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:**

1. Поля Галуа

**Определение**: Поля Галуа (GF) представляют собой конечные поля, обычно обозначаемые как GF(q), где q - степень простого числа p.

**Пример**: GF(2^m) — поле с 2m элементами.

2. Циклотомические классы

**Циклотомические классы -** это наборы элементов поля, которые являются корнями данного многочлена.

Для конечного поля GF(p^n) с примитивным элементом α, циклотомический класс для элемента α^k включает все степени этого элемента, которые также являются корнями соответствующего многочлена.

3. Минимальные многочлены

**Минимальный многочлен элемента поля** - это неприводимый многочлен с наименьшей возможной степенью, для которого данный элемент является корнем.

Если элемент α является корнем многочлена f(x) в поле GF(q), то f(x) будет делиться на минимальный многочлен элемента α.

4. Примитивность многочленов

**Примитивный многочлен** - это доказано неприводимый многочлен с такой особенностью, что его корни являются всеми элементами поля, кроме нуля.

Проверка на примитивность включает в себя определение порядка корня в мультипликативной группе поля.

**Ход работы:**

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

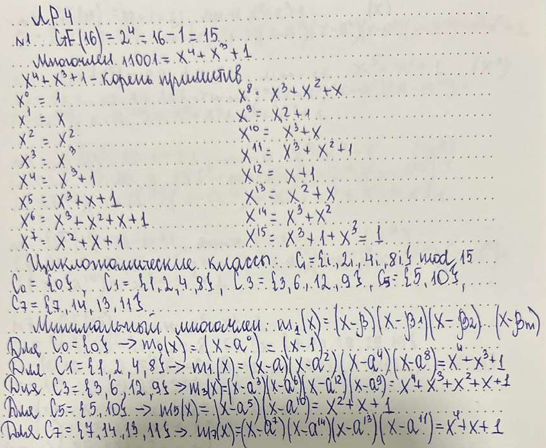


Рисунок 1 – Решение задания 1

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

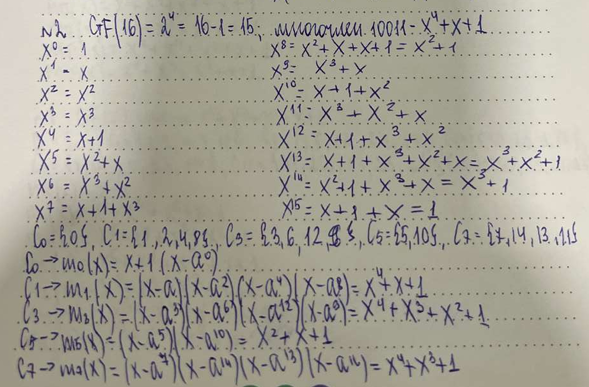


Рисунок 2 – Решение задания 2

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.

