Лабораторная работа 3. Проверка числа на простоту. Генерация простых чисел.

Задание на лабораторную работу:

Часть 1. Реализовать:

1. Метод пробных делений.
2. Тест простоты на основе малой теоремы Ферма.
3. Тест простоты Миллера–Рабина.
4. Любой способ генерации простых чисел.

Часть 2. Проверить корректность работы программ с помощью тестирующей системы Contester.

Часть 3. Используя подготовленные программы, заполнить таблицу в соответствии с примером (первая строка). Если по результатам проверки число является составным, укажите хотя бы один его делитель. Если число не является составным, укажите нескольких свидетелей его простоты.

Число	Метод делений	Тест на основе МТФ	Тест Миллера–Рабина
561	`composite, 3`	`pseudoprime, 3, 19`	`composite, 3`
1913			
7873			
40949			
172081			
433879			
499963			
900001			
5764643587			
810001800001			
100000380000361			
1000000016000000063			

Все ли строки таблицы вам удалось заполнить? Если не все, в чем причина?

Теоретический материал. О.Н. Василенко «Теоретико-числовые алгоритмы в криптографии», §1.2, §1.4, §1.7.

Отчет должен содержать:

1. Титульный лист.
2. Задание.
3. Листинг программы с комментариями.
4. Таблицу с результатами работы программы.
5. Выводы об эффективности и применимости метода пробных делений, теста на основе малой теоремы Ферма, теста Миллера–Рабина.