Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Основы теории чисел и их использование в криптографии»

Выполнил:

студент 3 курса 7 группы

специальности ПОИБМС

Кот И.В.

Минск 2020

1. Теоретические сведения.

В основе современной криптографии лежит теория чисел. Теория чисел или высшая арифметика–раздел математики, изучающий натуральные числа и иные похожие величины.

Определение1. Множество всех целых чисел (обозначим буквой Z) есть набор всех действительных чисел без дробной части: {..., -3, -2, -1, 0, 1, 2, 3, ...}.

Определение2. Натуральные числа являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

Определение3. Делимость–одно из основных понятий теории чисел.

Если для некоторого целого числами натурального числа b существует целое число q, такое, что bq=a, то говорят, что число a делится на b. В этом случае b называется делителем числа a, а a называется кратным числа b. При этом используются следующие обозначения: a⋮b – a делится на b или b|a – b делит a. Из последнего определения следует, что: •любое натуральное число является делителем нуля; •единица является делителем любого целого числа; •любое натуральное число является делителем самого себя.

Определение4. Делитель a называется собственным делителем числа b, если 1<|a|<|b|, и несобственным–в противном случае.Пример1.4|20; число 4делит число 20, так как 20= 4·5. При этом число 4является собственным делителем числа 20. Свойство1 собственного делителя. Положительный наименьший собственный делитель составного числа n не превосходит √n.Определение5. Всякое целое число аможнопредставитьспомощьюпо-ложительногоцелогочислаbравенствомвидаа = bq + r, 0 ≤r≤b. Число q называется неполным частным, а число r – остатком от деления, а на b.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным.

Определение6. Натуральное число n называется простым, если n> 1 и не имеет положительных делителей, отличных от 1 и n.

Наибольшее целое число, которое делит без остатка числа a и b называется наибольшим общим делителем этих чисел, НОД (a, b).

1. Постановка задачи

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 экспериментов с использованием приложения и результатов эксперимента.

1. Решение

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace Task\_1.\_0

{

public class PrimeNumbers

{

public static bool IsPrime(int x)

{

for (int i = 2; i <= x / i; i++)

if ((x % i) == 0) return false;

return true;

}

}

public class GCF

{

public static int GetGCF(int value1, int value2)

{

int b = 1;

int q = value1 < value2 ? value1 : value2;

int r = 1;

int a = value1 < value2 ? value2 : value1;

while (r > 0)

{

while (a - (b \* q) >= q)

{

b++;

}

r = a - (b \* q);

a = q;

q = r;

}

return a;

}

}

public class Program

{

public static int firstInRange=1;

public static int lastInRange=10;

static void Main(string[] args)

{

#region CheckPrime

Console.WriteLine($"Input range for search prime nubers: \nfirst in range: "); firstInRange = Convert.ToInt32(Console.ReadLine());

Console.WriteLine($"last in range: "); lastInRange = Convert.ToInt32(Console.ReadLine());

for (int i = firstInRange; i < lastInRange; i++)

if (PrimeNumbers.IsPrime(i))

Console.Write(i +" ");

Console.WriteLine();

#endregion

#region GCF

Console.WriteLine("greatest common factor for 2 numbers: \nInput numbers: ");

int gcfTwo = GCF.GetGCF(Convert.ToInt32(Console.ReadLine()), Convert.ToInt32(Console.ReadLine()));

Console.WriteLine("GCF = " + gcfTwo);

Console.WriteLine("greatest common factor for 3 numbers: \nInput numbers: ");

int gcfThree = GCF.GetGCF(GCF.GetGCF(Convert.ToInt32(Console.ReadLine()), Convert.ToInt32(Console.ReadLine())), Convert.ToInt32(Console.ReadLine()));

Console.WriteLine("GCF = " + gcfThree);

#endregion

}

}

}

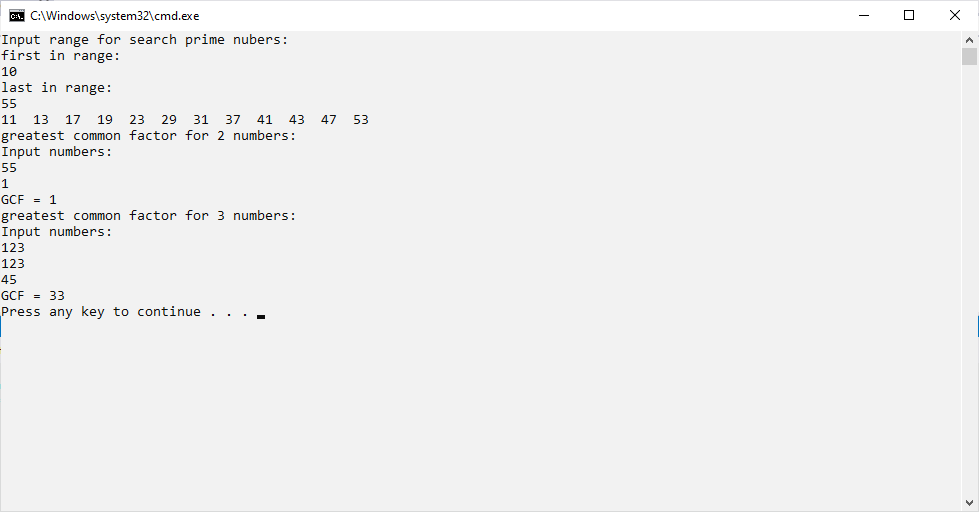


Рисунок 3.1 Пример работы программы

Вывод

Приобрел практические навыки по использованию операций с числами для решения задач в области криптографии, изучил модульную арифметику.

Также создал консольное приложения для демонстрации работы ­ нахождения простых чисел и НОД.