Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Димитриади А.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание разработанного приложения**

Авторское приложение написано на языке программирования C# и позволяет выполнять следующие функции:

* вычислять НОД двух либо трех чисел;
* выполнять поиск простых чисел на промежутке [431; 471];
* 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. 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. Также для проверки сделаем ручное Решето Эратосфена диапазона наших чисел (431-471). Простыми являются: 431, 433, 439, 443, 449, 457, 461, 463, 467 так как ни на что не делятся кроме самих себя и 1. Числа: 432,434,436,438,440,442,444,446,448,450,452,454,456,458,460,462,464,466,468,470 делятся на 2. Числа которые делятся на 3 (кроме повторяющихся, которые делятся на два): 453,459,471 (выписываем те, которые делятся на три, но исключаем которые делятся на 2, так как уже их выписали и так далее). Числа которые делятся на 5: 435,445,455,465. Числа которые делятся на 7: 441, 469.

В задании *n* и *n*/ln(*n*) не будут совпадать, так как существует погрешность, которая дает приблизительно близкое число но с погрешностью.

Описание двух алгоритмов приведены на рисунке 2.2 и 2.3.

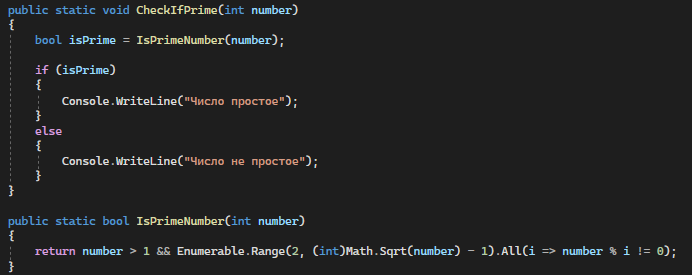


Рис. 2.2 – Перебор чисел

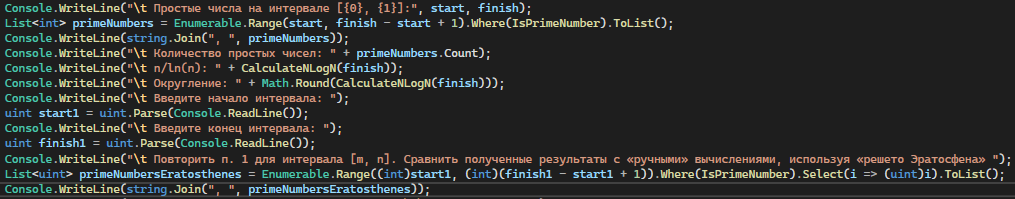


Рис. 2.3 – Работа решетэ Эратосфена

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

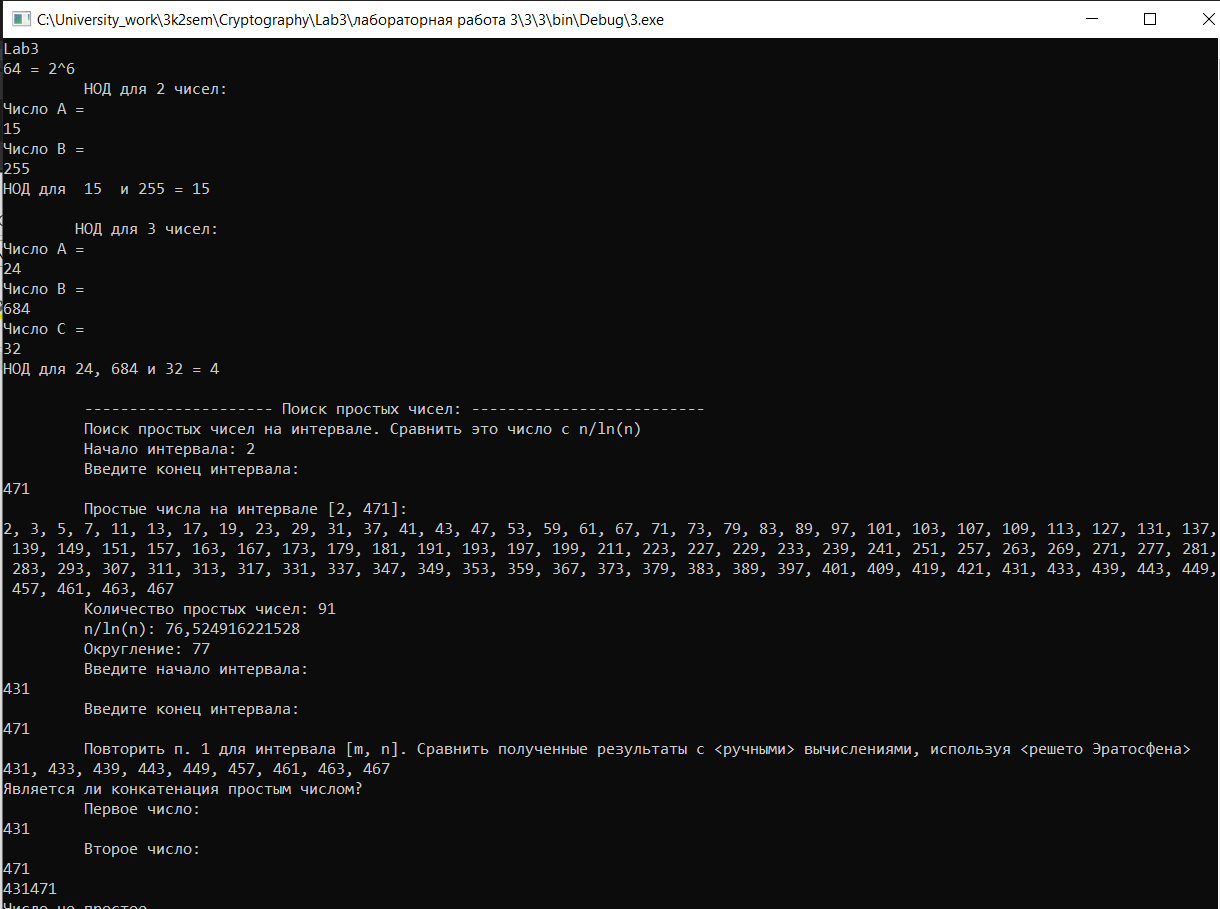


Рисунок 2.4– Результат выполнения функций

**Вывод**

В ходе лабораторной работы были приобретены навыки выполнения операций с числами для решения задач в области криптографии, поиск НОД чисел, поиск простых чисел, разработали приложение для выполнения этих операций.