Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет по лабораторной работе №1**

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

Выполнил:

студентка 3 курса 2 группы

Черноок Ю. С.

Проверил:

ассистент

Копыток Д. В.

Минск 2021

Цель: приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* вычислять НОД двух и трех чисел;
* выполнять поиск простых чисел на промежутке [m; n];
* находить все простые числа в интервале [2; n];

1. **Методика выполнения поставленных задач**

Для нахождения НОД двух в данном приложении используется алгоритм Евклида. Описание функции приводится на рисунке 1.

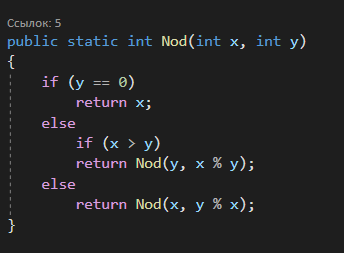


Рисунок 1 – Автоматизированный алгоритм Евклида

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.

Функция нахождения простых чисел в заданном интервале приведена на рисунке 2.

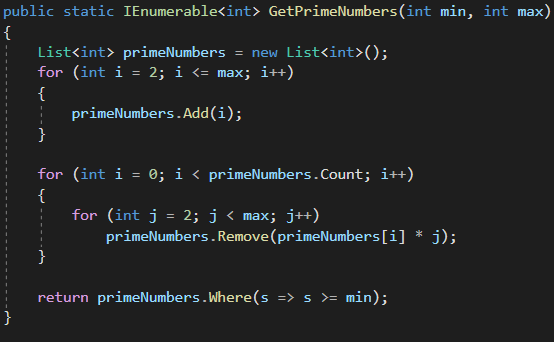


Рисунок 2 – Нахождение простых чисел в заданном интервале

На рисунке 3 представлено выполнения процедуры нахождения простых чисел в интервале [2; n], где n = 503.

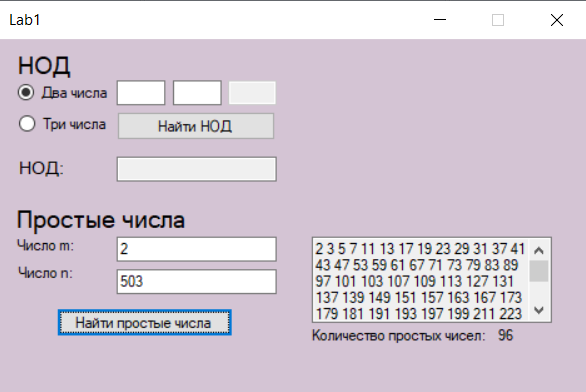


Рисунок 3 – Нахождение простых чисел в интервале [2; n]

Для интервала [m;n], где m = 450, n = 503, результат выполнения представлен на рисунке 4.

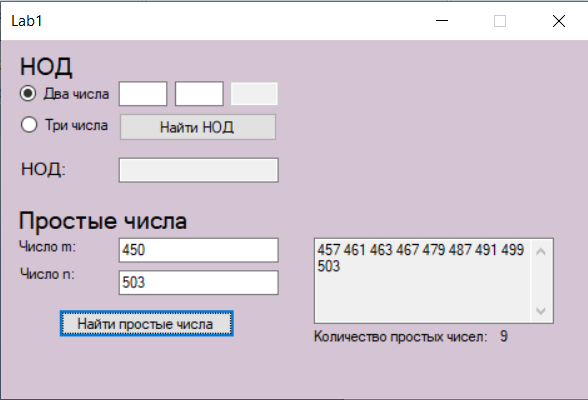


Рисунок 4 – Нахождение простых чисел в интервале [m; n]

Нахождение НОД двух чисел показано на рисунке 5.

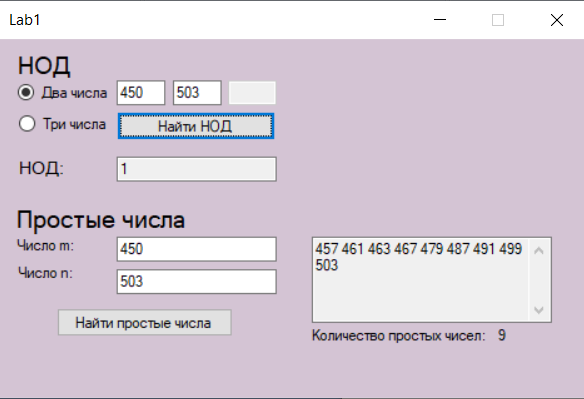


Рисунок 5 – Нахождение НОД двух чисел

Нахождение НОД трех чисел показано на рисунке 6.

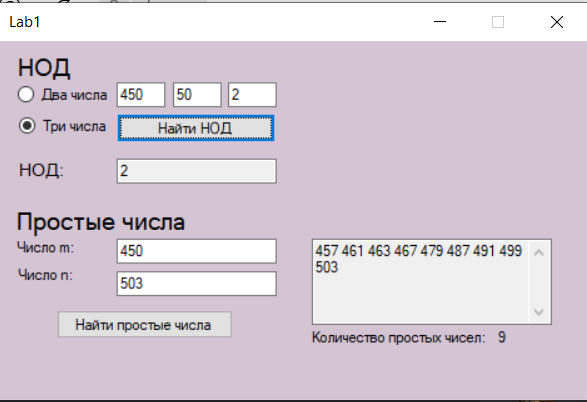


Рисунок 6 – Нахождение НОД двух чисел

Вывод: я приобрела практические навыки выполнения операций с числами для решения задач в области криптографии и разработки приложений для автоматизации этих операций.