МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 3**

**ОСНОВЫ ТЕОРИИ ЧИСЕЛ**

**И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ**

Разработала: Некрасова А.П.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

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

**Задачи**:

1. Закрепить теоретические знания по высшей арифметике.
2. Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.
3. Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его помощью операций над простыми числами.
4. Разработать приложение для реализации указанных преподавателем операций с числами.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

**Практическое задание**

**Вариант 9 m=399, n=433**

1. Используя L\_PROST, найти все простые числа в интервале [2, n]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем.

Подсчитать количество простых чисел в указанном интервале. Сравнить это число с *n*/ln(*n*).

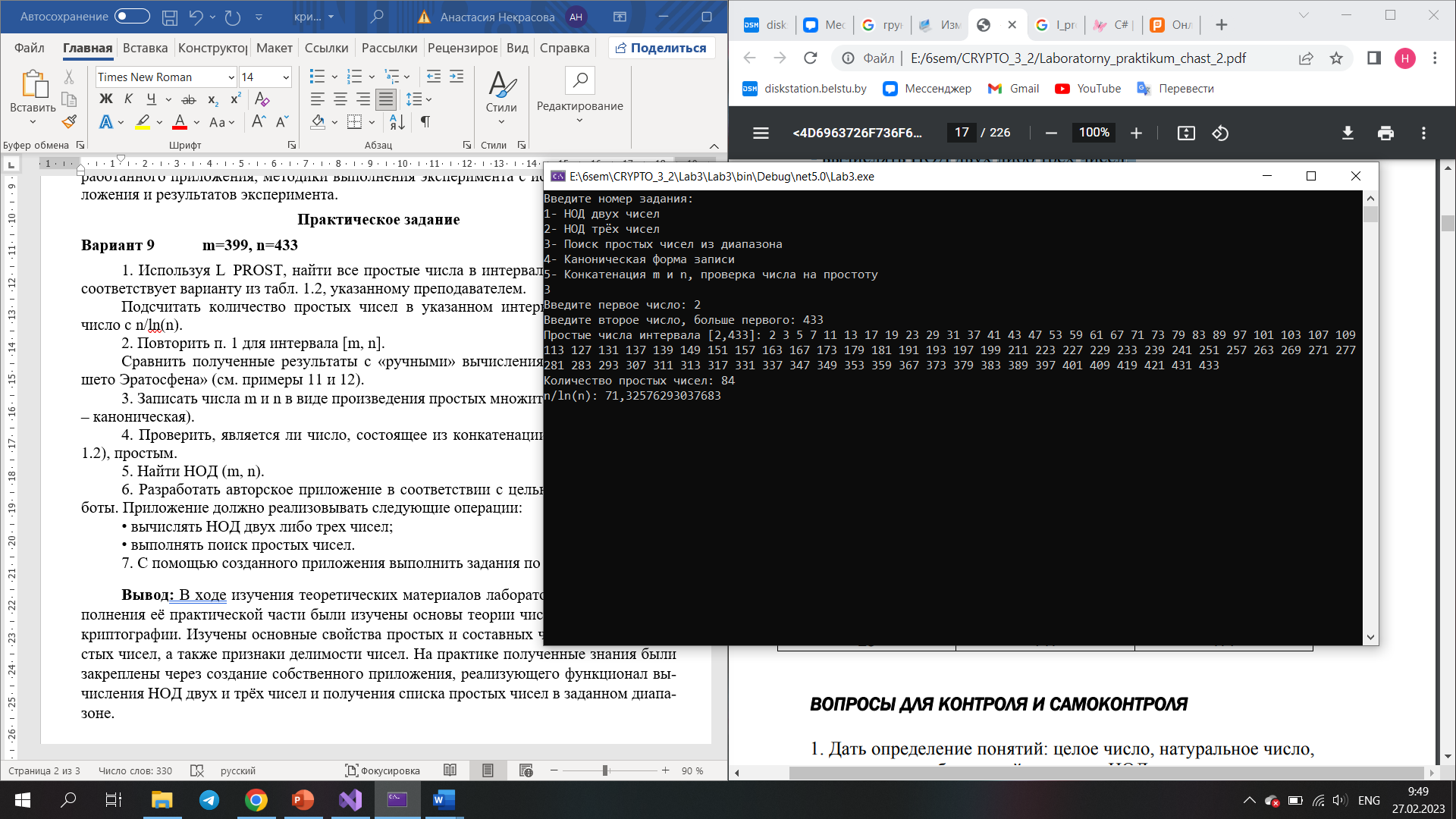


Рис.1 – Реализация поиска простых чисел на интервале

2. Повторить п. 1 для интервала [*m*, *n*].

Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».

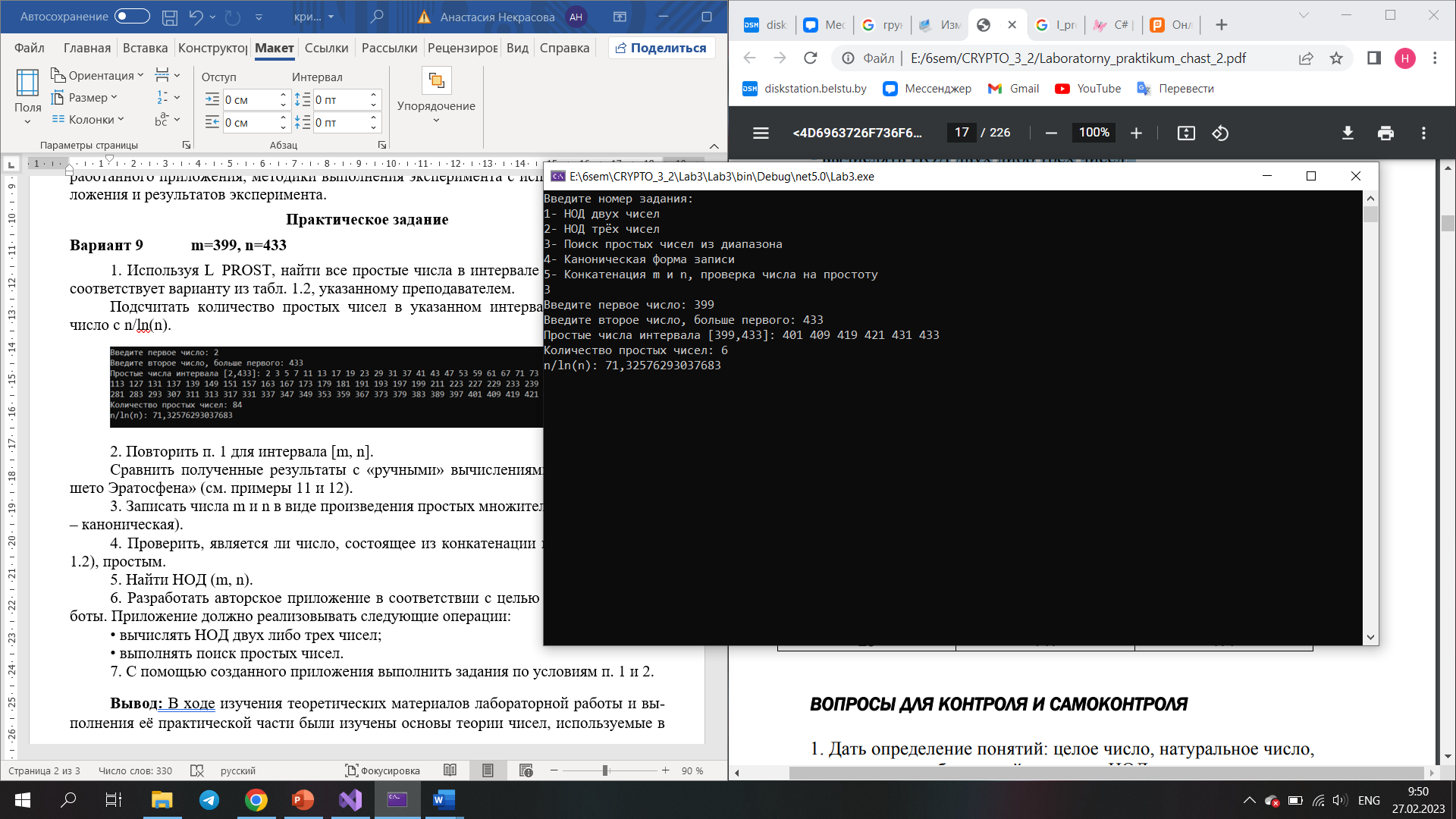


Рис.2 – Реализация поиска простых чисел на интервале

3. Записать числа *m* и *n* в виде произведения простых множителей (форма записи каноническая).

