Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 3**

« Основы теории чисел и их использование в криптографии»

Выполнил:

Студент: Дащинский М.Л..

ФИТ 2 курс 4 группа

Преподаватель: Сазонова Д.В.

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования Python и позволяет провести расчет НОД двух либо трех чисел, а также найти все простые числа в заданном промежутке.

Теория чисел или высшая арифметика – раздел математики, изучающий  
натуральные числа и иные похожие величины. В зависимости от используемых методов в теории чисел рассматривают несколько направлений. Нас будут интересовать вопросы делимости целых чисел, вычисления наибольшегообщего делителя (НОД).

1. **Методика выполнения расчетов**

В данной лабораторной работе была поставлена цель создания приложения, позволяющее произвести расчёт НОД двух либо трёх чисел, а также выполнить поиск простых чисел из диапазона. На листинге 2.1 представлен функции, реализующие данную функциональность.

def gcd(a, b):

    return math.gcd(a, b)

def gcd\_of\_three(a, b, c):

    return math.gcd(math.gcd(a, b), c)

def is\_prime(num):

*"""Function to check if a number is prime or not"""*

    if num < 2:

        return False

    for i in range(2, int(num \*\* 0.5) + 1):

        if num % i == 0:

            return False

    return True

def search\_primes(start, end):

*"""Function to search for prime numbers in a given interval"""*

    primes = []

    for num in range(start, end + 1):

        if is\_prime(num):

            primes.append(num)

    return primes

Листинг 2.1 – функции, реализующий необходимый функционал

Функция gcd используется для получения НОД двух чисел путём исполнения алгоритма Евклида. Метод is\_prime осуществляет проверку на то, является ли переданное в него в качестве параметра число простым. Метод search\_primes находит все простые числа в диапазоне, границы которого переданы в него в качестве двух параметров.

**3. Результаты работы приложения**

Для выполнения расчетов достаточно необходимо запустить приложение. Рисунок 3.1 показывает необходимые расчеты, требуемые в данной лабораторной работе.

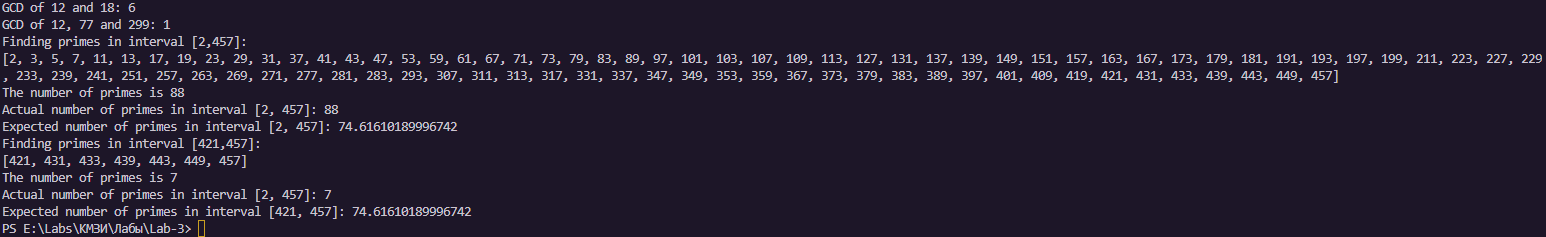


Рисунок 3.1 – Результат работы методе программы

**Вывод**

В ходе изучения теоретических материалов лабораторной работы и выполнения её практической части были изучены основы теории чисел, используемые в криптографии. Изучены основные свойства простых и составных чисел, взаимно простых чисел, а также признаки делимости чисел. На практике полученные знания были закреплены через создание собственного приложения, реализующего функционал вычисления НОД двух и трёх чисел и получения списка простых чисел в заданном диапазоне.