Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчёт**

**по лабораторной работе №4**

**Дисциплина: КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ**

**Тема: «ПОЛЯ ГАЛУА»**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Корнилов

Направление подготовки 02.03.02 Фундаментальная информатика и

информационные технологии

Направленность (профиль) Математическое и программное обеспечение

компьютерных технологий

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. А. Крамаренко

**Тема:** Поля Галуа.

**Цель:** Изучение свойств полей Галуа и цикломатических классов.

**Ход работы:**

1. Выделить циклотомические классы и найти соответствующие им минимальные многочлены для поля GF(16) для образующего многочлена 11001.

Для решения данной задачи воспользуемся определением цикломатического класса: С\_n = {s, sp, sp^2, … sp^(m-1)}, где m – степень образующего многочлена.

Тогда: C\_0 = {0}

C\_1 = {1,2,4,8} => x,x^2,x^4,x^8=x^3+x^2+x

C\_3 = {3,6,12,9} => x^3, x^6 = x^3+x^2+x+1, x^9 = x^2 + 1, x^12 = x + 1

C\_5 = {5,10} => x^5 = x^3 + x + 1, x^10 = x^3 + x

C\_7 = {7, 14, 13, 11} => x^7 = x^2+x+1, x^14=x^3+x^2, x^13=x^2+x, x^11=x^3+x^2+1

Тогда минимальные многочлены выглядят так:

M(g)=0

M1(g)=(g+x^3+x^2+x)(g+x)(g+x^2)(g+x^3+1) M3(g)=(g+x^2+1)(g+x^3)(g+x+1)(g+x^3+x^2+x+1) M5(g)=(g+x^3+x)(g+x^3+x+1)

M7(g)=(g+x^3+x^2+1)(g+x^2+x)(g+x^3+x^2)(g+x^2+x+1)

1. Выделить циклотомические классы и найти соответствующие им минимальные многочлены для поля GF(16) для образующего многочлена 10011.

Тогда: C\_0 = {0}

C\_1 = {1,2,4,8} => x,x^2,x+1,x^2+1

C\_3 = {3,6,12,9} => x^3, x^3+x^2, x^3+x^2+x+1, x^3+x

C\_5 = {5,10} => x^2+x, x^2+x+1

C\_7 = {7, 14, 13, 11} => x^3+x+1, x^3+1, x^3+x^2+1, x^3+x^2+x

Тогда минимальные многочлены выглядят так:

M(g)=0

M1(g)=(g+x^2+1)(g+x)(g+x^2)(g+x+1)

M3(g)=(g+x^3+x)(g+x^3)(g+x^3+x^2+x+1)(g+x^3+x^2) M5(g)=(g+x^2+x+1)(g+x^2+x) M7(g)=(g+x^3+x^2+x)(g+x^3+x^2+1)(g+x^3+1)(g+x^3+x+1)

1. Для многочлена х над полем GF (2^5) с образующим многочленом x^5+x^2+1 найти циклотомический класс и минимальный многочлен.

X = a^1 => C = {1,2,4,8,16} => x, x^2, x^4, x^3+x^2+1, x^4+x^3+x+1

M1(g) = (g+x)(g+x^2)(g+x^4)(g+x^3+x^2+1)(g+x^4+x^3+x+1)

1. Для многочлена х^3 над полем GF (2^5) с образующим многочленом x^5+x^2+1 найти циклотомический класс и минимальный многочлен.

X = a^3 => C = {3,6,12,24,17} => x^3, x^3+x, x^3+x^2+x, x^4+x^3+x^2+x, x^4+x+1

M3(g) = (g+x^3)(g+x^3+x)(g+x^3+x^2+x)(g+x^4+x^3+x^2+x)(g+x^4+x+1)

1. Для многочлена х^5 над полем GF (2^5) с образующим многочленом x^5+x^2+1 найти циклотомический класс и минимальный многочлен.

X = a^5 => C = {5, 10, 20, 9, 18 } => x^2+1, x^4+1, x^3+x^2, x^4+x^3+x, x+1

M5(g) = (g+x^2+1)(g+x^4+1)(g+x^3+x^2)(g+x^4+x^3+x)(g+x+1)

1. Для многочлена х^7 над полем GF (2^5) с образующим многочленом x^5+x^2+1 найти циклотомический класс и минимальный многочлен.

X = a^7 => C = {7,14,28,25,19} => x^4+x^2, x^4+x^3+x^2+1, x^4+x^2+x, x^4+x^3+1, x^2+x

M3(g) = (g+x^4+x^2) (g+x^4+x^3+x^2+1) (g+x^4+x^2+x) (g+x^4+x^3+1) (g+x^2+x)

1. Построить циклотомические классы и минимальные многочлены в поле Галуа x^5+x^3+1

M\_0 = 0

C\_1 = {1,2,4,8,16} => M\_1(g) = (g+x)(g+x^2)(g+x^4)(g+x^4+x^3+x)(g+x^3+x^2)

C\_3 = {3,6,12,24,17} => M\_3(g) = (g+x^3) (g+x^4+x) (g+x^4+x^3+x^2+x) (g+x^4+x^3+x^2) (g+x^4\_x^3)

C\_5 = {5,10,20,9,18} => M\_5(g) = (g+x^3+1) (g+x^4+x+1) (g+x^4+x^3+x^2+x+1) (g+x^4+x^3+x^2+1) (g+x^4+x^3+1)

C\_7 = {7,14,28,25,19} => M\_7(g) = (g+x^3+x^2+1) (g+x+1) (g+x^2+1) (g+x^4+1) (g+x^4+x^3+x+1)

C\_11 = {11, 22, 13, 26, 21} => M\_11(g) = (g+x^3+x^2+x+1) (g+x^2+x+1) (g+x^4+x^2+1) (g+x^3+x+1) (g+x^4+x^2+x+1)

C\_15 = {15,30,29,27,23} => M\_15(g) = (g+x^2+x) (g+x^4+x^2) (g+x^3+x) (g+x^4+x^2+x) (g+x^3+x^2+x)

1. Построить циклотомические классы и минимальные многочлены в поле Галуа x^5+x^3+x^2+x+1

M\_0 = 0

C\_1 = {1,2,4,8,16} => M\_1(g) = (g+x) (g+x^2) (g+x^4) (g+x^3+1) (g+x^4+x^3+x^2+x+1)

C\_3 = {3,6,12,24,17} => M\_3(g) = (g+x^3) (g+x^4+x^3+x^2+x) (g+x+1) (g+x^2+1) (g+x^4+1)

C\_5 = {5,10,20,9,18} => M\_5(g) = (g+x^3+x^2+x+1) (g+x^3+x+1) (g+x^4+x^3+x+1) (g+x^4+x) (g+x^3+x^2+1)

C\_7 = {7,14,28,25,19} => M\_7(g) = (g+x^4+x+1) (g+x^3+x^2) (g+x^3+x^2+x) (g+x^3+x) (g+x^4+x^3+x)

C\_11 = {11, 22, 13, 26, 21} => M\_11(g) = (g+x^4+x^2+x) (g+x^4+x^3+x^2+x+1) (g+x^2+x) (g+x^4+x^2) (g+x^4+x^3+1)

C\_15 = {15,30,29,27,23} => M\_15(g) = (g+x^4+x^3) (g+x^4+x^2+x+1) (g+x^4+x^3+x^2) (g+x^2+x+1) (g+x^4+x^2+1)

1. Проверить на примитивность неприводимый многочлен 100101

Пусть x – корень => возводя его в степень мы должны получить все элементы поля GF(2^5)

x, x^2, x^3, x^4, x^2+1, x^3+x, x^4+x^2, x^3+x^2+1, x^4+x^3+x,x^4+1, x^2+x+1, x^3+x^2+x, x^4+x^3+x^2, x^4+x^3+x^2+1, x^4+x^3+x^2+x+1, x^4+x^3+x+1, x^4+x+1, x+1, x^2+x, x^3+x^2, x^4+x^3, x^4+x^2+1, x^3+x^2+x+1, x^4+x^3+x^2+x, x^4+x^3+1, x^4+x^2+x+1, x^3+x+1, x^4+x^2+x, x^3+1, x^4+x, 1 => все элементы, кроме 0 есть => примитивный

1. Проверить на примитивность неприводимый многочлен 110111

Пусть x – корень => возводя его в степень мы должны получить все элементы поля GF(2^5)

x^2, x^3, x^4, x^4+x^2+x+1, x^4+x^3+1, x^2+1, x^3+x, x^4+x^2, x^4+x^3+x^2+x+1, x^3+1, x^4+x, x^4+x+1, x^4+1, x^4+x^2+1, x^4+x^3+x^2+1, x^3+x^2+1, x^4+x^3+x, x+1, x^2+x, x^3+x^2, x^4+x^3, x^2+x+1, x^3+x^2+x, x^4+x^3+x^2, x^3+x^2+x+1, x^4+x^3+x^2+x, x^3+x+1, x^4+x^2+x, x^4+x^3+x+1, 1 => все элементы, кроме 0 есть => примитивный

