Лабораторная работа №5

Дисциплина: Математические основы защиты информации и информационной безопасности

Аветисян Давид Артурович

Содержание

# 1 Цель работы

Познакомиться с вероятностными алгоритмами проверки чисел на простоту.

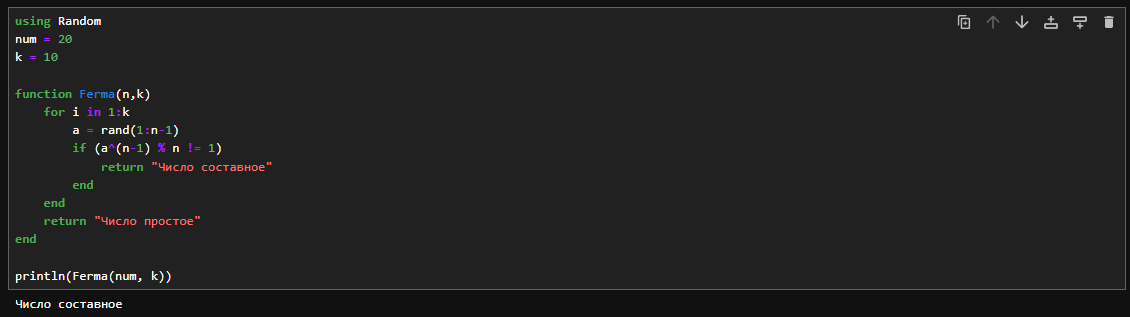
# 2 Задание

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

# 3 Выполнение лабораторной работы

Данная работа была выполнена на языку Julia.

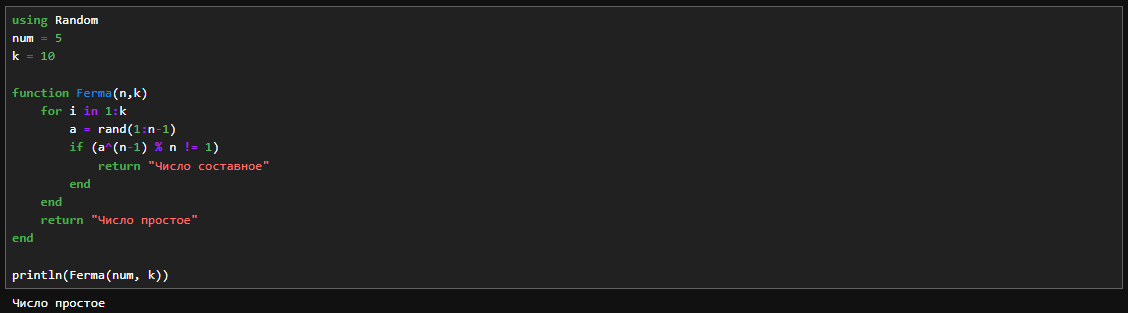
1. Для реализации теста Ферма была написана следующая программа.



Тест Ферма на языке Julia

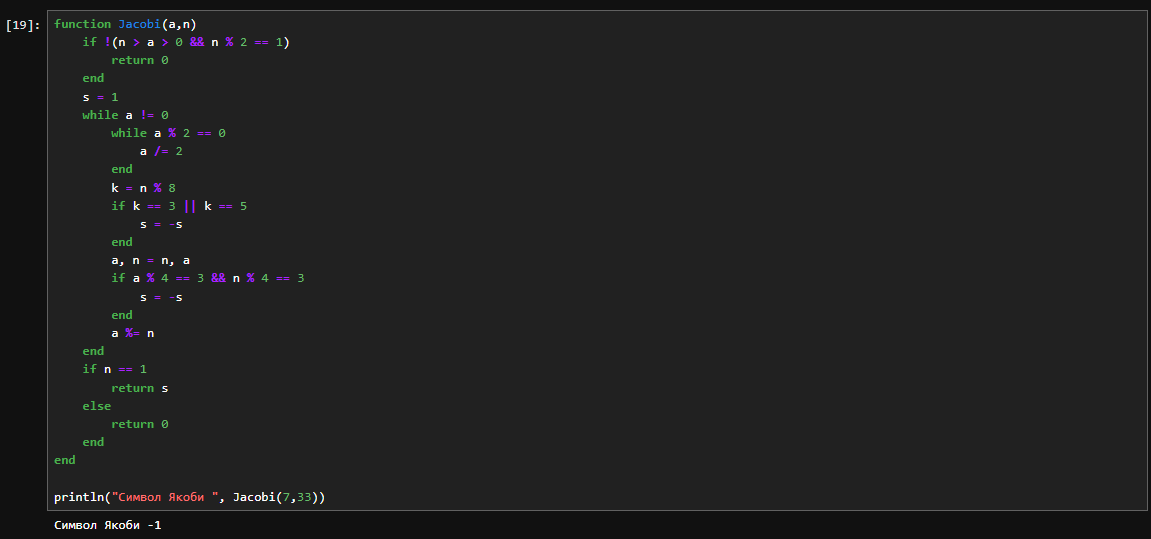
В данной программе: - 2-3 строки: задание числа, которое нужн проверить на простоту, и количество проверок. - 5 строка: задание функции. - 6 строка: цикл проверки выполняется раз. - 7 строка: берётся случайно число в диапазоне . - 8 строка: проводим проверку условия, при невыполнении сразу завершаем работу. - 9-13 строки: выводим результат, закрываем функцию.