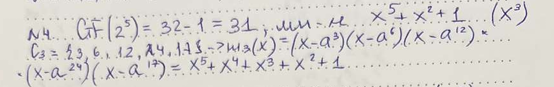


Рисунок 4 – Решение задания 4

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

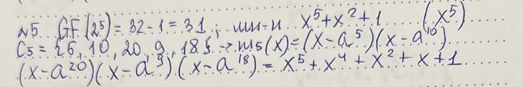


Рисунок 5 – Решение задания 5

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

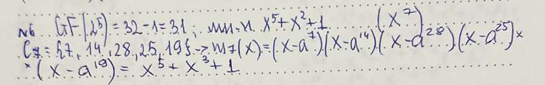


Рисунок 6 – Решение задания 6

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

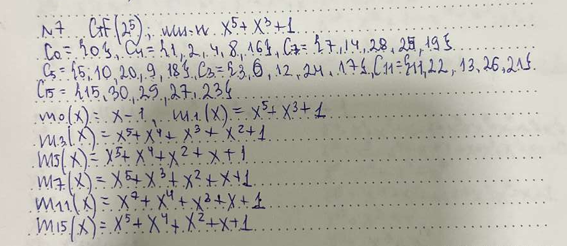


Рисунок 7 – Решение задания 7

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

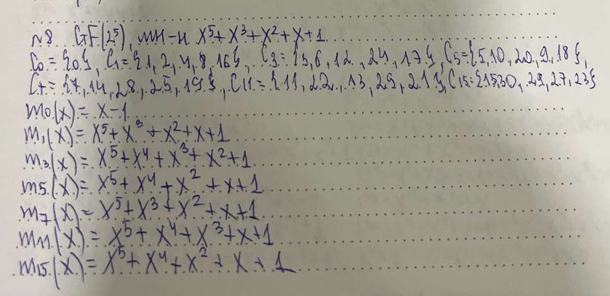


Рисунок 8 – Решение задания 8

1. Проверить на примитивность неприводимый многочлен 100101

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

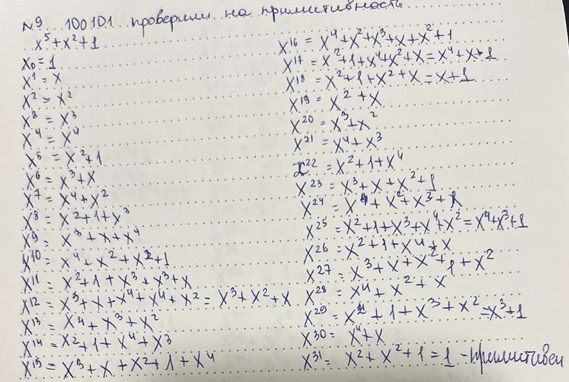


Рисунок 9 – Решение задания 9

1. Проверить на примитивность неприводимый многочлен 110111

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

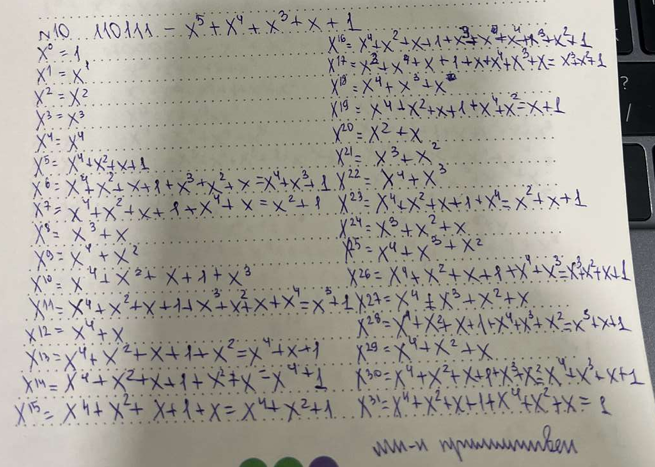


Рисунок 10 – Решение задания 10

1. Проверить на примитивность неприводимый многочлен 1011011

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

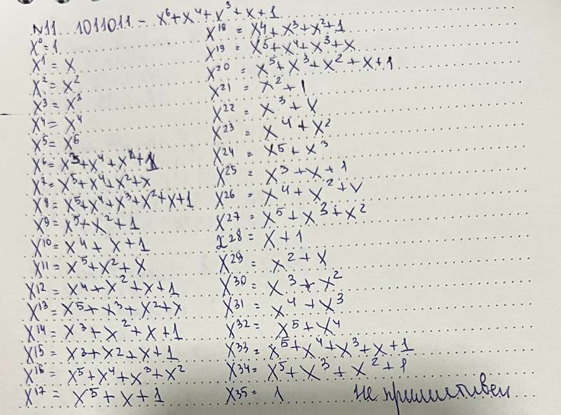


Рисунок 11 – Решение задания 11

1. Проверить на примитивность неприводимый многочлен 1100001

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

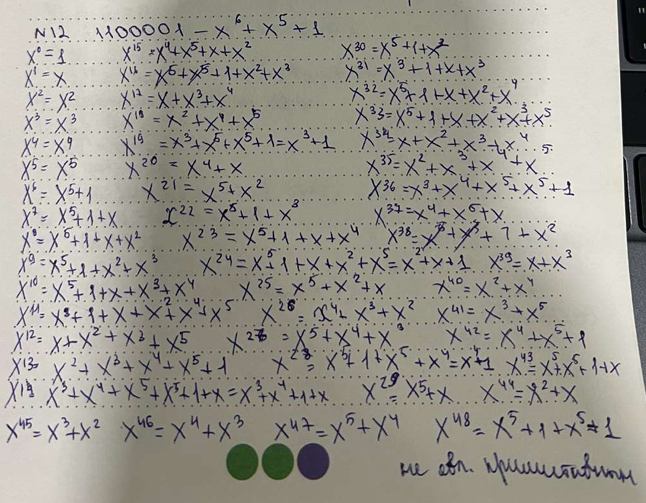


Рисунок 12 – Решение задания 12