1. Проверить на примитивность неприводимый многочлен 1011011

Пусть x – корень => возводя его в степень мы должны получить все элементы поля GF(2^6)

x^2, x^3, x^4, x^5, x^4+x^3+x+1, x^5+x^4+x^2+x, x^5+x^4+x^2+x+1, x^5+x^4+x^2+1, x^5+x^4+1, x^5+x^4+x^3+1, x^5+x^3+1, x^3+1, x^4+x, x^5+x^2, x^4+x+1, x^5+x^2+x, x^4+x^2+x+1, x^5+x^3+x^2+x, x^2+x+1, x^3+x^2+x, x^4+x^3+x^2, x^5+x^4+x^3, x^5+x^3+x+1, x^3+x^2+1, x^4+x^3+x, x^5+x^4+x^2, x^5+x^4+x+1, x^5+x^4+x^3+x^2+1, x^5+1, x^4+x^3+1, x^5+x^4+x, x^5+x^4+x^3+x^2+x+1, x^5+x^2+1, x^4+1, x^5+x, x^4+x^3+x^2+x+1, x^5+x^4+x^3+x^2+x, x^5+x^2+x+1, x^4+x^2+1, x^5+x^3+x, x^3+x^2+x+1, x^4+x^3+x^2+x, x^5+x^4+x^3+x^2, x^5+x+1, x^4+x^3+x^2+1, x^5+x^4+x^3+x, x^5+x^3+x^2+x+1, x^2+1, x^3+x, x^4+x^2, x^5+x^3, x^3+x+1, x^4+x^2+x, x^5+x^3+x^2, x+1, x^2+x, x^3+x^2, x^4+x^3, x^5+x^4, x^5+x^4+x^3+x+1, x^5+x^3+x^2+1, 1 => все элементы, кроме 0 есть => примитивный

1. Проверить на примитивность неприводимый многочлен 1100001

Пусть x – корень => возводя его в степень мы должны получить все элементы поля GF(2^6)

x^2, x^3, x^4, x^5, x^5+1, x^5+x+1, x^5+x^2+x+1, x^5+x^3+x^2+x+1, x^5+x^4+x^3+x^2+x+1, x^4+x^3+x^2+x+1, x^5+x^4+x^3+x^2+x, x^4+x^3+x^2+1, x^5+x^4+x^3+x, x^4+x^2+1, x^5+x^3+x, x^5+x^4+x^2+1, x^3+x+1, x^4+x^2+x, x^5+x^3+x^2, x^5+x^4+x^3+1, x^4+x+1, x^5+x^2+x, x^5+x^3+x^2+1, x^5+x^4+x^3+x+1, x^4+x^2+x+1, x^5+x^3+x^2+x, x^5+x^4+x^3+x^2+1, x^4+x^3+x+1, x^5+x^4+x^2+x, x^3+x^2+1, x^4+x^3+x, x^5+x^4+x^2, x^3+1, x^4+x, x^5+x^2, x^5+x^3+1, x^5+x^4+x+1, x^2+x+1, x^3+x^2+x, x^4+x^3+x^2, x^5+x^4+x^3, x^4+1, x^5+x, x^5+x^2+1, x^5+x^3+x+1, x^5+x^4+x^2+x+1, x^3+x^2+x+1, x^4+x^3+x^2+x, x^5+x^4+x^3+x^2, x^4+x^3+1, x^5+x^4+x, x^2+1, x^3+x, x^4+x^2, x^5+x^3, x^5+x^4+1, x+1, x^2+x, x^3+x^2, x^4+x^3, x^5+x^4, 1 => все элементы, кроме 0 есть => примитивный

1. Реализовать построение цикломатических классов и минимальных многочленов для произвольного примитивного многочлена над полем Галуа.

Для реализации поставленной задачи была использована программа из предыдущей лабораторной работы, содержащая реализацию базовой арифметики в поле Галуа по модулю полинома.

Была написана функция осуществляющая построения всех цикломатических классов для данного поля Галуа GF(2^m). Для этого запускается цикл, который проходится по всем элементам i от 1 до m-1. Если текущий элемент не встречался, то он добавляется в множестве seen и для него создается новый список в словаре цикломатических классов. Затем производится построение последовательности элементов вида s\*p^k, где s=i, p = 2, k = 1..m-1. Если в ходе построения встречается повтор элемента, то построение класса завершается. При этом все элементы в ходе построения заносятся в множество seen для избегания дубликатов цикломатических классов.

Для построения минимальных многочленов строится многочлен вида M(g) = (g+a1)(g+a2)…(g+ak), где a1,a2,…,ak – элементы цикломатического класса, для которого строится полином. Для этого перебираются все элементы цикломатического класса и строится строка по согласно общему виду полинома.

**Вывод:** Были изучены свойства полей Галуа и цикломатических классов.