

# 1 Цель работы

Целью данной лабораторной работы является ознакомление с вероятностными алгоритмами проверки чисел на простоту и программная реализация данных алгоритмов.

# 2 Задание

Реализовать все рассмотренные в инструкции к лабораторной работе алгоритмы проверки чисел на простоту программно.

# 3 Теоретическое введение

## 3.1 Тест Ферма

Тест простоты Ферма в теории чисел — это тест простоты натурального числа n, основанный на малой теореме Ферма[1].

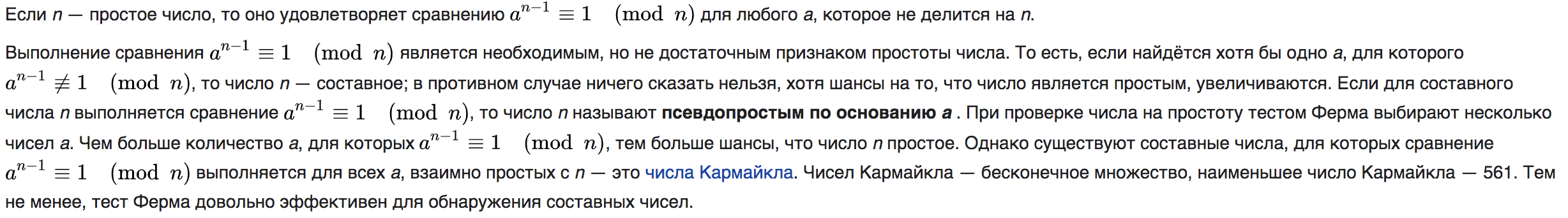


Figure 1: Основная информация по тесту Ферма

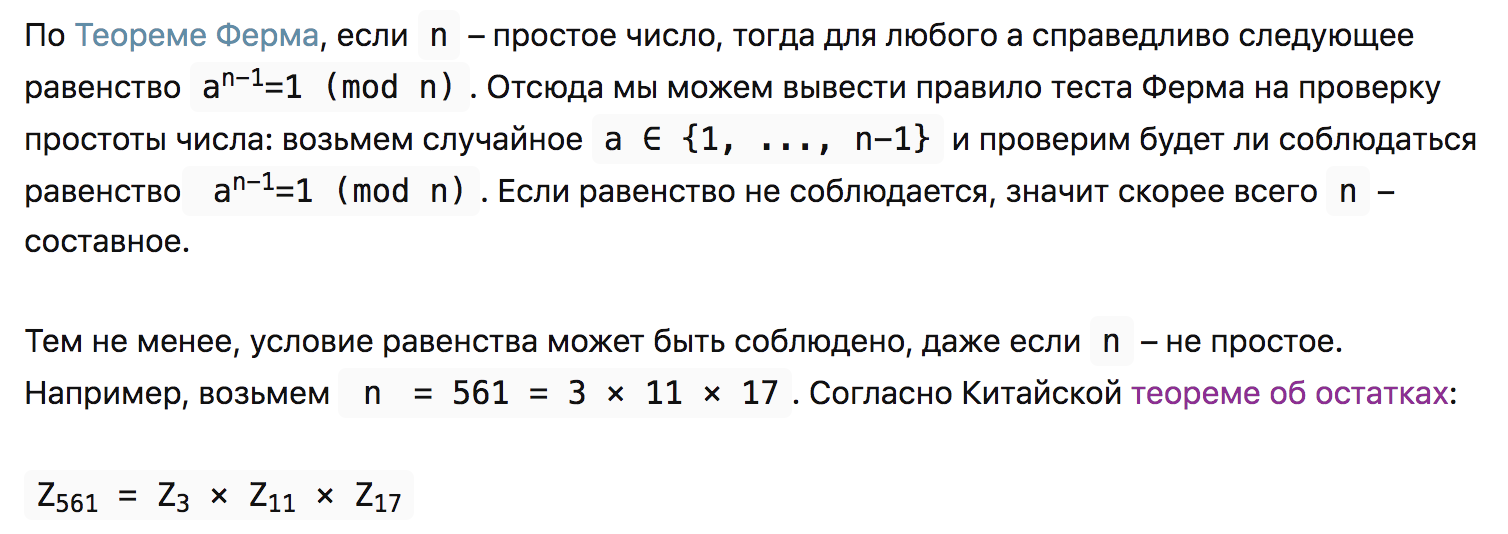


Figure 2: Численный пример по тесту Ферма. Часть 1

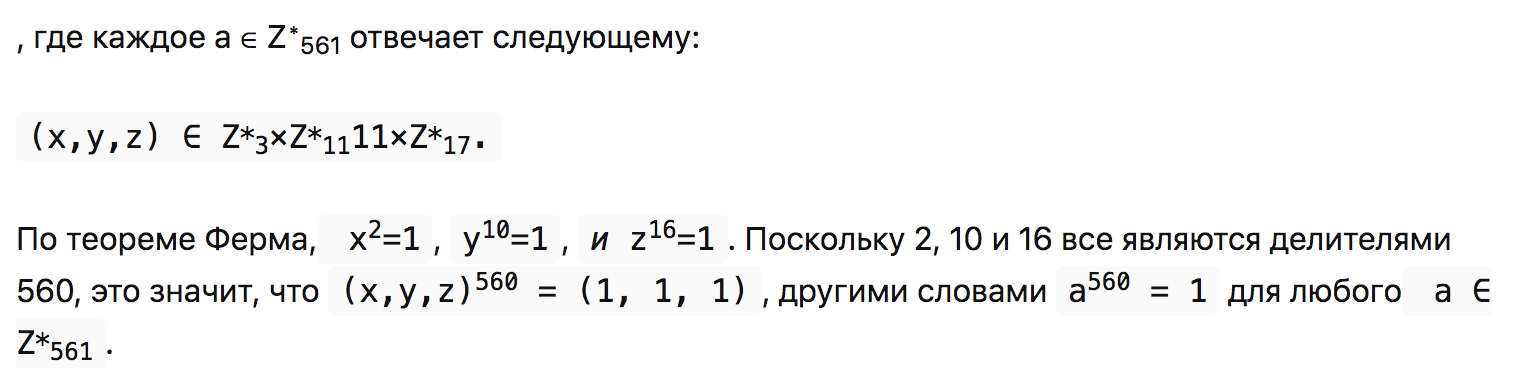


Figure 3: Численный пример по тесту Ферма. Часть 2

Не имеет значения какое a мы выберем, 561 всегда будет проходить тест Ферма несмотря на то, что оно составное, до тех пор, пока a является взаимно простым с n. Такие числа называются числами Кармайкла и оказывается, что их существует бесконечное множество.

Если a не взаимно простое с n, то оно тест Ферма не проходит, но в этом случае мы можем отказаться от тестов и продолжить искать делители n, вычисляя НОД(a,n)[2].

## 3.2 Символ Якоби

Символ Якоби — теоретико-числовая функция двух аргументов, введённая К. Якоби в 1837 году. Является квадратичным характером в кольце вычетов.

Символ Якоби обобщает символ Лежандра на все нечётные числа, большие единицы. Символ Кронекера — Якоби, в свою очередь, обобщает символ Якоби на все целые числа, но в практических задачах символ Якоби играет гораздо более важную роль, чем символ Кронекера — Якоби[3].