Мы можем видеть результат для двух случае на рисунках выше и ниже. Программа работает верно.



Тест Ферма на языке Julia

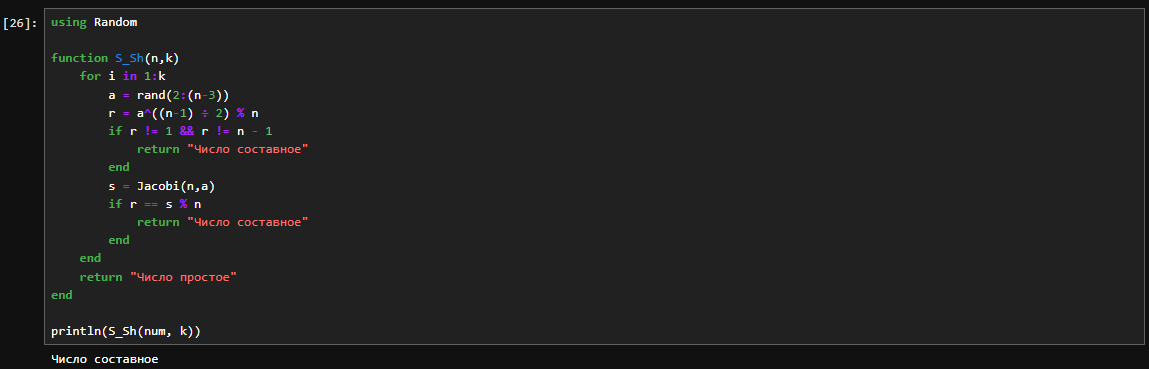
1. Для реализации поиска символа Якоби была написана следующая программа.



Поиск символа Якоби на языке Julia

В данной программе: - 1-5 строки: задание функции, проверка условия для вычисления символа Якоби. - 6-25 строки - реализация алгоритма: проверка трёх условия и действия согласно этим условиям: смена знака символа при четном и нечетном , проверка остатков от деления. - 26 строка: вывод результата раброты программы. В данном случае я вычислял Якоби 7 и 33. Вывод представлен на рисунке выше.

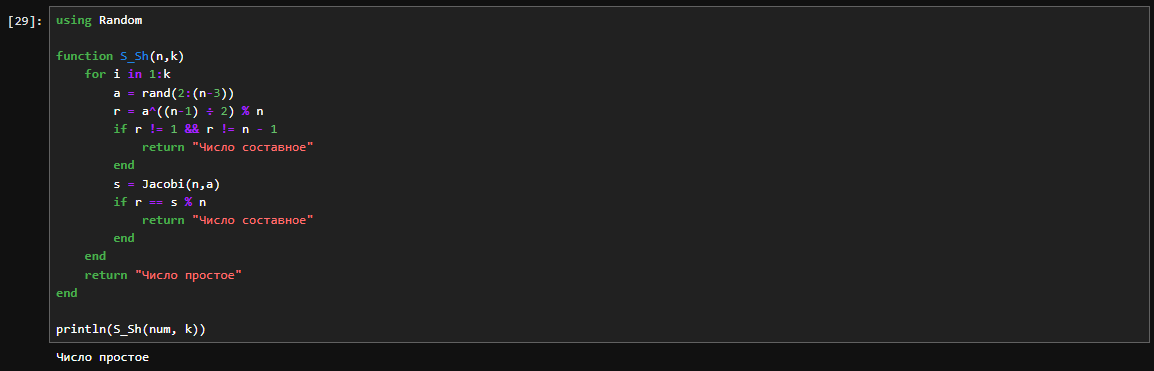
1. Для реализации теста Соловэя-Штрассена была написана следующая программа.



