БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №3**

**«**Основы теории чисел и их использование в криптографии»

Выполнила:

студентка 3 курса 5 группы

Почиковская Юлия Сергеевна

Вариант 10

Проверил:

Берников В. О.

Минск 2022

1. **Описание приложения**

**Приложение разработано на языке С++ позволяет выполнять:**

* вычислять НОД двух и трех чисел;
* выполнять поиск простых чисел на промежутке [m; n];
* находить все простые числа в интервале [2; n];
* сравнивать это число с n/ln(n);
* находить обратное число по модулю.

Значение n = 621; m = 587 – задано в варианте лабораторной работы.

1. **Выполнение заданий**

Нахождение НОД двух и трех чисел выполняется с помощью алгоритма Евклида. Для нахождения НОД для трех и более чисел функция Euclid2 вызывается сначала для двух чисел, а затем для третьего числа и НОД первых двух чисел. Описание функций на рисунке 2.1:

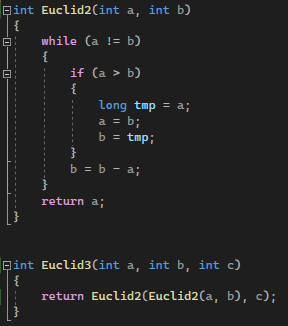
****

Рисунок 2.1 – Вычисление НОД с помощью алгоритма Евклида

Поиск простых чисел на заданном промежутке осуществляется с помощью «Решето Эратосфена». Определение промежутка осуществляется вводом граничных значений в консоли. Описание функции приведено на рисунке 2.2:

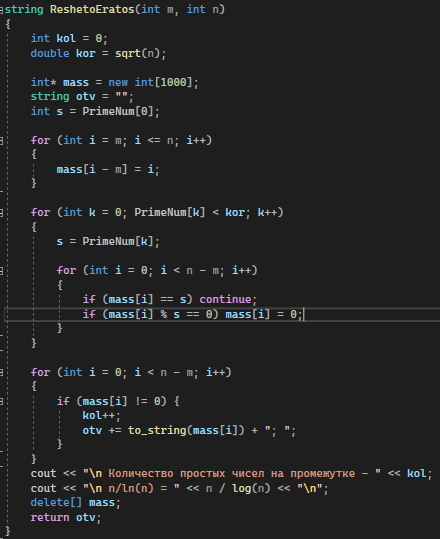


Рисунок 2.2 – Решето Эратосфена

Целые числа записываются в массив, каждый элемент массива проверяется на делимость на последовательность простых чисел, и, если, остаток равен нулю, удаляется из массива.

Результат выполнения функций выводится в консоль, содержимое показано на рисунке 2.3:

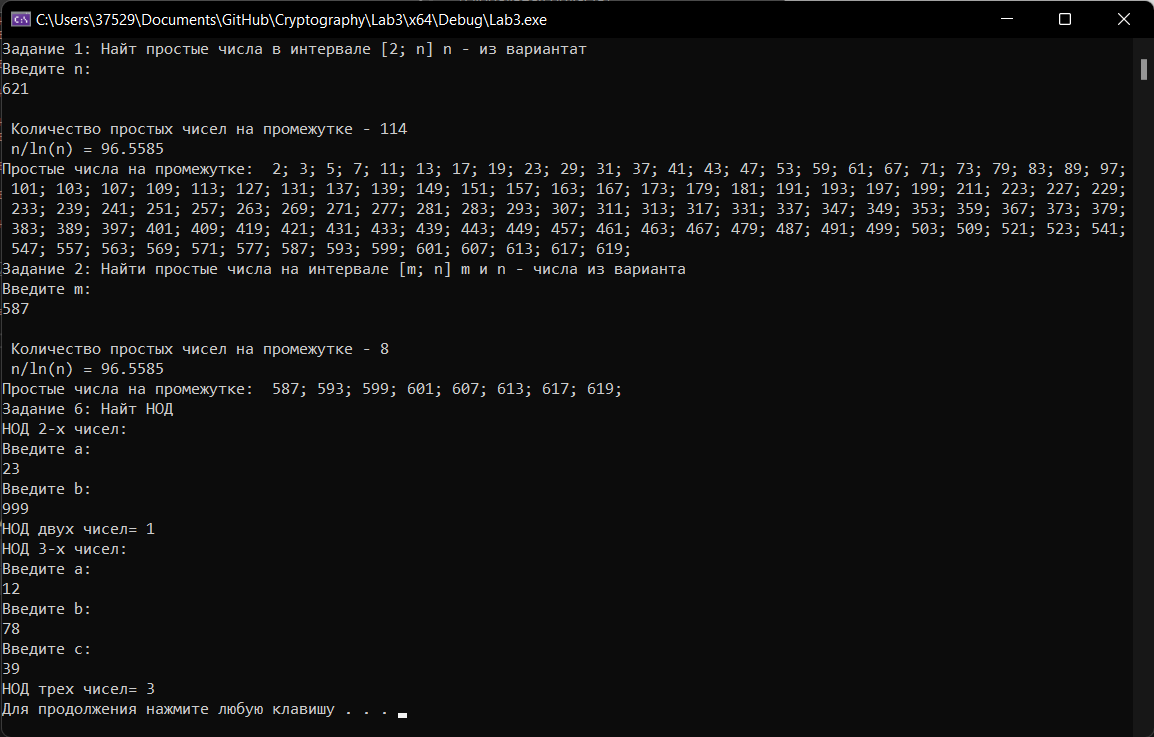


Рисунок 2.3 – Результат работы функций

**Вывод**

В ходе лабораторной работы были приобретены навыки выполнения операций с числами для решения задач в области криптографии, а также разработано приложение для автоматизации этих операций.