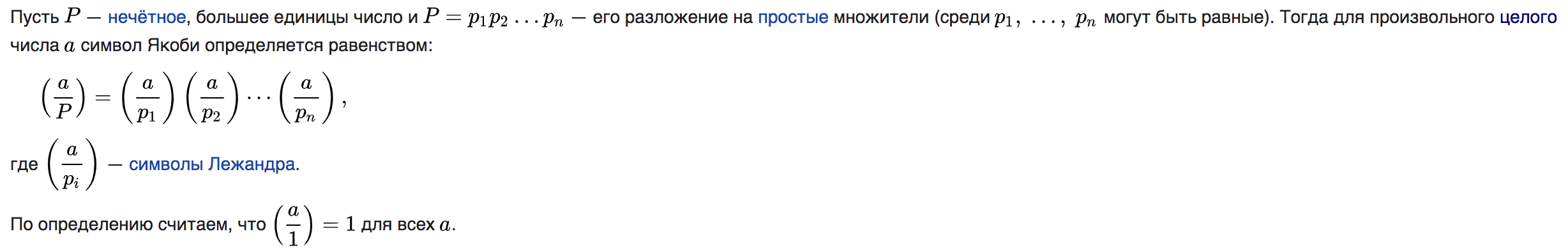


Figure 4: Определение символа Якоби

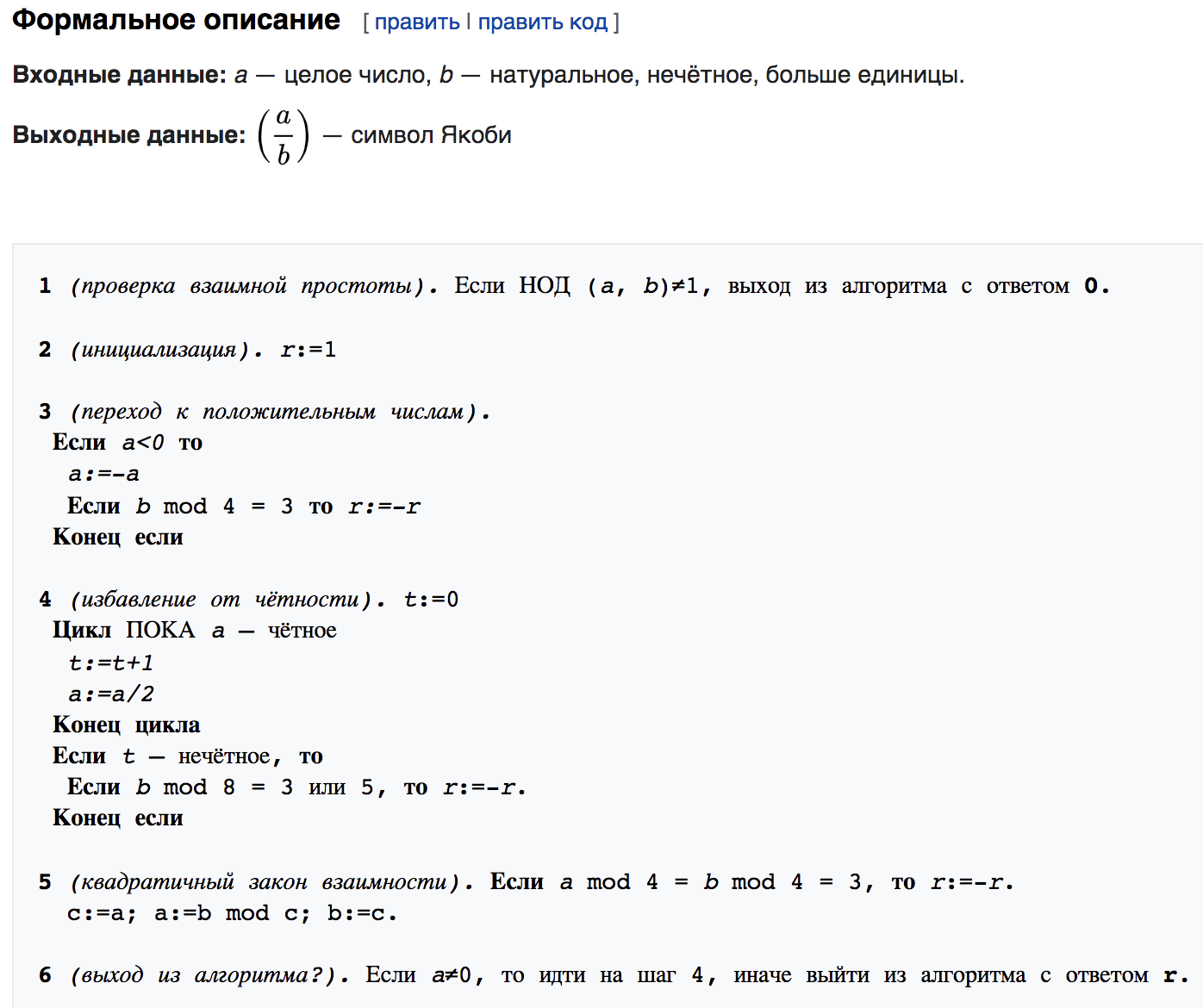


Figure 5: Алгоритм нахождения символа Якоби

## 3.3 Тест Соловэя-Штрассена

Роберт Соловей и Фолькер Штрассен разработали алгоритм вероятностного тестирования простоты числа, который использует символ Якоби. Определяет числа как составные или вероятно простые. Распознает числа Кармайкла как составные. Итак, для начала необходимо ввести нужные понятия[4].

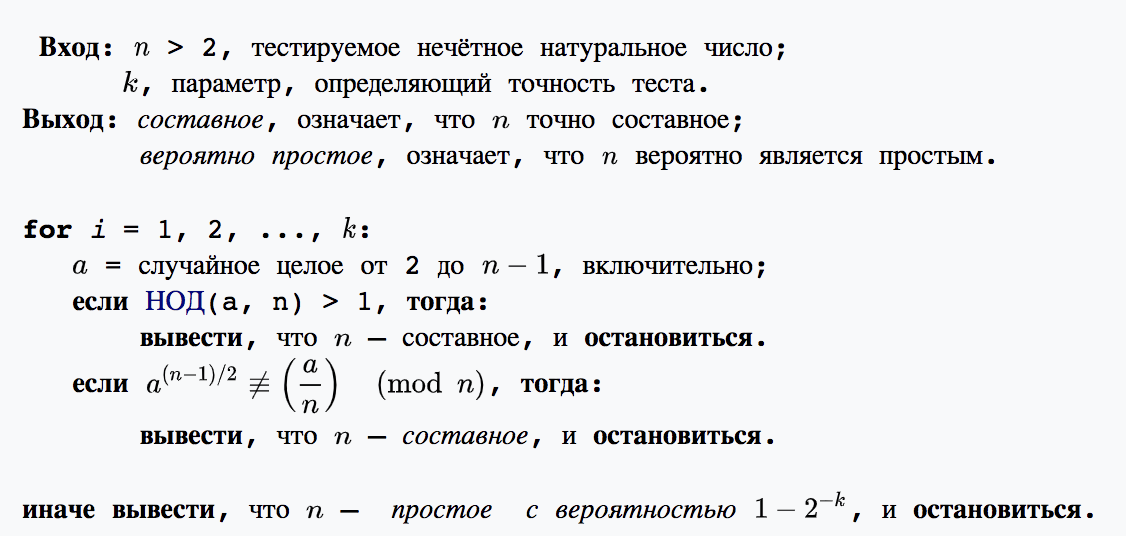


Figure 6: Алгоритм Cоловэя-Штрассена

Вероятностные тесты применяются в системах основанных на проблеме факторизации, например RSA или схема Рабина. Однако на практике степень достоверности теста Соловея — Штрассена не является достаточной, вместо него используется тест Миллера — Рабина. Более того, используются объединенные алгоритмы, например пробное деление и тест Миллера — Рабина, при правильном выборе параметров можно получить результаты лучше, чем при применении каждого теста по отдельности[5].

