

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 №1

по дисциплине: «Теоретико-числовые методы в криптографии»

на тему: «алгоритм Евклида»

Выполнил обучающийся гр. ВКБ42

Михайлов Александр Сергеевич

          Проверила:

Ст. пр. Артамонова Е.А.

Ростов-на-Дону

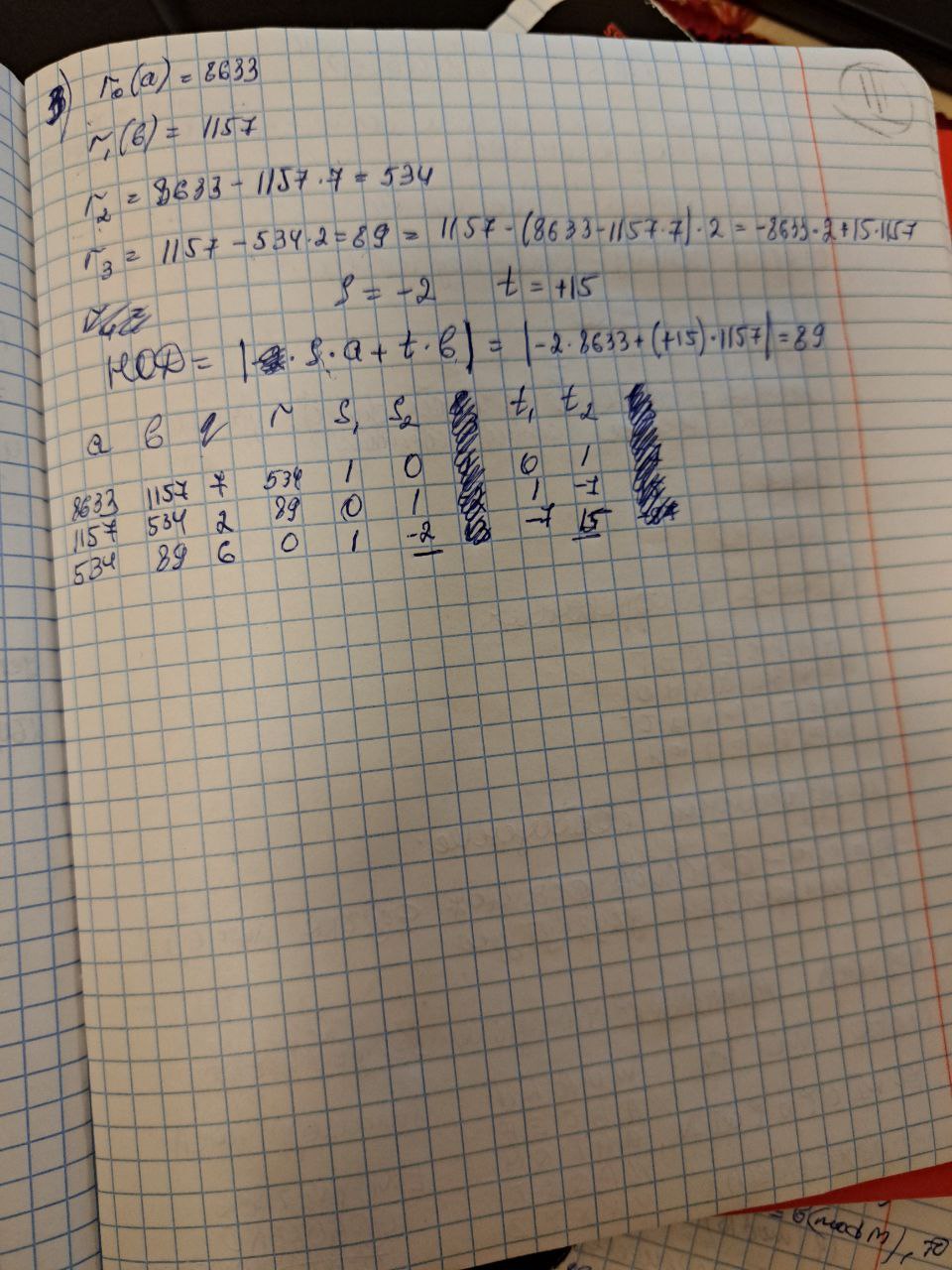
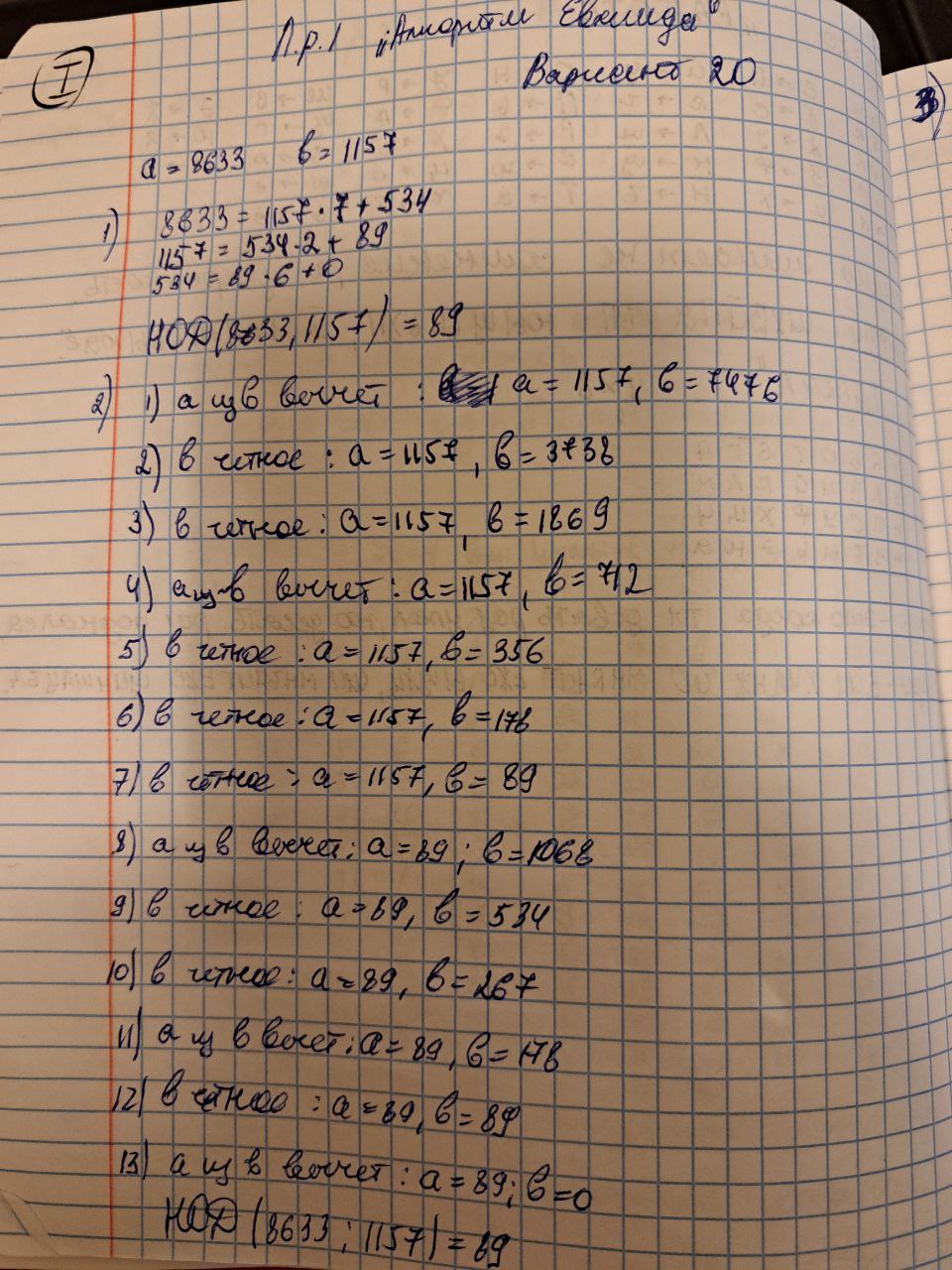
2024

