Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Каспер Н.В.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* рассчитать наибольший общий делитель 2 и 3 чисел;
* найти обратное число по модулю с помощью расширенного алгоритма Евклида;
* найти простые числа на заданном интервале.

1. **Методика выполнения поставленных задач**

Для поиска простых чисел на интервале реализована функция, представленная на рисунке 2.1, которая позволяет проверить является ли чисто простым. В случае, если число простое – возвращается true, в противном случае – false.

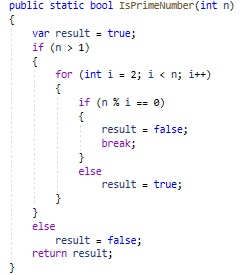


Рисунок 2.1 – Функция проверки числа на простоту

Вызов функции для нахождения простых чисел на интервале представлен на рисунке 2.2.

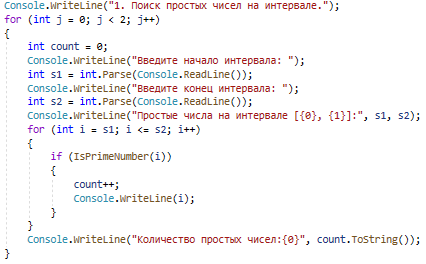


Рисунок 2.2 – Поиск простых чисел на интервале

Функция для поиска наибольшего общего делителя чисел, а также ее реализация, показана на рисунке 2.3.

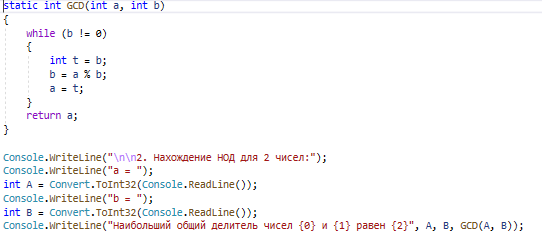


Рисунок 2.3 – Функция нахождения НОД

Реализация расширенного алгоритма Евклида представлена на рисунке 2.4.

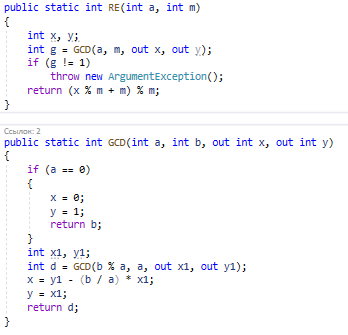


Рисунок 2.4 – Расширенный алгоритм Евклида

Таким образом, были реализованы все поставленные задачи.

**Вывод**

В ходе лабораторной работы были приобретены навыки по нахождению НОД для чисел, нахождению простых чисел, а также изучены принципы работы расширенного алгоритма Евклида.

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с теорией чисел.