## 3.4 Тест Миллера-Рабина

Тест Миллера — Рабина — вероятностный полиномиальный тест простоты. Тест Миллера — Рабина, наряду с тестом Ферма и тестом Соловея — Штрассена, позволяет эффективно определить, является ли данное число составным. Однако, с его помощью нельзя строго доказать простоту числа. Тем не менее тест Миллера — Рабина часто используется в криптографии для получения больших случайных простых чисел[6].

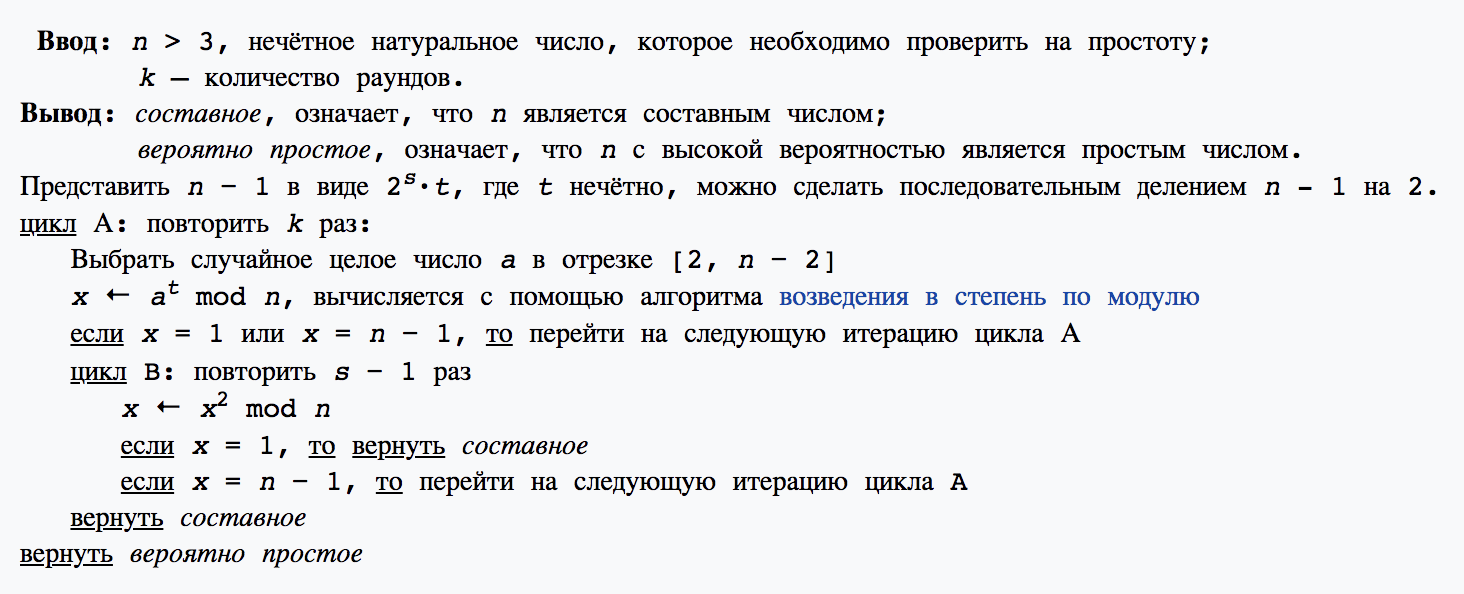


Figure 7: Алгоритм Миллера-Рабина

# 4 Выполнение лабораторной работы

**Примечание:** комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

В соответствии с заданием, были написаны программы реализации алгоритмов проверки чисел на простоту. Нами были рассмотрены следующие алгоритмы:

1. Тест Ферма;
2. Символ Якоби;
3. Тест Соловэя-Штрассена;
4. Тест Миллера-Рабина.

Программный код и результаты выполнения программ представлен ниже.

## 4.1 Тест Ферма

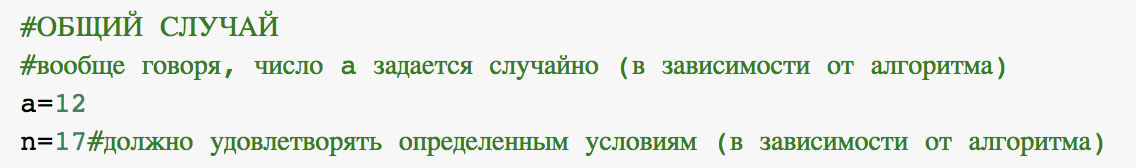


Figure 8: Входные данные для реализации алгоритмов проверки чисел на простоту

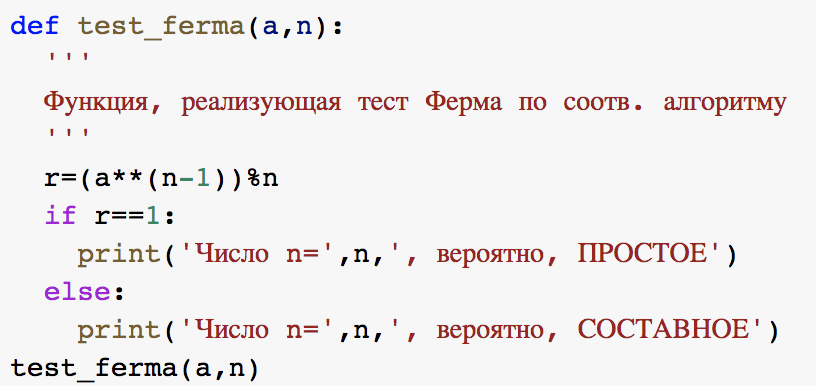


Figure 9: Реализация алгоритма теста Ферма

Результаты выполнения программы представлены ниже (см. рис. 10).

