Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №3»**

“ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Сапегина Екатерина Игоревна,

Вариант 11

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.

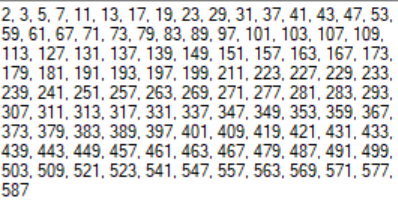
4. Разработать приложение для реализации указанных преподавателем операций с числами.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

***Практическая часть:***

***Задание 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).

**n = 591;**



Количество простых чисел в интервале [0,591]: 107.

591 / ln(591) = 92,6068690147249

***Задание 2.*** Повторить п. 1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена» (см. примеры 11 и 12).

m=555



Количество простых чисел в интервале [555,591]: 6.

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

n = 591

591 = 3 · 197

m =555

555 = 3 · 5 · 37

***Задание 4.*** Проверить, является ли число, состоящее из конкатенации цифр m ǀǀ n (табл. 1.2), простым.

***555591***

Для решения этого задания была разработана функция, которая проверяет остаток от деления числа 555591 на каждое число из промежутка [2, 555591].

|  |
| --- |
|  |

Число является составным (см. результат в конце).

***Задание 5.*** Найти НОД (555, 591).

*591 : 555 = 1 (остаток 36),* так как 591 = 555 ∙ 1 + 36, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 555 на 36  
*555 : 36 = 15 (остаток 15),*так как 555 = 36 ∙ 15 + 15, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 36 на 15  
*36 : 15 = 2 (остаток 6),* так как 36 = 15 ∙ 2 + 6, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 15 на 6  
*15 : 6 = 2 (****остаток 3****),* так как 15 = 6 ∙ 2 + 3, остаток от деления не равен нулю, поэтому продолжаем деление, разделим 6 на 3  
*6 : 3 = 2 (остаток 0),* так как 6 = 3 ∙ 2 + 0, равен нулю, значит НОД равен предыдущему остатку от деления

Ответ: НОД (591; 555) = 3

***Задание 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.

*Функции вычисляющие НОД для 2-х и 3-х чисел:*

|  |
| --- |
| public static int Evklid(int a, int b)  {  while (a != b)  {  if (a > b) a -= b;  else b -= a;  }  return a;  }  public static int Evklid\_3(int a, int b, int c)  {  return Evklid(Evklid(a, b), c);  } |

*Код выполняющий поиск простых чисел:*

|  |
| --- |
| while (a <= b)  {  if (funcForLab.IsPrimeNumber(a))  {  result = result + Convert.ToString(a) + ',';  countNum++;  }  a++;  } |

*Функция IsPrimeNumber проверяет является ли число простым.*

|  |
| --- |
| public static bool IsPrimeNumber(int n)  {  bool result = true;  if (n > 1)  {  for (int i = 2; i < n; i++)  {    if (n % i == 0)  {  result = false;  break;  }  }  }  else  {  result = false;  }  return result;  } |

***Задание 7.*** Результаты работы приложения:

