

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

Лабораторная работа №3

по дисциплине: «Теоретико-числовые методы в криптографии»

на тему: «Сравнение первой степени»

Выполнил обучающийся гр. ВКБ42

Михайлов Александр Сергеевич

          Проверила:

Ст. пр. Артамонова Е.А.

Ростов-на-Дону

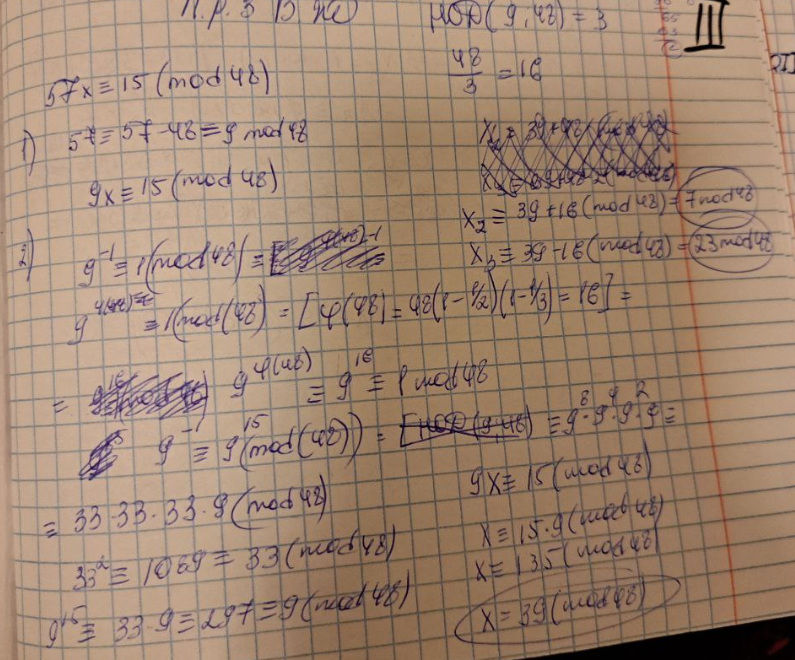
2024

Лабораторная работа №3

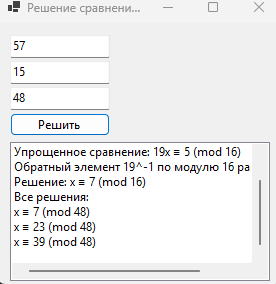
«Остаток от деления»

Вариант №20

**Ручная реализация.**



**Входные данные.**



**Листинг программы.**

using System.Windows.Forms;

namespace Эйлерпервойстепени

{

public partial class Form1 : Form

{

private TextBox textBox1;

private TextBox textBox2;

private TextBox textBox3;

private Button button1;

private ListBox listBox1;

public Form1()

{

InitializeComponent();

this.textBox1 = new System.Windows.Forms.TextBox();

this.textBox2 = new System.Windows.Forms.TextBox();

this.textBox3 = new System.Windows.Forms.TextBox();

this.button1 = new System.Windows.Forms.Button();

this.listBox1 = new System.Windows.Forms.ListBox();

this.SuspendLayout();

//

// textBox1

//

this.textBox1.Location = new System.Drawing.Point(12, 12);

this.textBox1.Name = "textBox1";

this.textBox1.Size = new System.Drawing.Size(100, 20);

this.textBox1.TabIndex = 0;

this.textBox1.Text = "10"; // Пример значения

//

// textBox2

//

this.textBox2.Location = new System.Drawing.Point(12, 38);

this.textBox2.Name = "textBox2";

this.textBox2.Size = new System.Drawing.Size(100, 20);

this.textBox2.TabIndex = 1;

this.textBox2.Text = "12"; // Пример значения

//

// textBox3

//

this.textBox3.Location = new System.Drawing.Point(12, 64);

this.textBox3.Name = "textBox3";

this.textBox3.Size = new System.Drawing.Size(100, 20);

this.textBox3.TabIndex = 2;

this.textBox3.Text = "14"; // Пример значения

//

// button1

//

this.button1.Location = new System.Drawing.Point(12, 90);

this.button1.Name = "button1";

this.button1.Size = new System.Drawing.Size(100, 23);

this.button1.TabIndex = 3;

this.button1.Text = "Решить";

this.button1.UseVisualStyleBackColor = true;

this.button1.Click += new System.EventHandler(this.button1\_Click);

//

// listBox1

//

this.listBox1.FormattingEnabled = true;

this.listBox1.Location = new System.Drawing.Point(12, 119);

this.listBox1.Name = "listBox1";

this.listBox1.Size = new System.Drawing.Size(260, 147);

this.listBox1.TabIndex = 4;

this.listBox1.HorizontalScrollbar = true;

//

// Form1

//

this.ClientSize = new System.Drawing.Size(284, 261);

this.Controls.Add(this.listBox1);

this.Controls.Add(this.button1);

this.Controls.Add(this.textBox3);

this.Controls.Add(this.textBox2);

this.Controls.Add(this.textBox1);

this.Name = "Form1";

this.Text = "Решение сравнения первой степени";

this.ResumeLayout(false);

this.PerformLayout();

}

private void button1\_Click(object sender, EventArgs e)

{

listBox1.Items.Clear();

int a = int.Parse(textBox1.Text);

int b = int.Parse(textBox2.Text);

int m = int.Parse(textBox3.Text);

listBox1.Items.Add($"Исходное сравнение: {a}x ≡ {b} (mod {m})");

int gcd = GCD(a, m);

listBox1.Items.Add($"gcd({a}, {m}) = {gcd}");

if (b % gcd != 0)

{

listBox1.Items.Add("Решение не существует, так как gcd не делит b.");

return;

}

int aPrime = a / gcd;

int bPrime = b / gcd;

int mPrime = m / gcd;

listBox1.Items.Add($"Упрощенное сравнение: {aPrime}x ≡ {bPrime} (mod {mPrime})");

int inverse = ModInverse(aPrime, mPrime);

if (inverse == -1)

{

listBox1.Items.Add("Обратный элемент не найден.");

return;

}

listBox1.Items.Add($"Обратный элемент {aPrime}^-1 по модулю {mPrime} равен {inverse}");

int x = (bPrime \* inverse) % mPrime;

if (x < 0) x += mPrime; // Убеждаемся, что x неотрицательно

listBox1.Items.Add($"Решение: x ≡ {x} (mod {mPrime})");

listBox1.Items.Add("Все решения:");

for (int k = 0; k < gcd; k++)

{

int solution = x + k \* mPrime;

listBox1.Items.Add($"x ≡ {solution} (mod {m})");

}

}

private int GCD(int a, int b)

{

while (b != 0)

{

int temp = b;

b = a % b;

a = temp;

}

return a;

}

private int ModInverse(int a, int m)

{

int m0 = m, t, q;

int x0 = 0, x1 = 1;

if (m == 1)

return 0;

while (a > 1)

{

q = a / m;

t = m;

m = a % m;

a = t;

t = x0;

x0 = x1 - q \* x0;

x1 = t;

}

if (x1 < 0)

x1 += m0;

return x1;

}

}

}

**Вывод по работе:**

В ходе выполнения лабораторной работы были изучены лекционный материал и алгоритм для решения сравнений первой степени.