Лабораторная работа №5

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования вероятностные алгоритмы проверки чисел на простоту.

# 2 Теоретическое введение

Пусть - целое число. Числа , называются **тривиальными делителями** числа .

Целое число называется **простым**, если оно не является делителем единицы и не имеет других делителей, кроме тривиальных. В противном случае число называется **составным**.

Алгоритмы проверки на простоту можно разделить на вероятностные и детерминированные.

**Детерминированный** алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа). **Вероятностный** алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ. Вероятностные алгоритмы в общем случае не менее эффективны, чем детерминированные (если используемый генератор случайных чисел всегда дает набор одних и тех же чисел, зависящих от входных данных, то вероятностный алгоритм становится детерминированным).

Для проверки на простоту числа вероятностным алгоритмом выбирают случайное число и проверяют условия алгоритма. Если число не проходит тест по основанию , то алгоритм выдает результат “Число составное”, и число действительно является составным.

Если же проходит тест по основанию , ничего нельзя сказать о том, действительно ли число является простым. Последовательно проведя ряд проверок таким тестом для разных и получив для каждого из них ответ “Число , вероятно, простое”, можно утверждать, что число является простым с вероятностью, близкой к 1. При независимых выполнений теста вероятность того, что составное число будет раз объявлено простым (вероятность ошибки), не превосходит .

Более подробно см. в [1], [2], [3], [4].

# 3 Выполнение лабораторной работы

Тест Ферма реализуем по следующей схеме:

На вход подается нечетное целое число .

1. Выбрать случайное целое число .
2. Вычислить .
3. При результат: “Число , вероятно, простое”. В противном случае результат: “Число составное”.

Код программы (рис. 1).

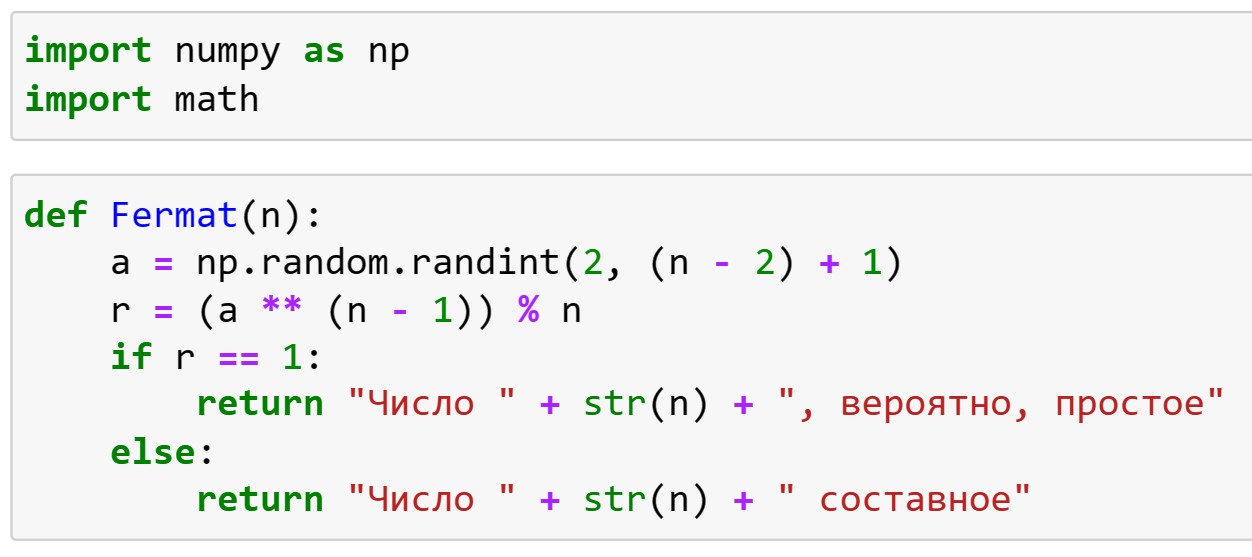


Рис. 1: Тест Ферма

Вычисление символа Якоби реализуем по следующей схеме:

На вход подаются нечетное целое число и целое число , .

1. Положить .
2. При результат .
3. При результат .
4. Представить в виде , где число нечетное.
5. При четном положить , при нечетном положить , если ; положить , если .
6. При результат: .
7. Если и , то .
8. Положить и вернуться на шаг 2.

Код программы (рис. 2).

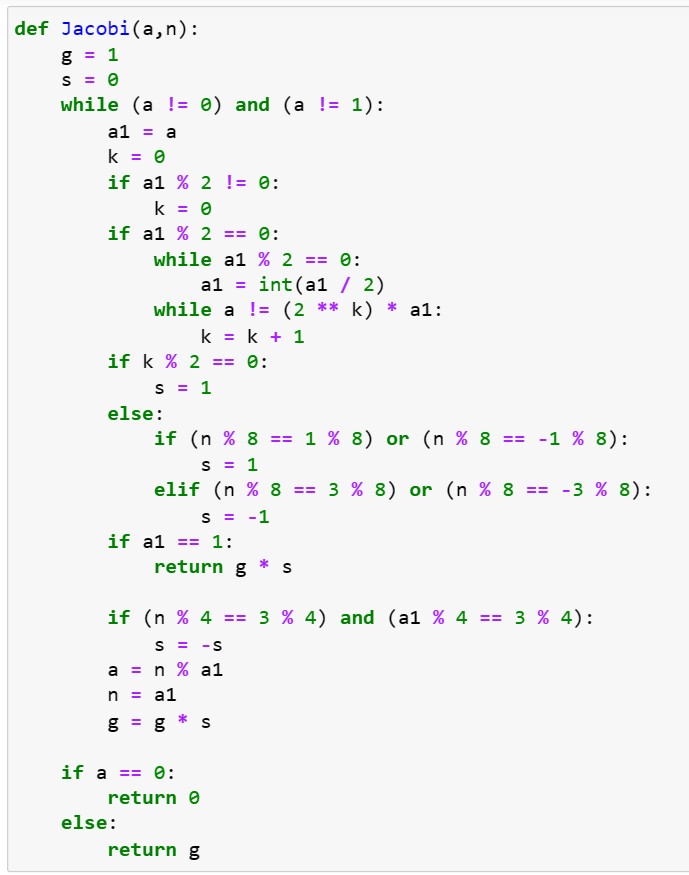


Рис. 2: Вычисление символа Якоби

Тест Соловэя-Штрассена реализуем по следующей схеме:

На вход подается нечетное целое число .

1. Выбрать случайное целое число .
2. Вычислить .
3. При и результат: “Число составное”.
4. Вычислить символ Якоби .
5. При результат: “Число составное”. В противном случае результат: “Число , вероятно, простое”.

Код программы (рис. 3).

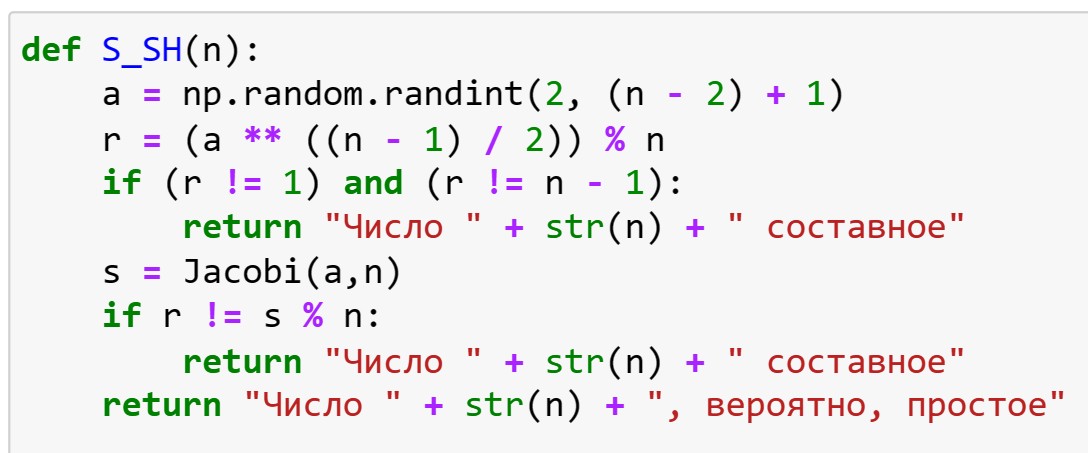


Рис. 3: Тест Соловэя-Штрассена

Тест Миллера-Рабина реализуем по следующей схеме:

На вход подается нечетное целое число .

1. Представить в виде , где число нечетное.
2. Выбрать случайное целое число .
3. Вычислить .
4. При и выполнить следующие действия.

4.1. Положить .

4.2. Если и , то

4.2.1. Положить .

4.2.2. При результат: “Число составное”.

4.2.3. Положить .

4.3. При результат: “Число составное”.

1. Результат: “Число , вероятно, простое”.

Код программы (рис. 4).

