МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №12**

**ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ**

Выполнил:

Cтудент 3 курса 1 группы

Парибок И. А.

Вариант 5

Минск 2022

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

**Практическое задание:**

1.Найти все простые числа в интервале [2, *n*]. Значение n соответствует варианту из рисунка 2, указанному преподавателем.

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

2. Повторить п. 1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».

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

• вычислять НОД двух либо трех чисел;  
• выполнять поиск простых чисел

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

**Выполнение работы:**

Результаты выполнения заданий представлены в рисунках 2. Листинг программы изложен в приложении А.



Рисунок 1 – Варианты заданий

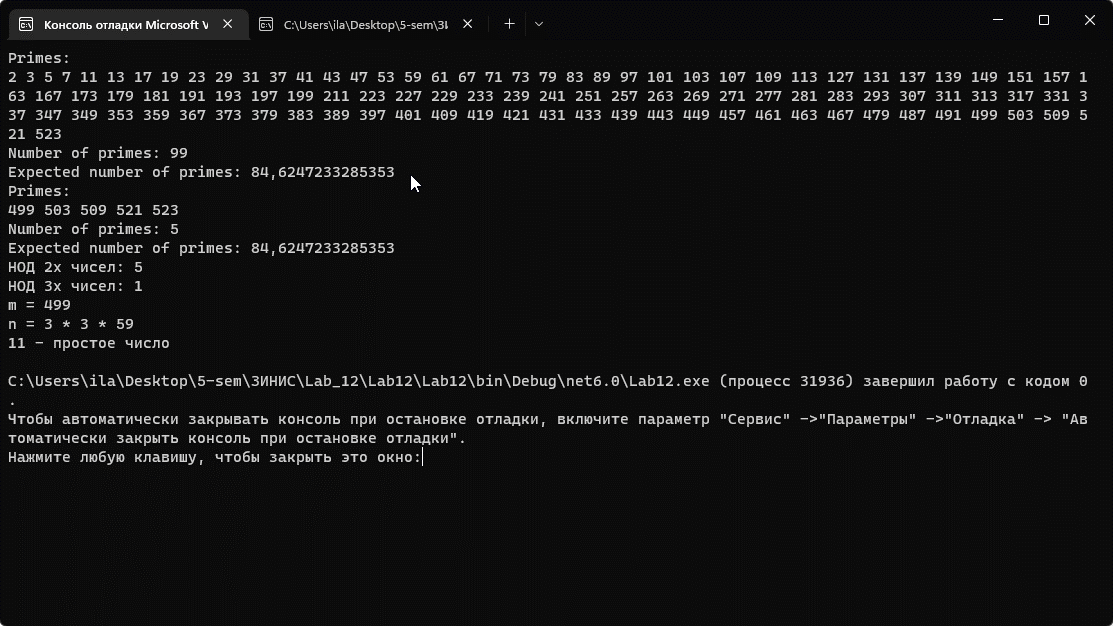


Рисунок 2 – Результат выполнения

**Вывод:** В результате выполнения работы были изучены принципы работы с простыми числами и разработано авторское приложение, которое умеет вычислять НОД двух либо трех чисел, а также выполнять поиск простых чисел.

В первом задании был найден интервал простых чисел [2, *n*] и посчитано их количество, которое было сравнено с *n*/ln(*n*). Во втором задании этот процесс был повторен для интервала [*m*, *n*].

С помощью разработанного приложения были выполнены задания по условиям первого и второго пункта, что позволило получить навыки работы с программным обеспечением для решения задач с простыми числами.

В заключении работы можно сделать вывод, что приобретение практических навыков работы с простыми числами является важным шагом в развитии навыков программирования и в понимании основ математики. Эти навыки могут быть полезны в различных областях, таких как криптография, алгоритмы и структуры данных. Разработанное приложение может быть использовано для автоматизации рутинных задач и упрощения работы с простыми числами.

**Приложение А**

int GCD(int a, int b)

{

while (a != 0 && b != 0)

{

if (a > b)

a %= b;

else

b %= a;

}

return a == 0 ? b : a;

}

int GCD\_third(int a, int b, int c)

{

return GCD(GCD(a, b), c);

}

List<int> FindPrimesInRange(int m, int n)

{

List<int> primes = new List<int>();

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

{

bool isPrime = true;

for (int j = 2; j < i; j++)

{

if (i % j == 0)

{

isPrime = false;

break;

}

}

if (isPrime)

primes.Add(i);

}

return primes;

}

void ComparePrimesInRange(int m, int n)

{

List<int> primes = FindPrimesInRange(m, n);

int numPrimes = primes.Count;

double expectedNumPrimes = n / Math.Log(n);

Console.WriteLine("Number of primes: " + numPrimes);

Console.WriteLine("Expected number of primes: " + expectedNumPrimes);

}

void PrintPrimes(List<int> primes)

{

Console.WriteLine("Primes: ");

foreach (int prime in primes)

{

Console.Write(prime + " ");

}

Console.WriteLine();

}

var ints = FindPrimesInRange(2,531);

PrintPrimes(ints);

ComparePrimesInRange(2, 531);

var ints2 = FindPrimesInRange(499, 531);

PrintPrimes(ints2);

ComparePrimesInRange(499, 531);

int gcd = GCD(10, 15);

int gcd\_third = GCD\_third(10, 15, 23);

Console.WriteLine("НОД 2х чисел: " + gcd);

Console.WriteLine("НОД 3х чисел: " + gcd\_third);