МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №1

Основы теории чисел и их использование в криптографии

Выполнил студент: Плюто Э. В.

ФИТ 3 курса, 5 группа

Проверил: Савельева М. Г.

Минск 2024

**Практическое задание:**

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

Для вывода канонического разложения была написана функция, которая представлена на рисунке 1.

|  |
| --- |
| public static void Canon(int n)  {  Console.Write("Каноническое разложение " + n + ": ");  int i = 2;  while (n > 1)  {  if (n % i == 0)  {  Console.Write(i + " ");  n /= i;  i = 2;  }  else  i++;  }  Console.WriteLine();  } |

Листинг 1 – Реализация функции канонического разложения

Результат выполнения данной функции представлен ниже.



Рисунок 1 – Результат поиска простых чисел

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

Число называется простым, если оно не имеет делителей, кроме самого себя и единицы.

Для данного задания была реализована функция конкатенации цифр.

|  |
| --- |
| public static int Concat(int a, int b)  {  string astr = a.ToString();  string bstr = b.ToString();  return int.Parse(astr + bstr);  } |

Листинг 2 – Реализация функции конкатенации цифр

В результате выполнения получили, что конкатенация 555 и 591 не является простым числом.

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

• вычислять НОД двух чисел;

• выполнять поиск простых чисел.

Реализация функции для вычисления НОД двух чисел представлена на листинге 3.

|  |
| --- |
| public static int NOD(int a, int b)  {  int temp = int.MaxValue, max = Math.Max(a, b), min = Math.Min(a, b);  while (temp > 0)  {  temp = max % min;  max = min;  min = temp;  }  return max;  } |

Листинг 3 – Реализация функции расчета НОД

Реализация функции для проверки на простое число представлена на листинге 4.

|  |
| --- |
| public static bool IsPrime(int a)  {  for (int i = 2; i < a; i++)  {  if (a % i == 0)  return false;  }  return true;  } |

Листинг 4 – Реализация функции проверки на простое число

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

«Ручные» вычисления поиска простых чисел, используя «решето Эратосфена» представлены на рисунке 2.

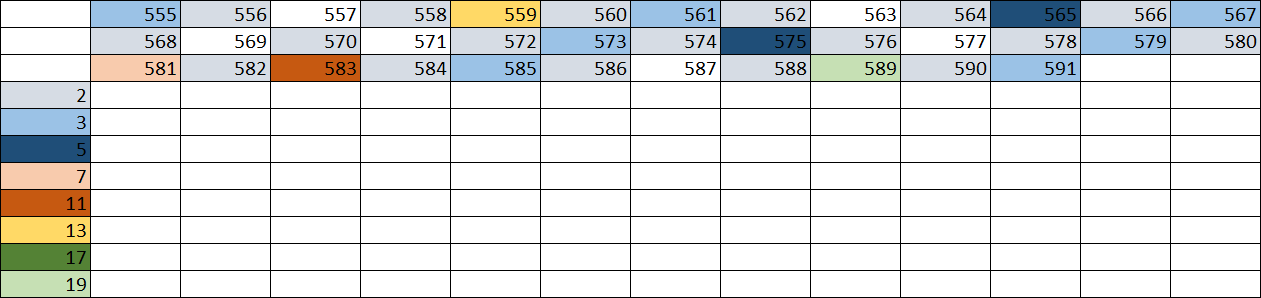


Рисунок 2 – «Решето Эратосфена»

Для выполнения использовались вышеописанные функции, результат выполнения представлен на рисунке 3.

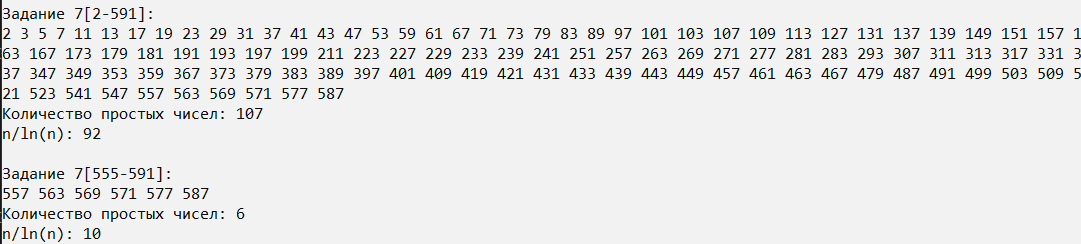


Рисунок 3 – Результат поиска простых чисел

**Вывод:**

Были приобретены практические навыки выполнения операций с числами для решения задач в области криптографии и разработки приложений для автоматизации этих операций. Был выполнен поиск простых чисел вручную и с помощью созданной программы.