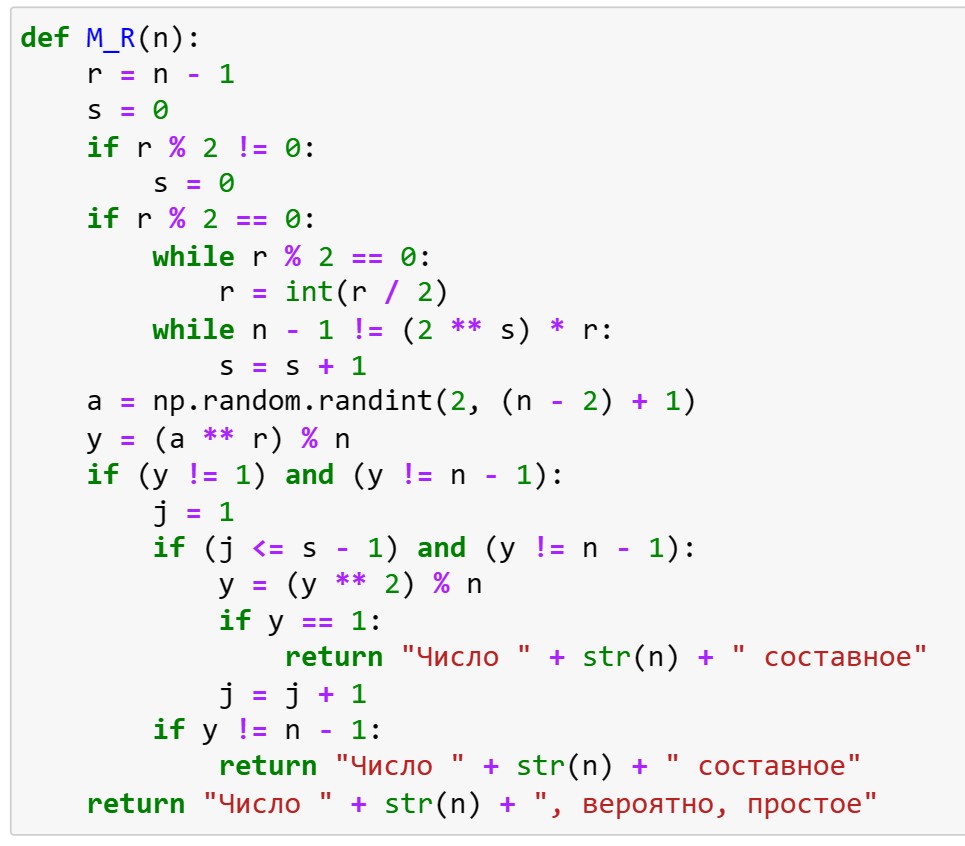


Рис. 4: Тест Миллера-Рабина

В итоге были получены следующие результаты (рис. 5) - (рис. 8).

