Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание разработанного приложения**

Приложение написано на языке программирования C# и позволяет:

* вычислять НОД двух и трех чисел;
* выполнять поиск простых чисел на промежутке [555; 591];
* находить все простые числа в интервале [2;*n*];
* сравнивать это число с *n*/ln(*n*);
* Сравнить полученные результаты c вычислениями, используя «решето Эратосфена»

1. **Методика выполнения поставленных задач**

Для нахождения НОД двух чисел в данном приложении используется алгоритм Евклида, который мы разработали для языка c#. Описание функции приводится на рисунке 2.1.

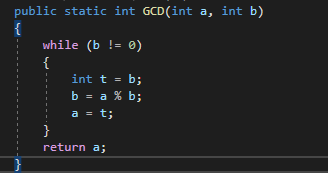


Рис. 2.1 – Функция для расчета энтропии

Для нахождения НОД 3 и более чисел вызывается функция приведенная выше сначала для двух чисел, а затем для третьего числа и НОД первых двух чисел.

Для поиска простых чисел на заданном промежутке используется два подхода: перебор чисел и Решето Эратосфена. Передача границ искомого промежутка осуществляется с консоли. Все целые числа на промежутке записываются в массив, после чего каждый его элемент проверяется на делимость на последовательность простых чисел, и, если остаток равен нулю, удаляется из массива. Описание двух функций приведены на рисунке 2.2 и 2.3.

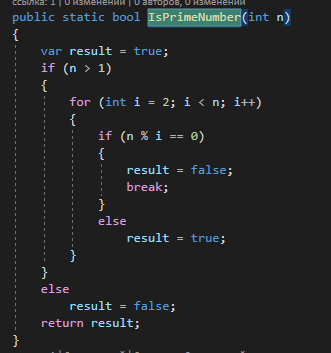


Рис. 2.2 – Перебор чисел

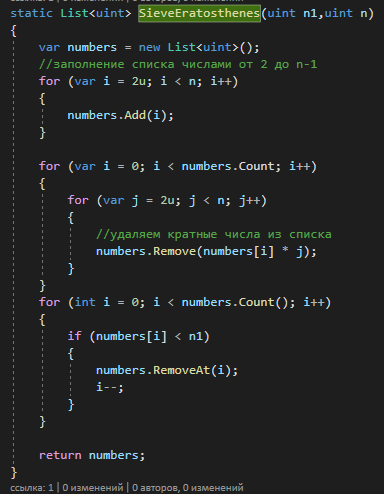


Рис. 2.3 – Автоматизированное решето Эратосфена

Результат выполнения всех описанных ранее функций выводится на консоль, содержимое которой представлено на рисунке 2.4, 2.5.

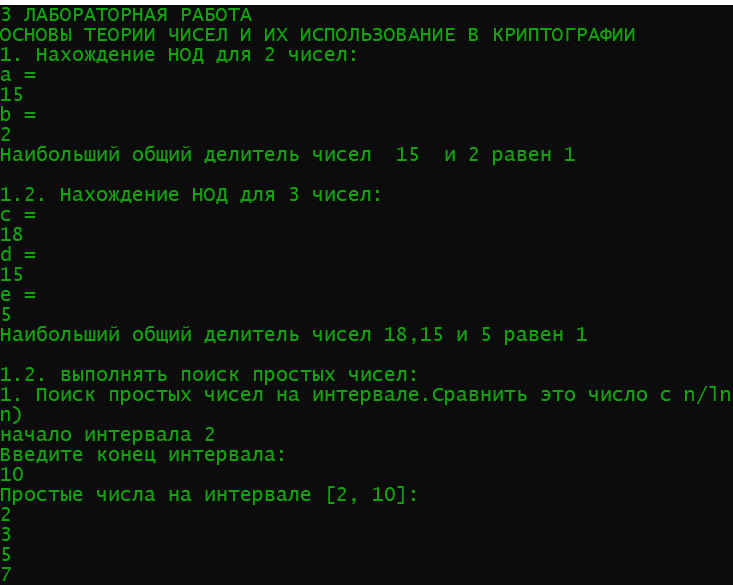


Рисунок 2.4– Результат выполнения функций

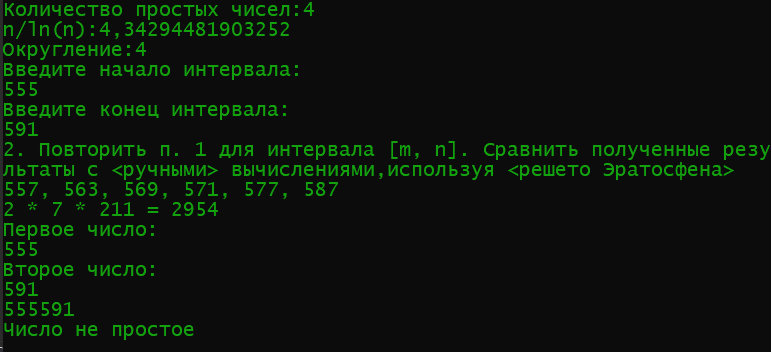


Рисунок 2.5 – Результат выполнения функций

**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.