Казанский (Приволжский) Федеральный университет

Институт Вычислительной математики и информационных технологий

**Отчёт лаб. задания № 2 «Вычисления в конечных полях».**

Студент 09-641

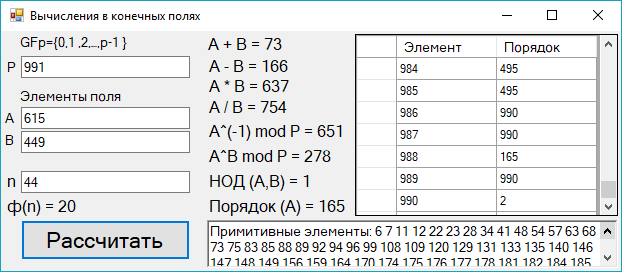
Десятов Александр

Казань – 2018

**Описание программы.**

Цель программы – вычисления в конечном поле простое число. Программа выполняет сложение, вычитание, умножение, вычисление обратного по модулю p, деление и возведение в целую степень элементов поля. В программе реализованы алгоритмы быстрого возведения в степень, алгоритм Евклида вычисления НОД целых чисел, расширенный алгоритм Евклида. Также программа находит порядки элементов поля, примитивные элементы поля и вычисляет функцию Эйлера

**Скриншот программы.**



**Код программы.**

using System;

using System.Collections.Generic;

using System.Windows.Forms;

namespace Вычисления\_в\_конечных\_полях

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

private void button\_Calc\_Click(object sender, EventArgs e)

{

int P = Convert.ToInt32(textBox\_P.Text);

if (prostoe(P))

{

int A = Convert.ToInt32(textBox\_A.Text);

int B = Convert.ToInt32(textBox\_B.Text);

int n = Convert.ToInt32(textBox\_n.Text);

int res = 0;

// A+B

res = ( A + B ) % P;

label\_plus.Text = "A + B = " + res;

// A-B

res = ( A - B ) % P;

if (res < 0)

res += P;

label\_minus.Text = "A - B = " + res;

// A\*B

res = ( A \* B ) % P;

if (res < 0)

res += P;

label\_ymnoz.Text = "A \* B = " + res;

// A/B

res = ( A \* find\_obr\_element(B, P) ) % P;

if (res < 0)

res += P;

label\_del.Text = "A / B = " + res;

// A^(-1)

res = find\_obr\_element(A, P);

if (res < 0)

res += P;

label\_obr\_A.Text = "A^(-1) mod P = " + res;

// A^(B)

res = step(A, B, P);

if (res < 0)

res += P;

label\_step.Text = "A^B mod P = " + res;

// НОД (A,B)

res = nod(A, B);

label\_nod.Text = "НОД (A,B) = " + res;

// Порядок A - элемента поля

res = poryadok(A, P);

label\_por.Text = "Порядок (A) = " + res;

// Функция Эйлера ф(n) =

res = eyler(n);

label\_f\_n.Text = "ф(n) = " + res;

// Примитивные элементы поля

richTextBox\_primit.Text = "Примитивные элементы: " + primit(P);

}

else

{

MessageBox.Show("P должно быть простым числом");

}

}

private int find\_obr\_element(int A, int P)

{

int i = 0;

Stack<int> celaya = new Stack<int>();

for(int temp = P % A; temp > 0; i++)

{

celaya.Push(P / A);

P = A;

A = temp;

temp = P % A;

}

int y = 1;

for(int temp, x = 0; i > 0; i--)

{

temp = x;

x = y;

y = temp - y \* celaya.Pop();

}

return y;

}

private int step(int A, int B, int P)

{

Stack<bool> bin = new Stack<bool>();

while( B > 1)

{

bool temp = B % 2 == 1;

bin.Push(temp);

B /= 2;

}

int x = A;

while(bin.Count > 0)

{

if (bin.Pop())

x = ( x \* x \* A ) % P;

else

x = ( x \* x ) % P;

}

return x;

}

private int nod(int A, int B)

{

while(A != B)

{

if (A > B)

A -= B;

else

B -= A;

}

return A;

}

private int eyler(int n)

{

int res = 0;

for(int i = 1; i < n; i++)

if (nod(i, n) == 1)

res++;

return res;

}

private int poryadok(int A, int P)

{

int res = 1;

while (step(A, res, P) != 1)

res++;

return res;

}

private string primit(int P)

{

dataGridView\_por\_primit.Rows.Clear();

dataGridView\_por\_primit.Columns.Clear();

dataGridView\_por\_primit.Columns.Add("", "Элемент");

dataGridView\_por\_primit.Columns.Add("", "Порядок");

int max\_por = 1;

for(int i = 0; i < P-1; i++)

{

int por = poryadok(i+1, P);

if (max\_por < por)

max\_por = por;

dataGridView\_por\_primit.Rows.Add("", "");

dataGridView\_por\_primit.Rows[i].Cells[0].Value = (i+1).ToString();

dataGridView\_por\_primit.Rows[i].Cells[1].Value = por;

}

string elementi = "";

for (int i = 0; i < P-1; i++)

{

int por = Convert.ToInt32(dataGridView\_por\_primit.Rows [i].Cells [1].Value);

int el = Convert.ToInt32(dataGridView\_por\_primit.Rows [i].Cells [0].Value);

if (por == max\_por)

elementi += el + " ";

}

return elementi;

}

private bool prostoe(int P)

{

for(int i = 2; i <= Math.Sqrt(P); i++)

{

if (P % i == 0)

return false;

}

return true;

}

}

}