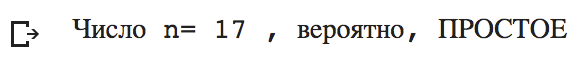


Figure 10: Результат реализации алгоритма теста Ферма

## 4.2 Символ Якоби

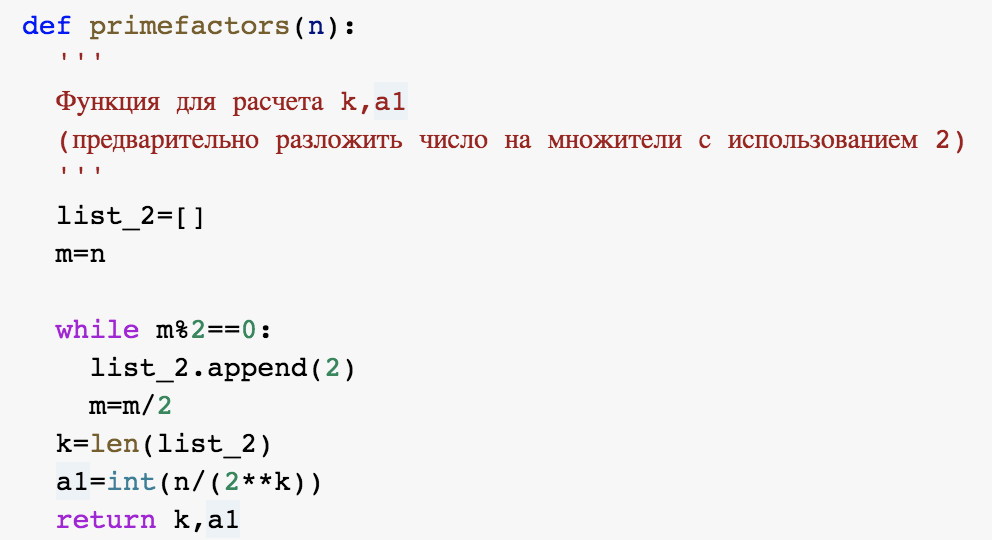


Figure 11: Реализация алгоритма вычисления символа Якоби 1 часть

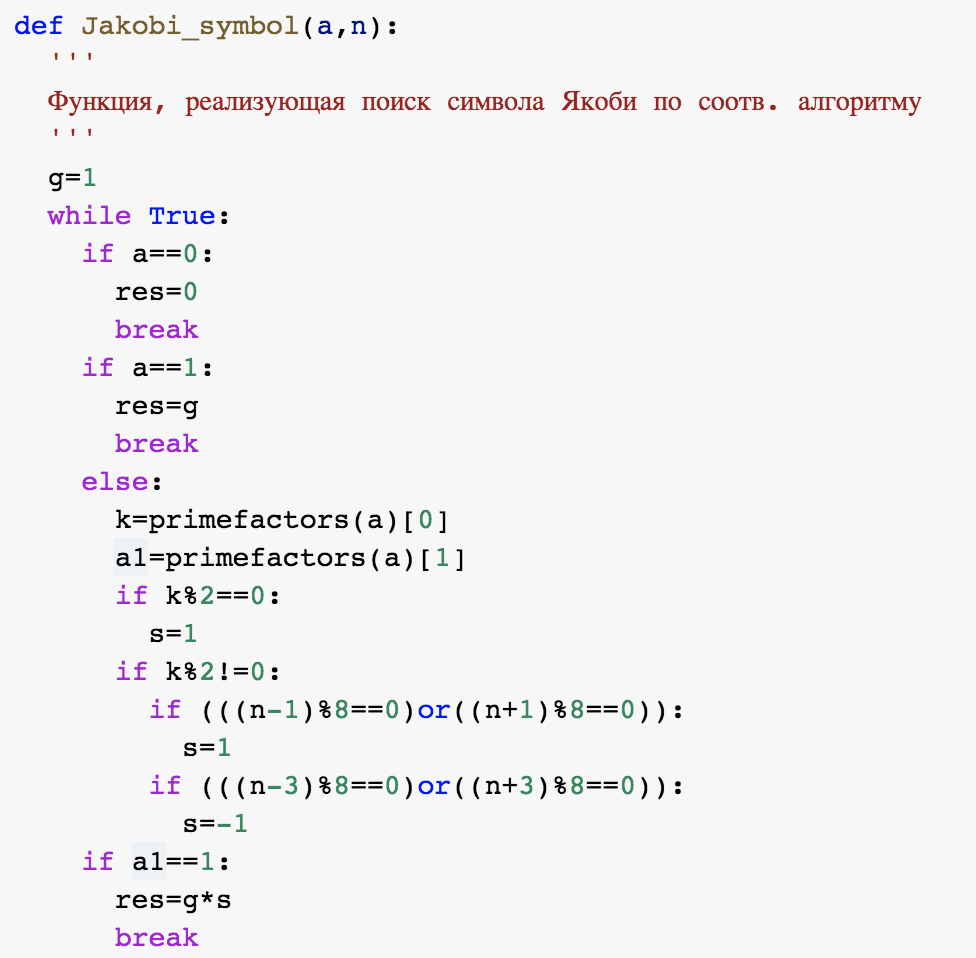


Figure 12: Реализация алгоритма вычисления символа Якоби 2 часть

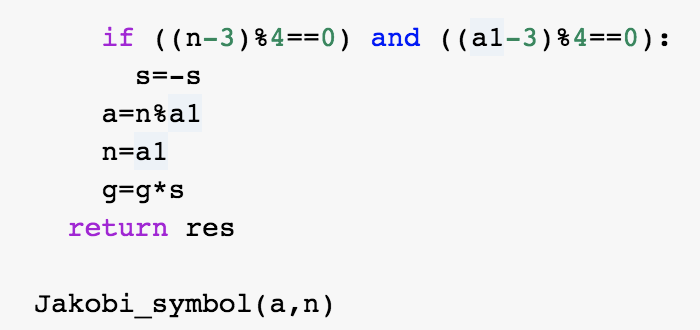


Figure 13: Реализация алгоритма вычисления символа Якоби 3 часть

Результаты выполнения программы представлены ниже (см. рис. 14).

