МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №12 НА ТЕМУ:**

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

Ф.И.О.

Качалкин Даниил Сергеевич

Минск 2022

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

**Теоретические сведения**

В основе современной криптографии лежит теория чисел. 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 наибольшего общего делителя (НОД), разложение числа на простые множители, малая теорема Ферма́, теорема Эйлера, элементы теории вычетов.

Простое число – если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным. Взаимно простые числа – целые числа, наибольший общий делитель которых равен 1.

Наибольший общий делитель двух и более натуральных чисел – это наибольшее из натуральных чисел, на которое делится каждое из данных чисел.

**Ход работы**

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

* Вычислять НОД двух или трех чисел
* Выполнять поиск простых чисел

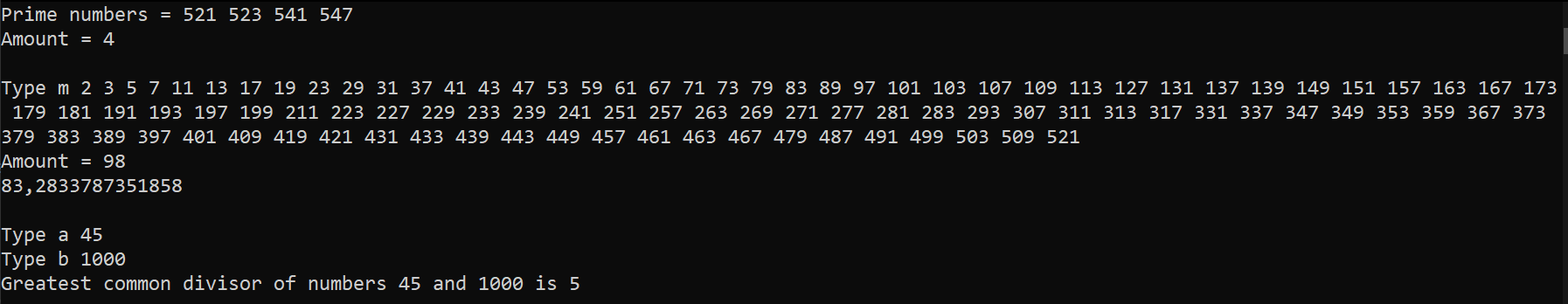
****

Рисунок 1 – Результат выполнения программы

|  |
| --- |
| using System;  namespace TwelvethLab  {  internal class Program  {  public static bool IsPrime(int number)  {  for (int i = 2; i < number; i++)  {  if (number % i == 0)  return false;  }  return true;  }  static int GCD(int a, int b)  {  while (b != 0)  {  var t = b;  b = a % b;  a = t;  }  return a;  }  static void Main(string[] args)  {  Console.Write("Prime numbers = ");  int count = 0;  for (int i = 521; i <= 553; i++)  {  if (IsPrime(i))  {  Console.Write($"{i} ");  count++;  }  }  Console.WriteLine("\nAmount = {0}",count);  Console.Write("\nType m ");  int count2 = 0;  for (int i = 2; i <= 521; i++)  {  if (IsPrime(i))  {  Console.Write($"{i} ");  count2++;  }  }  Console.WriteLine("\nAmount = {0}", count2);  double inter = 521/Math.Log(521);  Console.WriteLine(inter);  Console.Write("\nType a ");  int a = Convert.ToInt32(Console.ReadLine());  Console.Write("Type b ");  int b = Convert.ToInt32(Console.ReadLine());  Console.WriteLine("Greatest common divisor of numbers {0} and {1} is {2}",a,b,GCD(a,b));  Console.ReadLine();  }  }  } |

Листинг 1 – Код программы

**Вывод**: в данной работе были приобретены практические навыки выполнения операций с числами для решения задач в области криптографии, закреплены знания по общей арифметике и алгоритмам нахождения простых чисел и НОД.