Тест Соловэя-Штрассена на языке Julia

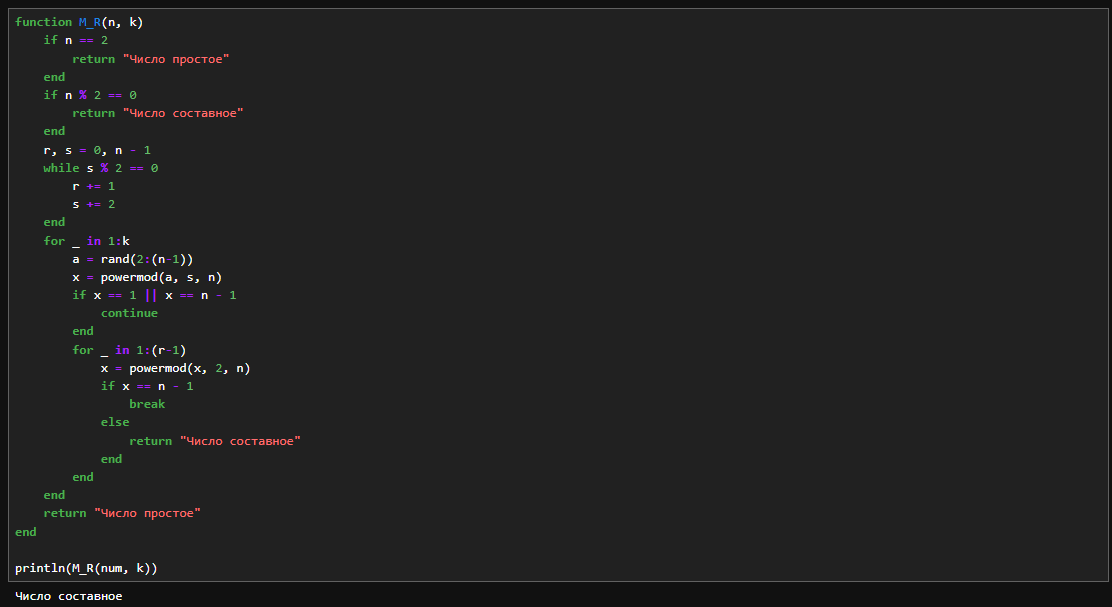
В данной программе: - 3 строка: задаём функцию. - 4 строка: повторим проверку раз - 5-16 строки - реализация алгоритма: выбираем случайное число , вычисляем число по формуле в строке 6, а затем проверяем получившееся значение на два условия. Если оно не проходит, проверку, то сразу заканчиваем работу программы. Далее следует ещё одна проверка условия в строке 11, при провале также завершаем работу. - 18 строка: вывод на экран. Результат работы программы с числами 20 и 5 и 10-ю проверками.

Мы можем видеть результат для двух случае на рисунках выше и ниже. Программа работает верно.



Тест Соловэя-Штрассена на языке Julia

1. Для реализации теста Миллера-Рабина была написана следующая программа.



Тест Миллера-Рабина на языке Julia

Данная программа работает рекурсивно, рассматривая 4 случая: - 3 строка: задаём функцию. - 4-9 строки: отсеивание числа 2 и остальных четных чисел. - 11-29 строки - реализация алгоритма: выбираем случайное число и вычисляем число по формуле в строке 17. При условии в строке 18 выполняем дополнительные действия - вычисление остатка от деления квадра на проверяемое число. Если число прошло все проверки раз, мы определяем его как “вероятно, простое”.

Результат работы программы с числом 20 и 10-ю проверками представлен на рисунке выше.

# 4 Выводы

Я познакомился с вероятностными алгоритмами проверки чисел на простоту.