Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

# Национальный исследовательский университет «МЭИ»

Кафедра Вычислительных машин, систем и сетей

**Лабораторная работа №11(ч.1)**

**по курсу «Методы и средства передачи информации»**

Задание выполнил: Винокуров Р.Н.

Студент группы А-12-19

Проверил: Оцоков Ш.А.

Оценка: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2021 НИУ «МЭИ»

**Задание**

Задание 1.

Написать программу для умножения двух полиномов над полем Zp. В программу вводится простое число p. Полиномы задаются коэффициентами и степенью. Например, p=2,

1-й полином: x+1,

2-й полином: x+1,

результат: x^2+1.

Задание 2.

На примере разложения двучлена x15+1 над полем GF(2), построенному по модулю p(x) = x4+x+1. Проверить, а) что сопряженные элементы поля α, α2, α4, α8, соответствуют минимальному многочлену x4+x+1.

б) что сопряженные элементы поля α3, α6, α9, α12, соответствуют минимальному многочлену x4+x3+x2+x+1

в) что сопряженные элементы поля α5, α10 x2+x+1

**Описание результатов**

Для задания 1:

|  |  |  |  |
| --- | --- | --- | --- |
| № теста | Смысл теста | Вводные значения | Вывод |
| 1 | Размерность поля – не простое число. | Размерность поля, в котором умножаются полиномы: 6. | «Данное множество не является полем, повторите ввод!» |
| 2 | Умножаемые полиномы нулевые. | Размерность поля, в котором умножаются полиномы: 2. Степень первого полинома: 0. Индекс при x^0: 0. Введите степень второго полинома: 0. Индекс при x^0: 0. | «Произведение полиномов в поле: 0» |
| 3 | Размерность поля отлична от двух. | Размерность поля, в котором умножаются полиномы: 7. Степень первого полинома: 2. Индекс при x^0: 3. Индекс при x^1: 4. Индекс при x^2: 5. Введите степень второго полинома: 1. Индекс при x^0: 1. Индекс при x^1: 2. | «Произведение полиномов в поле: 3x^3+6x^2+3x+3» |
| 4 | Умножаемые полиномы нулевой степени. | Размерность поля, в котором умножаются полиномы: 7. Степень первого полинома: 0. Индекс при x^0: 2. Степень первого полинома: 0. Индекс при x^0: 3. | «Произведение полиномов в поле: 6» |
| 5 | Размерность поля равна 2. | Размерность поля, в котором умножаются полиномы: 2. Степень первого полинома: 1. Индекс при x^0: 1. Индекс при x^1: 1. Введите степень второго полинома: 1. Индекс при x^0: 1. Индекс при x^1: 1. | «Произведение полиномов в поле: 1x^2+1» |

Для задания 2:

Заметим, что .

Тогда справедливо разложение:

Т.к. :

Найдем элементы данного поля:

Введем обозначение .

Тогда:

Найдем первые 4 множителя полученного произведения:

Таким образом,

Запишем сопряженные элементы поля и их минимальные многочлены в таблицу:

|  |  |
| --- | --- |
| Сопряженные элементы поля | Минимальный многочлен |
| 1 |  |
|  |  |
|  |  |
|  |  |

**Текст программы**

#include <iostream>

#include <math.h>

#include <windows.h>

#include <stdio.h>

using namespace std;

bool prime\_number(int a)

{

int m = 1;

for(int i = 2;i<a;i++)

m\*=(a % i);

return (m==0) ? false : true;

}

int main()

{

SetConsoleCP(1251);

SetConsoleOutputCP(1251);

int razm,por1,por2;

do

{

cout<<"Введите размерность поля, в котором умножаются полиномы: "<<endl;

cin>>razm;

if(!prime\_number(razm))

cout<<"Данное множество не является полем, повторите ввод!"<<endl;

}while(!prime\_number(razm));

cout<<"Введите степень первого полинома: "<<endl;

cin>>por1;

int pol1[por1+1];

for(int i = 0;i<=por1;i++)

{

cout<<"Введите индекс при x^"<<i<<":"<<endl;

cin>>pol1[i];

}

cout<<"Введите степень второго полинома: "<<endl;

cin>>por2;

int pol2[por2+1];

for(int i = 0;i<=por2;i++)

{

cout<<"Введите индекс при x^"<<i<<":"<<endl;

cin>>pol2[i];

}

int comp[por1+por2+1];

for(int i = 0;i<por1+por2+1;i++)

comp[i]=0;

for(int l = 0;l<por1+por2+1;l++)

{

for(int i = 0;i<=por1;i++)

for(int j = 0;j<=por2;j++)

if(i+j==l) comp[l]+=pol1[i]\*pol2[j];

}

cout<<"Произведение полиномов в поле:"<<endl;

int j = 0;

for(int i = por1+por2;i>1;i--)

if((comp[i] % razm)!=0 && ++j)

cout<<(comp[i] % razm)<<"x^"<<i<<"+";

if((comp[1] % razm)!=0 && ++j)

cout<<(comp[1] % razm)<<"x+";

if((comp[0] % razm)!=0 && ++j)

cout<<(comp[0] % razm);

else

{

putchar('\b');

putchar(' ');

putchar('\b');

}

if(j==0)

cout<<"0";

return 0;

}

**Выводы**

В ходе выполнения данной лабораторной работы мы ознакомились с таким математическим объектом, как конечные поля, а также с его свойствами, реализовали алгоритм перемножения многочленов в поле на языке C++.