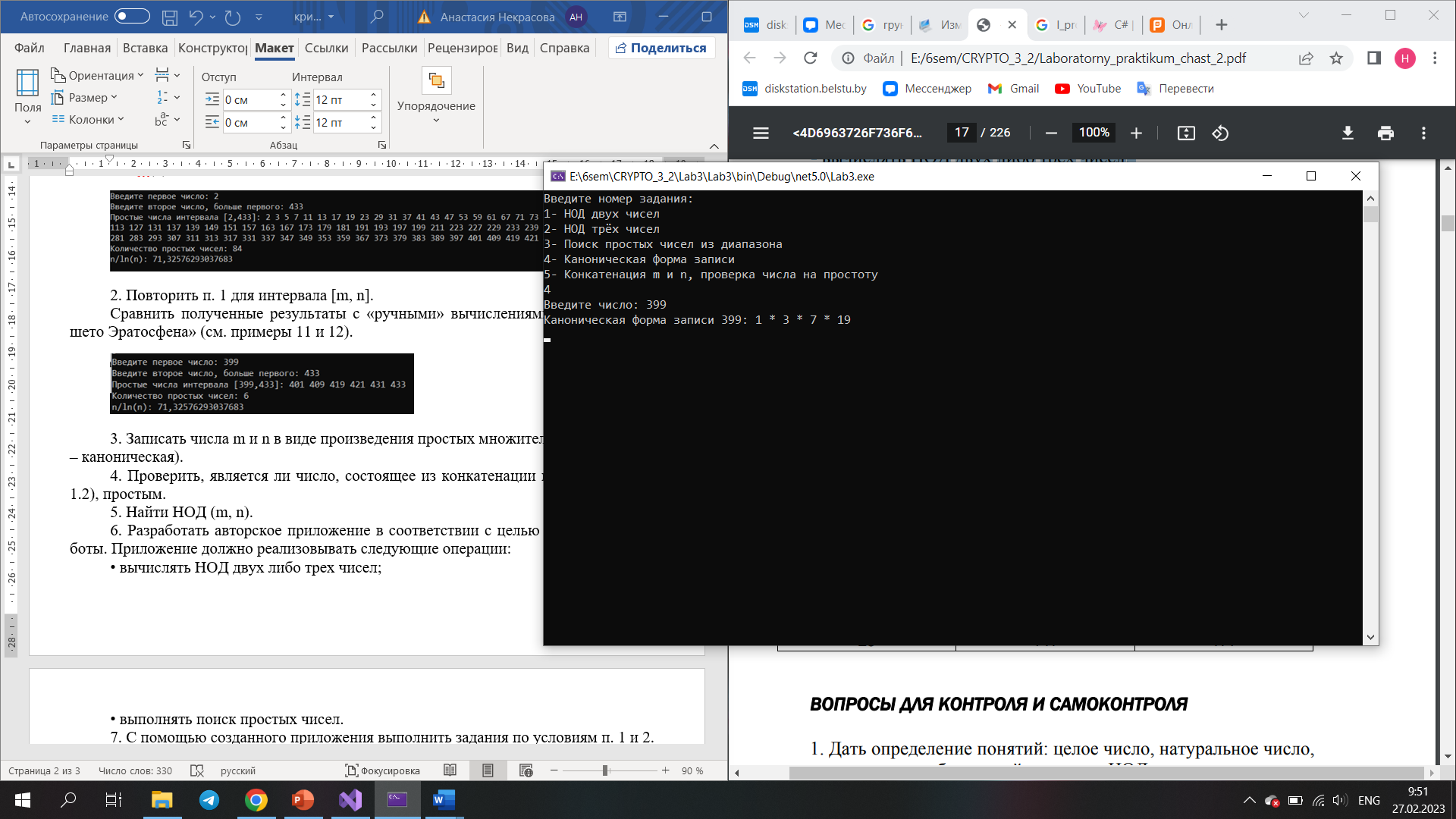


Рис.3 – Каноническая форма записи числа

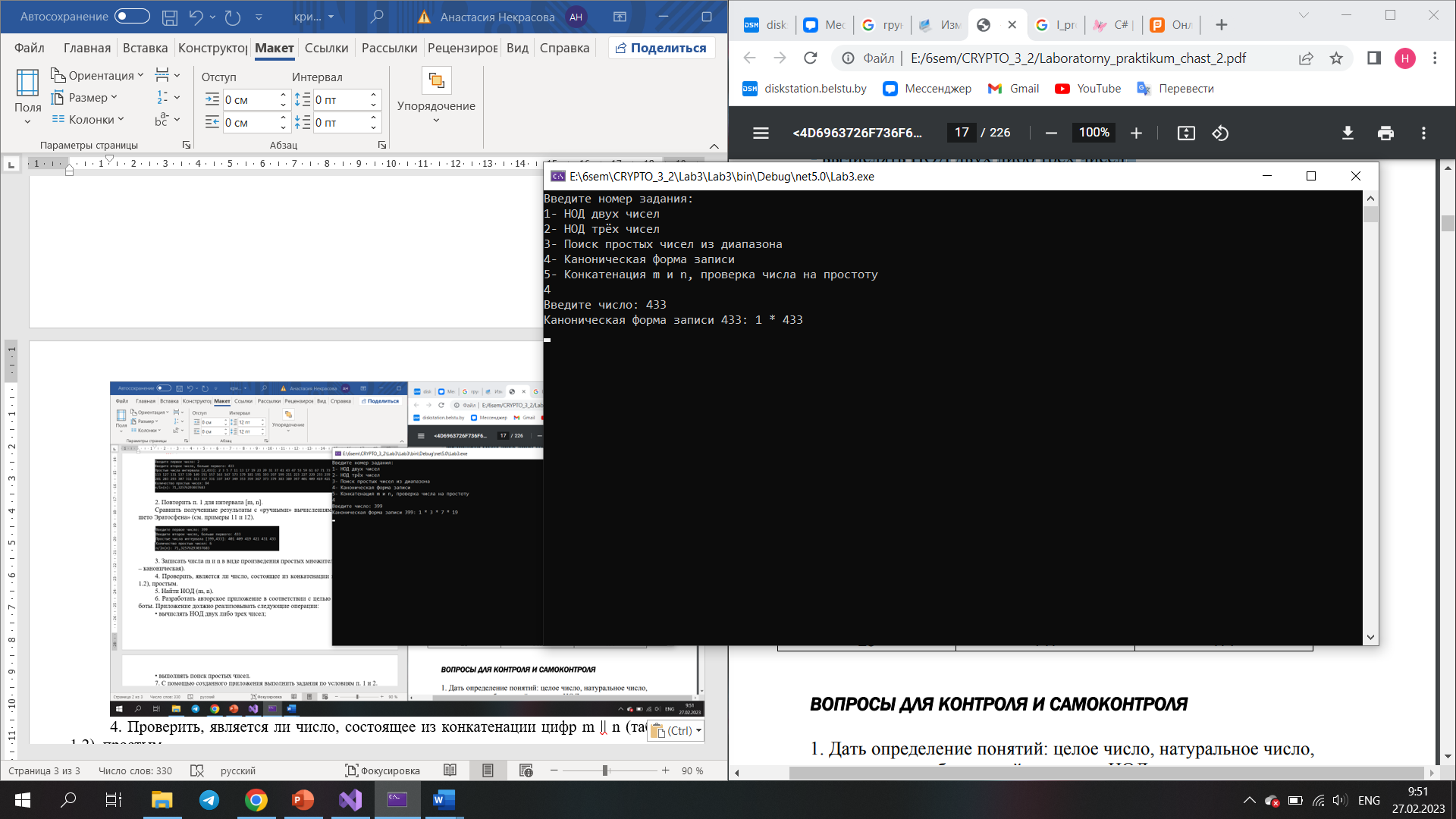


Рис.4 – Каноническая форма записи числа

4. Проверить, является ли число, состоящее из конкатенации цифр *m* ǀǀ *n* простым.

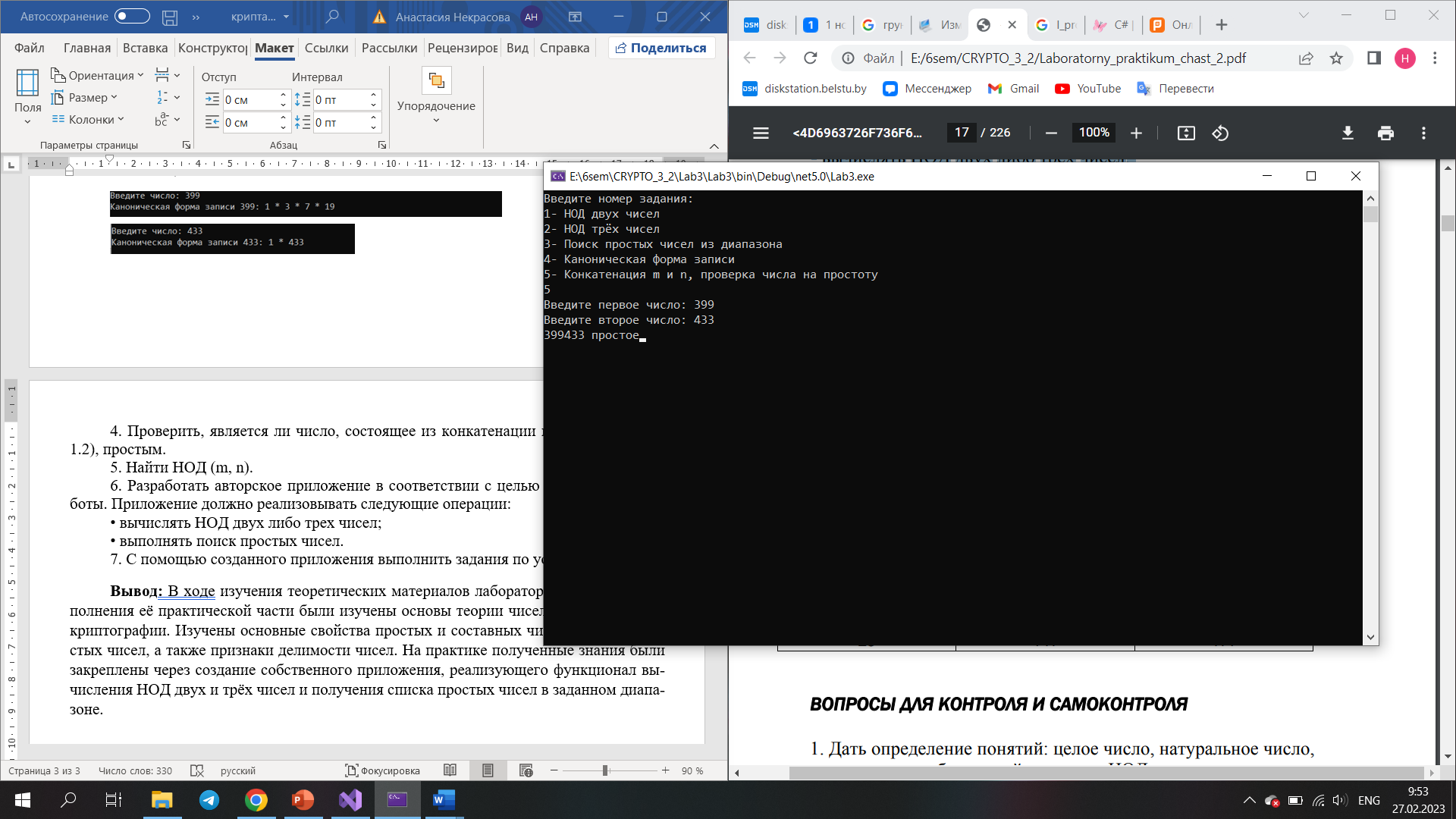


Рис.5 – Определение принадлежности числа к простому

1. Найти НОД (*m*, *n*).