Лабораторная работа №1

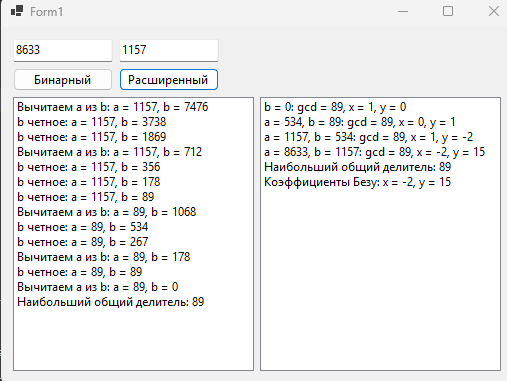
«алгоритм Евклида»

Вариант №20

**Ручная реализация.**



**Входные данные.**



**Листинг программы.**

namespace WinFormsApp1

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

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

{

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

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

int gcd = BinaryGCD(a, b);

listBox1.Items.Add($"Наибольший общий делитель: {gcd}");

}

private int BinaryGCD(int a, int b)

{

if (a == 0) return b;

if (b == 0) return a;

int shift = 0;

while (((a | b) & 1) == 0)

{

a >>= 1;

b >>= 1;

shift++;

listBox1.Items.Add($"Оба числа четные: a = {a}, b = {b}, shift = {shift}");

}

while ((a & 1) == 0)

{

a >>= 1;

listBox1.Items.Add($"a четное: a = {a}, b = {b}");

}

do

{

while ((b & 1) == 0)

{

b >>= 1;

listBox1.Items.Add($"b четное: a = {a}, b = {b}");

}

if (a > b)

{

int temp = a;

a = b;

b = temp;

}

b -= a;

listBox1.Items.Add($"Вычитаем a из b: a = {a}, b = {b}");

} while (b != 0);

return a << shift;

}

private void button2\_Click(object sender, EventArgs e)

{

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

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

int gcd, x, y;

ExtendedGCD(a, b, out gcd, out x, out y);

listBox2.Items.Add($"Наибольший общий делитель: {gcd}");

listBox2.Items.Add($"Коэффициенты Безу: x = {x}, y = {y}");

}

private void ExtendedGCD(int a, int b, out int gcd, out int x, out int y)

{

if (b == 0)

{

gcd = a;

x = 1;

y = 0;

listBox2.Items.Add($"b = 0: gcd = {gcd}, x = {x}, y = {y}");

return;

}

int x1, y1;

ExtendedGCD(b, a % b, out gcd, out x1, out y1);

x = y1;

y = x1 - (a / b) \* y1;

listBox2.Items.Add($"a = {a}, b = {b}: gcd = {gcd}, x = {x}, y = {y}");

}

**Вывод по работе:**

В процессе выполнения лабораторной работы были рассмотрены лекционные материалы, а также алгоритмы нахождения наибольшего общего делителя и наименьшего общего кратного с использованием алгоритма Евклида.