Федеральное государственное автономное образовательное учреждение высшего профессионального образования

Национальный исследовательский университет «Высшая школа экономики»

Московский институт электроники и математики

Департамент прикладной математики

Кафедра «Компьютерная безопасность»

**ОТЧЁТ**

**ПО КУРСОВОЙ РАБОТЕ**

по дисциплине «Теоретико-числовые методы в криптографии»

Реализация теста Прота

Выполнил:

студент группы СКБ-172

Булгаков В.В.

МОСКВА 2021

Оглавление

[Цель работы 3](#_Toc73208856)

[Теоретическая часть 3](#_Toc73208857)

[Код программы: 5](#_Toc73208858)

[Результаты тестов: 5](#_Toc73208859)

[Инструкция по запуску кода: 6](#_Toc73208860)

[Источники 6](#_Toc73208861)

# Цель работы

Реализация проверки числа на число Прота и реализация тестирования Прота этого же числа на простоту в Sage (система компьютерной алгебры).

Необходимо:

1. Реализовать проверку введенного числа на число Прота

2. Реализовать тестирование Прота.

Произвести тестирование:

1. Проверить, что введенное число является числом Прота.

2. Проверить введенное число на простоту, с помощью теста Прота.

# Теоретическая часть

**Число Прота** – натуральное число вида:

Без последнего условия числами Прота были бы все нечётные целые числа больше 1.

Названы в честь французского математика Франсуа Прота (1852–1879).

Первые числа Прота:

Однако, наибольший интерес представляют простые числа Прота, первые из них:

Теорема Прота – детерминированный тест на простоту с полиномиальным временем. Т.е. он дает гарантированно точный ответ, простое ли исследуемое число или нет, при этом время его работы ограничено сверху многочленом от размера входа алгоритма. Однако, тест не получил широкого практического применения вследствие сложности алгоритма его реализации – алгоритм работает только с числами Прота.

**Теорема Прота** звучит так:

Если – число Прота вида , где – нечетно и , то – простое число Прота тогда и только тогда, когда для некоторого квадратичного невычета выполняется сравнение:

**Тестирование чисел Прота на простоту**

Теорема Прота может быть использована для тестирования простоты чисел Прота. Алгоритм вероятностного теста, основанного на теореме, выглядит следующим образом:

Случайный образом выбирается целое число , такое что и вычисляется .

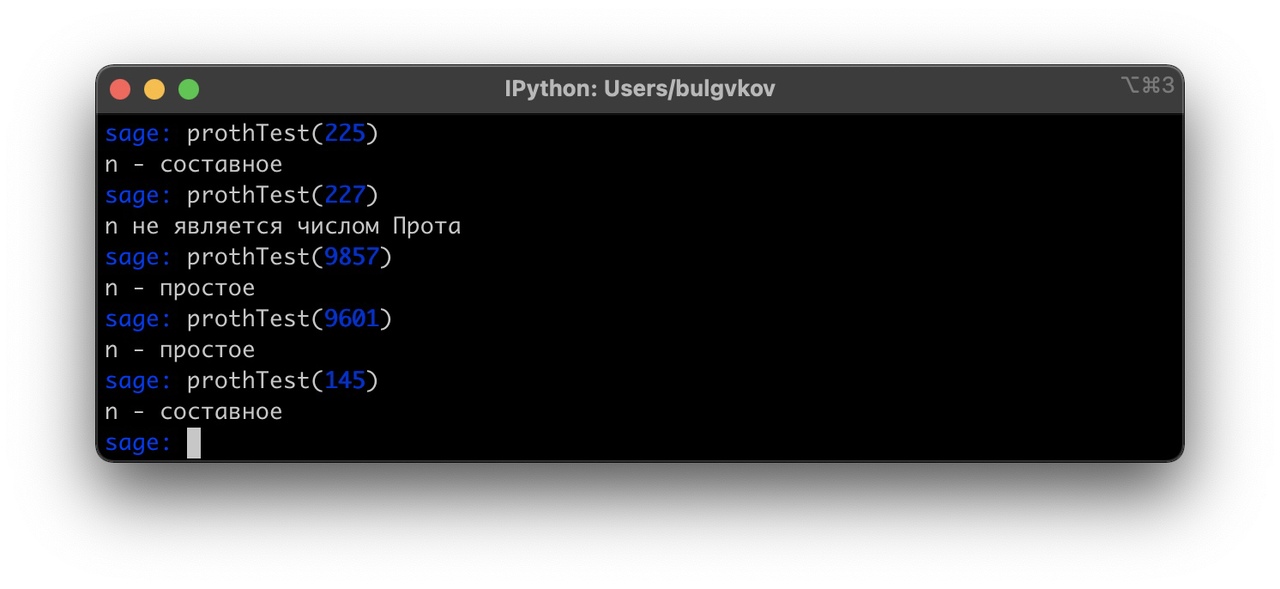
Возможные исходы:

Исход под номером 4 является причиной того, что тест вероятностный. В случае 1 – квадратичный невычет по модулю . Процедура повторяется пока простота не будет установлена. Если – простое, то тест с вероятностью подтвердит это за одну итерацию, так как количество квадратичных невычетов по модулю равно .

# Код программы:

1. **def** checkProth(n):
2. k **=** 1
3. **while** k < ceil(sqrt(n)):
4. **if** floor((n **-** 1) **/** k) & floor((n **-** 2) **/** k) **==** 0:
5. **return** True
6. **else**:
7. k **=** k **+** 2
8. **return** False
10. **def** prothTest(n):
11. **if** checkProth(n):
12. R **=** IntegerModRing(n) #кольцо вычетов по mod n
13. a **=** R(sage.misc.prandom.choice(range(2, n)))
14. b **=** a ^ ((n **-** 1) **/** 2)
15. **if** b **==** R(**-**1):
16. print('n - простое')
17. **elif** b !**=** 1 **and** b !**=** **-**1 **and** b ^ 2 **==** 1 **or** b ^ 2 !**=** 1:
18. print('n - составное')
19. **elif** b **==** 1:
20. prothTest(n)
21. **else**:
22. print('n не является числом Прота')

# Результаты тестов:



# Инструкция по запуску кода:

Код находится по ссылке: <https://github.com/bulgvkov/prothTest>

Для запуска кода, у Вас должна быть установлена SageMath, ссылка на скачивание: <https://www.sagemath.org/>.

# Источники

1. Теорема Прота: <https://ru.wikipedia.org/wiki/Теорема_Прота>
2. Статья на хабре о теореме и тесте Прота: <https://habr.com/ru/post/545208/>
3. Мануал SageMath: <https://www.sagemath.org/>.