Figure 14: Результат реализации алгоритма вычисления символа Якоби

Figure 14: Результат реализации алгоритма вычисления символа Якоби

## 4.3 Тест Соловэя-Штрассена



Figure 15: Реализация алгоритма теста Соловэя-Штрассена

Результаты выполнения программы представлены ниже (см. рис. 16).

Figure 16: Результат реализации алгоритма теста Соловэя-Штрассена

Figure 16: Результат реализации алгоритма теста Соловэя-Штрассена

## 4.4 Тест Миллера-Рабина

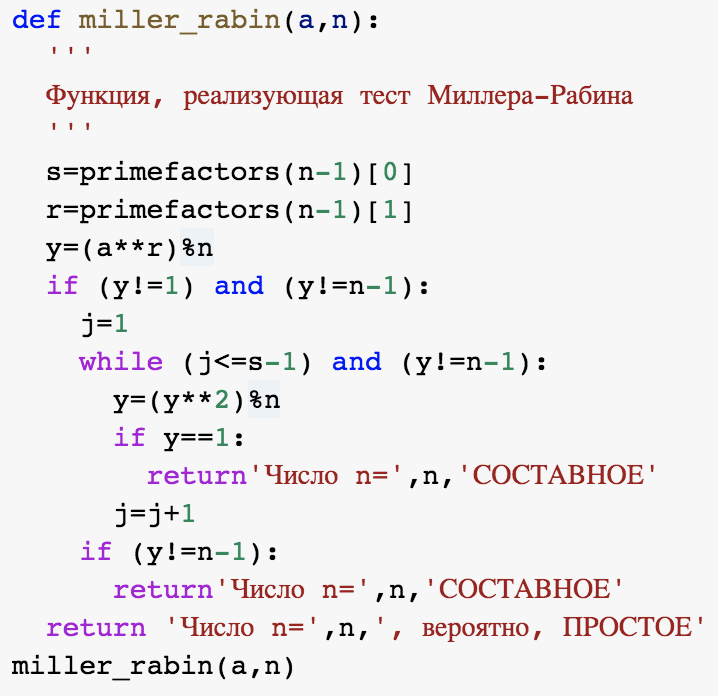


Figure 17: Реализация алгоритма теста Миллера-Рабина

Результаты выполнения программы представлены ниже (см. рис. 18).

Figure 18: Результат реализации алгоритма теста Миллера-Рабина

Figure 18: Результат реализации алгоритма теста Миллера-Рабина

# 5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с алгоритмами проверки чисел на простоту, – а так же реализовала данные алгоритмы на языке программирования Python 3.

# Список литературы

1. Википедия. Тест Ферма [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0> (дата обращения: 10.12.2021).

2. MaxRokatansky. Тесты Ферма и Миллера-Рабина на простоту [Электронный ресурс]. Хабр, 2020. URL: <https://habr.com/ru/company/otus/blog/486116/> (дата обращения: 10.12.2021).

3. Википедия. Символ Якоби [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%B2%D0%BE%D0%BB_%D0%AF%D0%BA%D0%BE%D0%B1%D0%B8> (дата обращения: 10.12.2021).

4. UsmiMashka. Алгоритм Соловея-Штрассена [Электронный ресурс]. Хабр, 2011. URL: <https://habr.com/ru/company/otus/blog/486116/> (дата обращения: 10.12.2021).

5. Википедия. Тест Соловея — Штрассена [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Solovay%E2%80%93Strassen_primality_test> (дата обращения: 10.12.2021).

6. Википедия. Тест Миллера — Рабина [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test> (дата обращения: 10.12.2021).