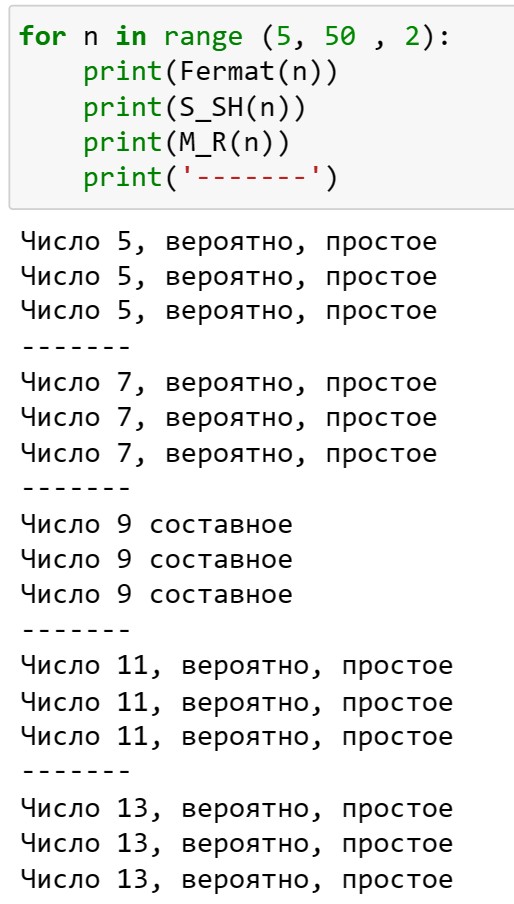


Рис. 5: Результаты выполнения алгоритмов

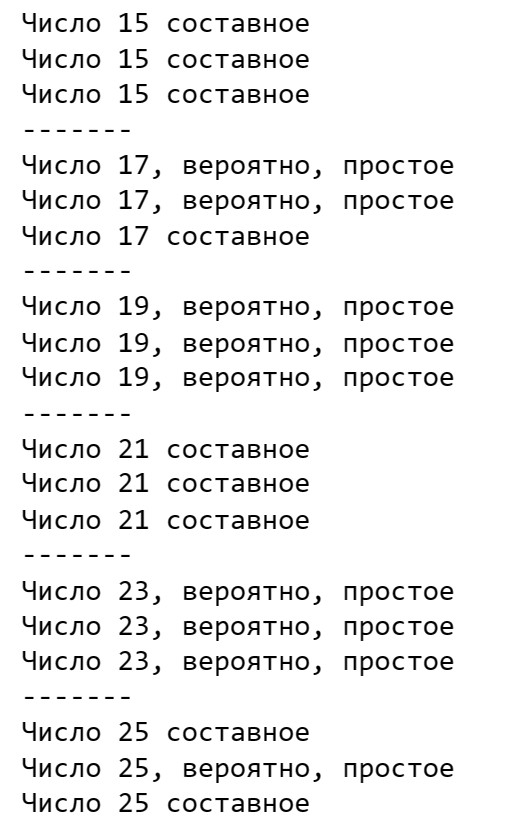


Рис. 6: Результаты выполнения алгоритмов

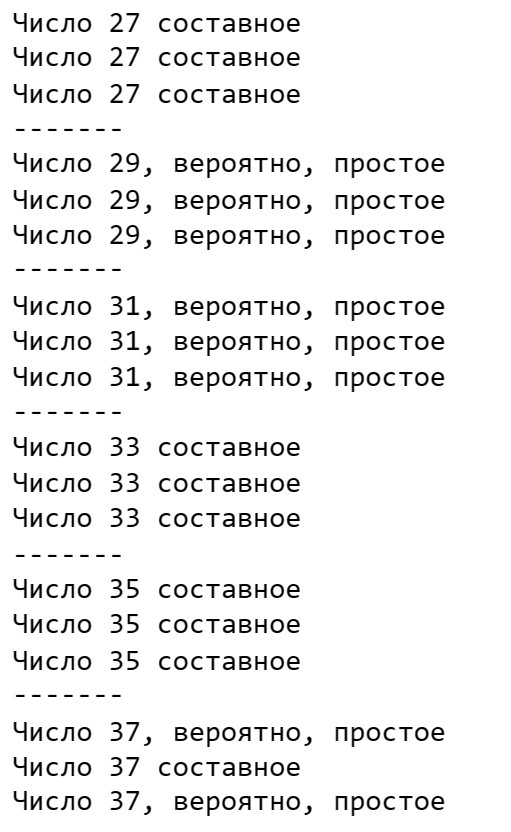


Рис. 7: Результаты выполнения алгоритмов

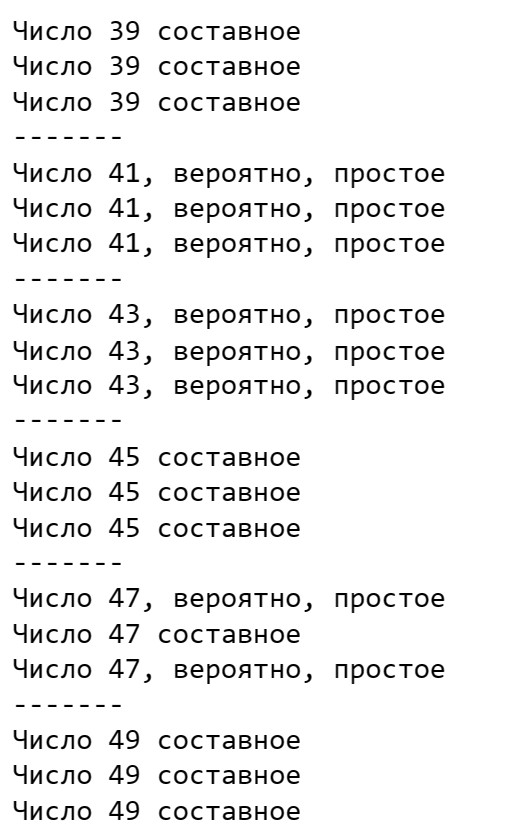


Рис. 8: Результаты выполнения алгоритмов

# 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы вероятностные алгоритмы проверки чисел на простоту.

# Список литературы

1. Тест Ферма [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0>.

2. Символ Якоби [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/Jacobi_symbol>.

3. Тест Соловэя-Штрассена [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A1%D0%BE%D0%BB%D0%BE%D0%B2%D0%B5%D1%8F_%E2%80%94_%D0%A8%D1%82%D1%80%D0%B0%D1%81%D1%81%D0%B5%D0%BD%D0%B0>.

4. Тест Миллера-Рабина [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%9C%D0%B8%D0%BB%D0%BB%D0%B5%D1%80%D0%B0_(%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D1%87%D0%B8%D1%81%D0%B5%D0%BB)>.