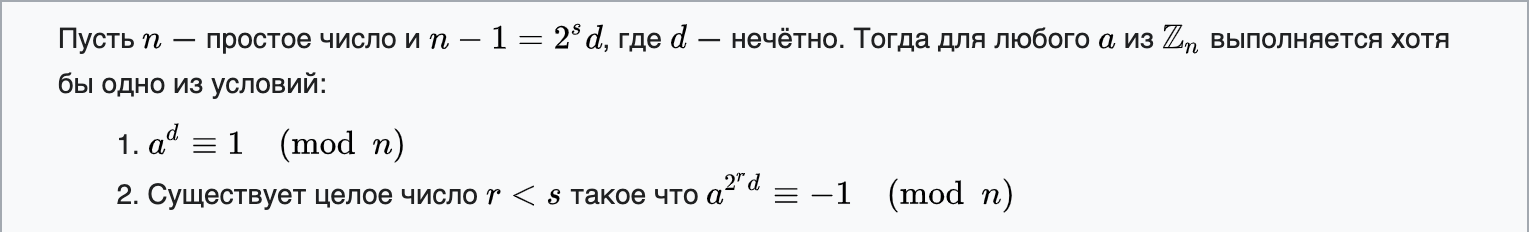
**Гончаренко Андрей Дмитриевич, 15 гр. 5 вариант**

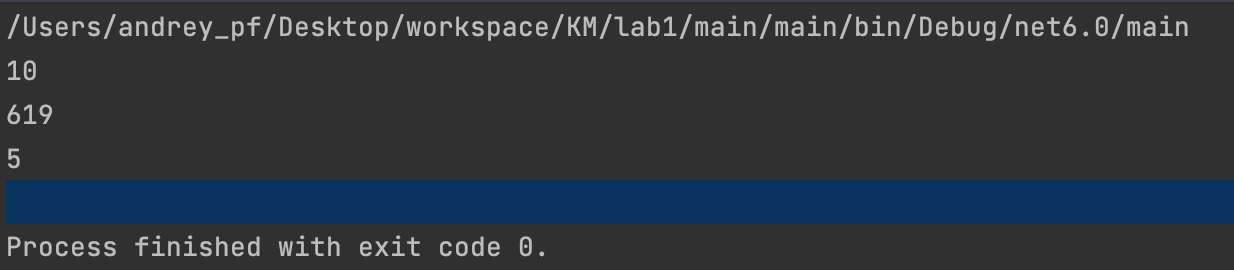
1) Тест Миллера-Рабина — вероятностный полиномиальный тест простоты. Тест Миллера-Рабина, наряду с тестом Ферма и тестом Соловея-Штрассена, позволяет эффективно определить, является ли данное число [составным](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE" \o "Составное число). Однако, с его помощью нельзя строго доказать [простоту числа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE" \o "Простое число). Тем не менее тест Миллера-Рабина часто используется в [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F" \o "Криптография) для получения больших [случайных простых чисел](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE" \o "Случайное простое число).

Как и тесты [Ферма](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0" \o "Тест Ферма) и Соловея-Штрассена, тест Миллера-Рабина опирается на проверку ряда равенств, которые выполняются для простых чисел. Если хотя бы одно такое равенство не выполняется, это доказывает что число составное.

Для теста Миллера-Рабина используется следующее утверждение:



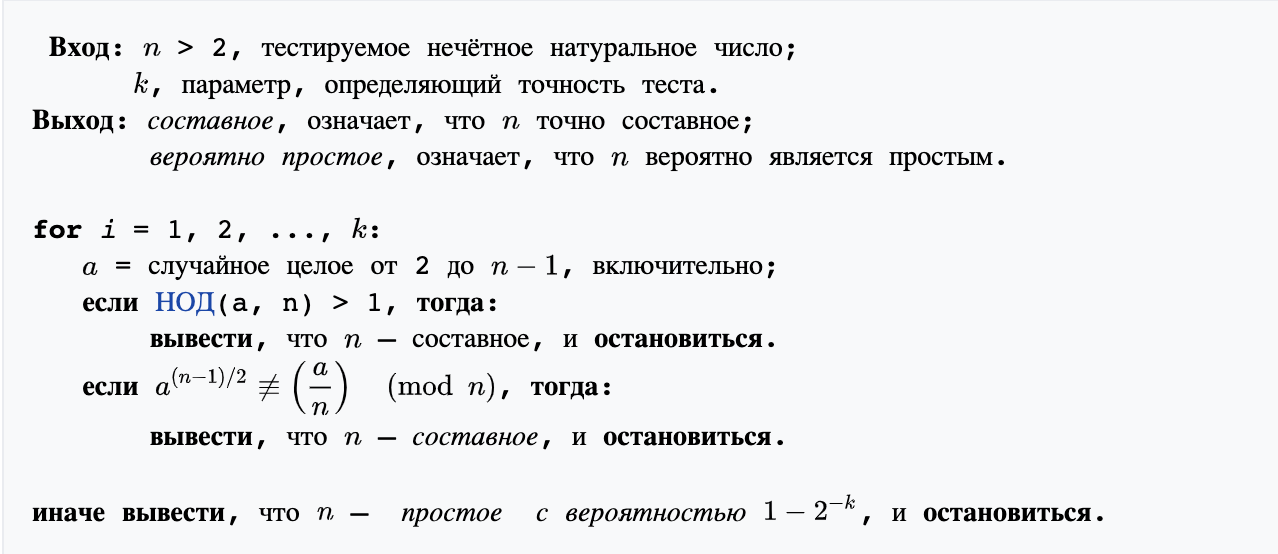
Результат выполнения программы:



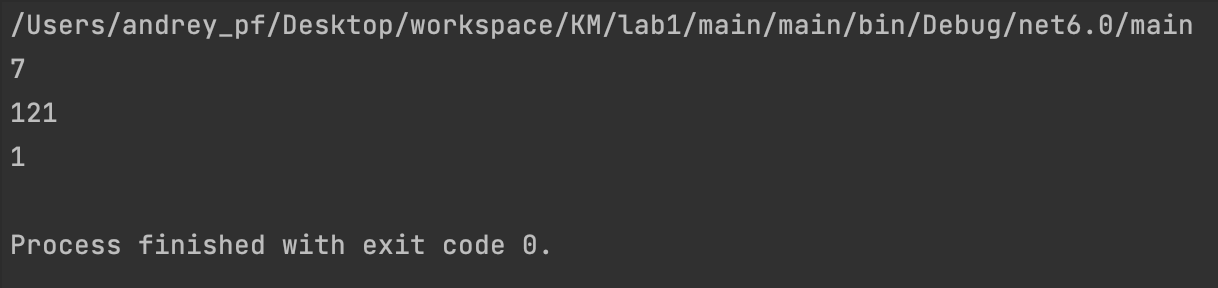
1. В первой строке мы вписываем размер простого числа в битах
2. Во второй строке получаем простое число
3. В третье строке получаем кол-во выполненных циклов

2) Тест Соловея-Штрассена — вероятностный [тест простоты](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D1%82%D1%8B), открытый в 1970-х годах [Робертом Мартином Соловеем](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%BB%D0%BE%D0%B2%D0%B5%D0%B9,_%D0%A0%D0%BE%D0%B1%D0%B5%D1%80%D1%82_%D0%9C%D0%B0%D1%80%D1%82%D0%B8%D0%BD) совместно с Фолькером Штрассеном. Тест всегда корректно определяет, что [простое число](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) является простым, но для составных чисел с некоторой вероятностью он может дать неверный ответ. Основное преимущество теста заключается в том, что он, в отличие от [теста Ферма](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0), распознает [числа Кармайкла](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%B0_%D0%9A%D0%B0%D1%80%D0%BC%D0%B0%D0%B9%D0%BA%D0%BB%D0%B0) как составные.

Алгоритм Соловея-Штрассена параметризуется количеством раундов k. В каждом раунде случайным образом выбирается число . Если , то выносится решение, что n составное. Иначе проверяется справедливость сравнения . Если оно не выполняется, то выносится решение, что n — составное. Если это сравнение выполняется, то a является свидетелем простоты числа n. Далее выбирается другое случайное a и процедура повторяется. После нахождения k свидетелей простоты в k раундах выносится заключение, что n является простым числом с вероятностью  .

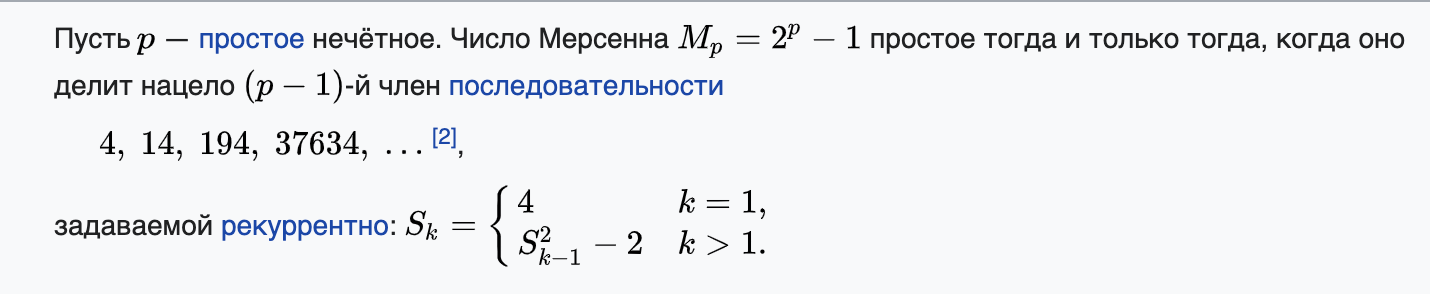


Результат выполнения программы:



1. В первой строке мы вписываем размер простого числа в битах
2. Во второй строке получаем простое число
3. В третье строке получаем кол-во выполненных циклов

3) При заданном [простом числе](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE)  тест позволяет за полиномиальное время от битовой длины  числа Мерсенна  определить, является  простым или [составным](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE). [Доказательство](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) справедливости теста существенно опирается на [функции Люка](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%9B%D1%8E%D0%BA%D0%B0), что позволило обобщить тест Люка — Лемера на некоторые числа, вид которых отличен от чисел Мерсенна.



Результат выполнения программы:

