МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КУБГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчет**

**по практическому заданию №4**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнила

Студентка 49 группы

Шестак В. А.

Преподаватель:

Крамаренко А. А.

Краснодар 2025

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

**Теория:**

Для реализации программного продукта, который строит все примитивные элементы заданного поля GF(2n), необходимо понимать следующие теоретические аспекты:

1. Конечные поля (поля Галуа)

Поле Галуа  GF(2n) — это конечное поле, содержащее 2n2n элементов. Каждый элемент поля может быть представлен как многочлен степени меньше nn с коэффициентами из  GF(2) (т.е. коэффициенты 0 или 1).

Пример: В поле GF(2^4) элементы представляются как многочлены степени меньше 4, например, x^3+x+1.

2. Неприводимые многочлены

Неприводимый многочлен — это многочлен, который нельзя разложить на множители меньшей степени над GF(2).

Неприводимый многочлен используется для построения поля GF(2n). Например, для GF(2^4) можно использовать p(x)=x^4+x+1.

3. Примитивные элементы

Примитивный элемент — это элемент поля GF(2^n), который является генератором мультипликативной группы поля. Это означает, что все ненулевые элементы поля могут быть получены как степени примитивного элемента.

Порядок примитивного элемента равен 2^n−1. Например, в  GF(2^4) порядок примитивного элемента равен 15.

4. Проверка на примитивность

Чтобы проверить, является ли элемент αα примитивным, нужно убедиться, что его порядок равен 2^n−1. Это означает, что:

a^2^n−1=1 (единичный элемент поля).

Α^k≠1 для всех  k<2^n−1.

Если элемент не удовлетворяет этим условиям, он не является примитивным.

5. Арифметика в поле GF(2^n)

Сложение в GF(2^n) выполняется как побитовое XOR.

Умножение выполняется как умножение многочленов с последующим приведением по модулю неприводимого многочлена.

Возведение в степень выполняется через быстрое возведение в степень с использованием умножения в поле.

**Ход работы;**

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

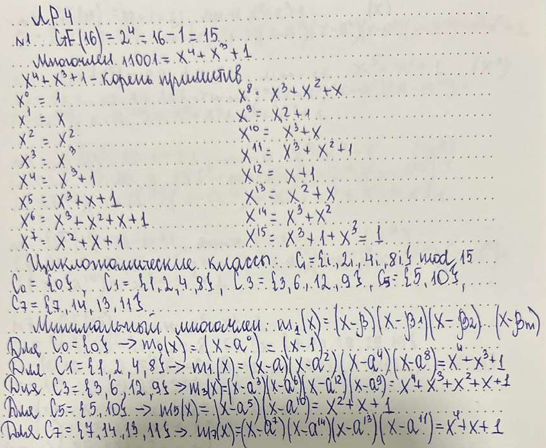


Рисунок 1 – Решение задания 1

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

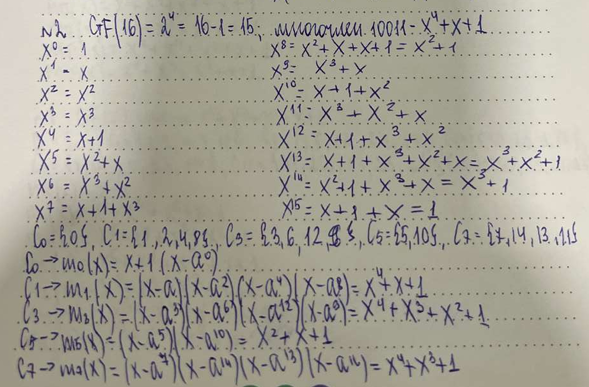


Рисунок 2 – Решение задания 2

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



Рисунок 3 – Решение задания 3

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

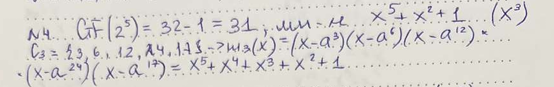


Рисунок 4 – Решение задания 4

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

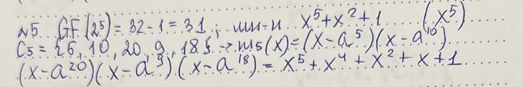


Рисунок 5 – Решение задания 5

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

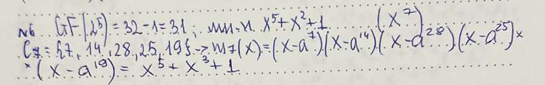


Рисунок 6 – Решение задания 6

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

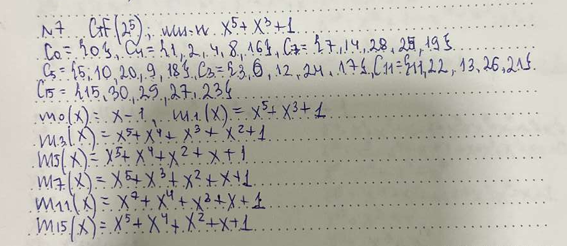


Рисунок 7 – Решение задания 7

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

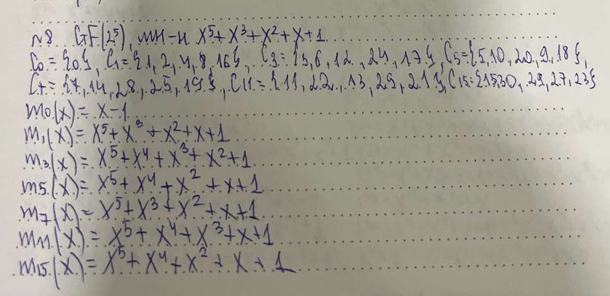


Рисунок 8 – Решение задания 8

1. Проверить на примитивность неприводимый многочлен 100101

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

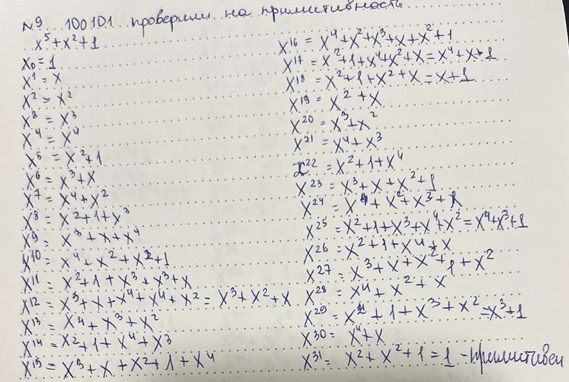


Рисунок 9 – Решение задания 9

1. Проверить на примитивность неприводимый многочлен 110111

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

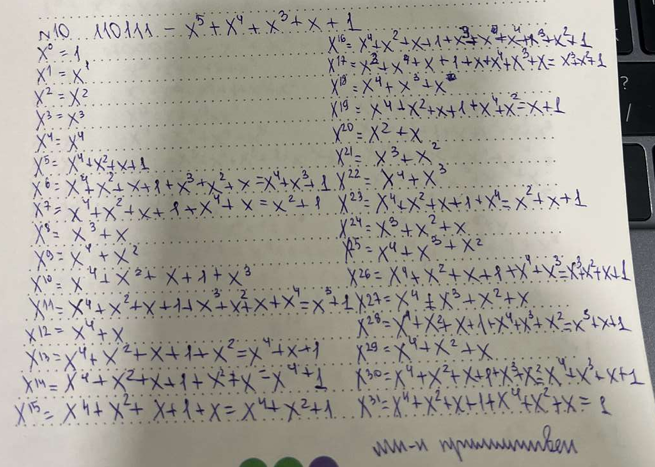


Рисунок 10 – Решение задания 10

1. Проверить на примитивность неприводимый многочлен 1011011

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

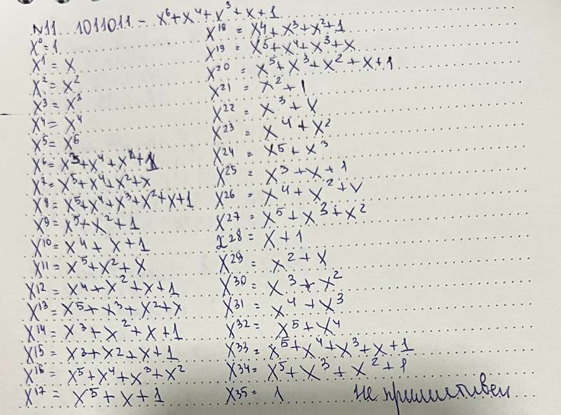


Рисунок 11 – Решение задания 11

1. Проверить на примитивность неприводимый многочлен 1100001

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

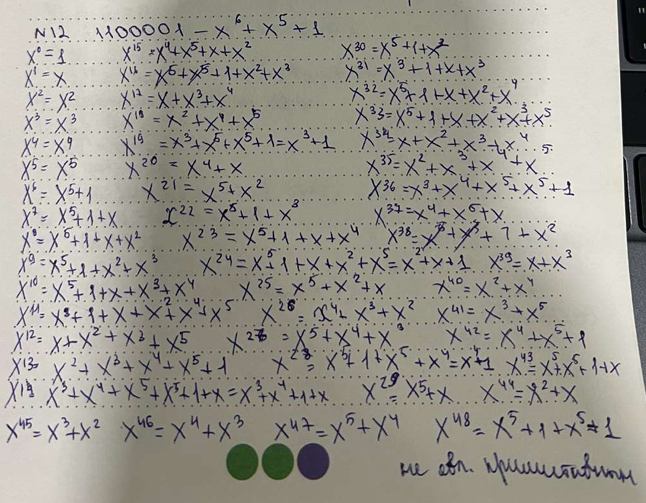


Рисунок 12 – Решение задания 12