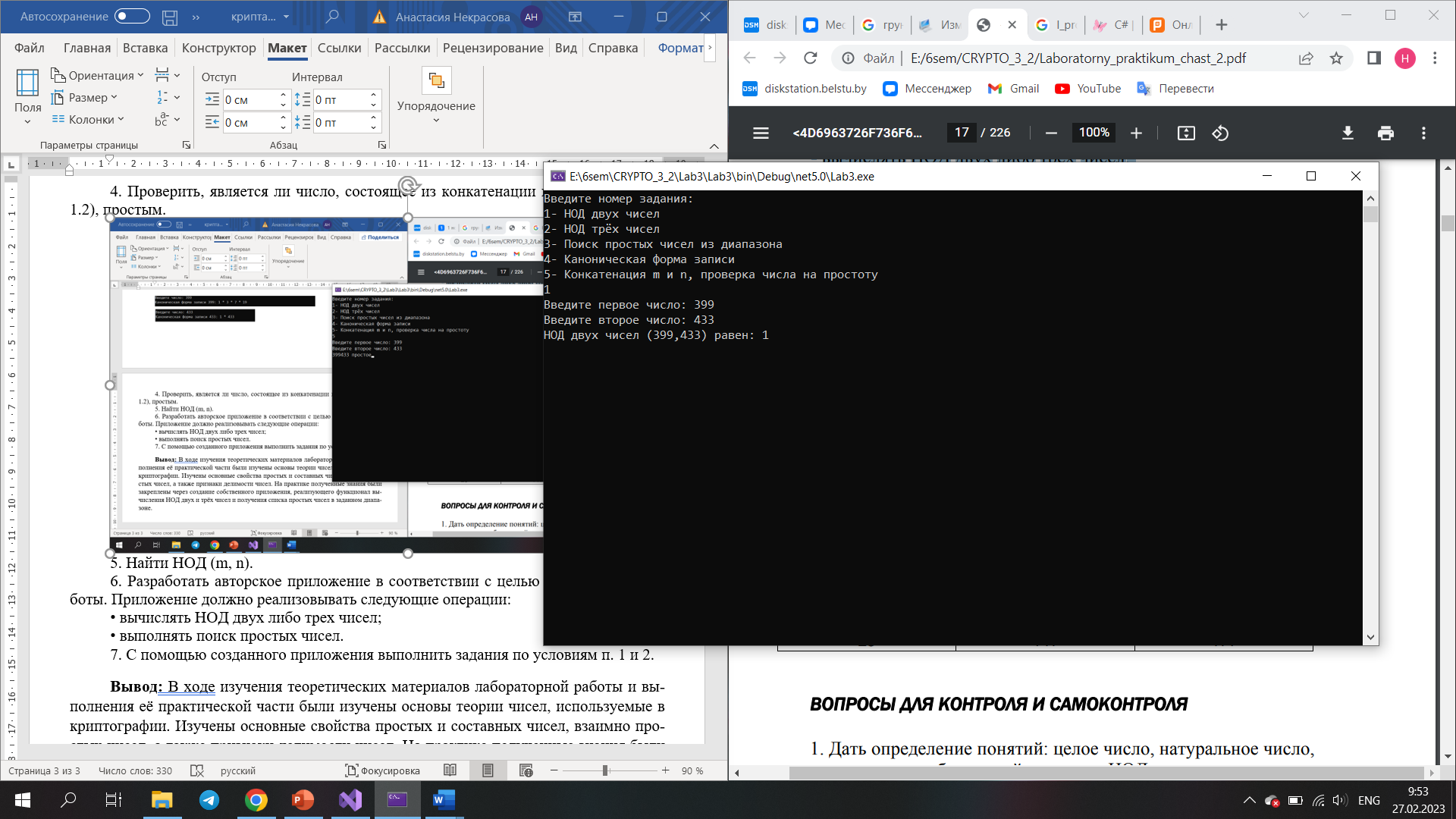


Рис.6 – Нахождение НОД чисел

6. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

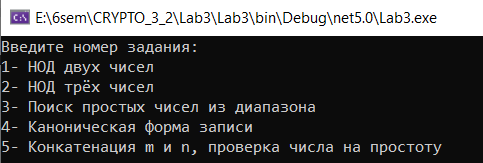


Рис.7 – Реализация интерфейса программы

1. С помощью созданного приложения выполнить задания по условиям п. 1 и 2.

*Реализация функций*

static class MathFunctions

{

public static int NODCompute(int x, int y) // НАХОЖДЕНИЕ НОД ЧИСЛА

{

while (x != 0 && y != 0)

{

if (x > y)

{

x -= y;

}

else

{

y -= x;

}

}

return Math.Max(x, y);

}

public static bool IsSimple(int x)

{

for (int i = 2; Math.Pow(i, 2) <= x; i++)

{

if (x % i == 0)

{

return false;

}

}

return true;

}

public static int FindSimple(int m, int n) // ПОДСЧЕТ ПРОСТЫХ ЧИСЕЛ В ДИАПАЗОНЕ

{

int counter = 0;

if (n < m)

{

Console.WriteLine("Неверный промежуток");

}

Console.Write($"Простые числа интервала [{m},{n}]: ");

for (int i = m; i <= n; i++)

{

if (IsSimple(i))

{

Console.Write(i.ToString() + " ");

counter++;

}

}

Console.WriteLine();

Console.WriteLine($"Количество простых чисел: {counter}");

return counter;

}

public static void CanonicalDecomposition(int x) // ЗАПИСЬ РАЗЛОЖЕНИЯ В КАНОНИЧЕСКУЮ ФОРМУ

{

string str = $"Каноническая форма записи {x}: 1";

for (int i = 0; x % 2 == 0; x /= 2)

{

str += " \* 2";

}

for (int i = 3; i <= x;)

{

if (x % i == 0)

{

str += " \* " + i.ToString();

x /= i;

}

else

{

i += 2;

}

}

Console.WriteLine(str);

}

}

Листинг 1 – Реализация класса MathFunctions

**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.