Государственное образовательное учреждение
высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

В. М. Охорзин

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ТЕОРИИ СЕТЕЙ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ (ЦИКЛИЧЕСКИЕ КОДЫ)

КОНТРОЛЬНАЯ РАБОТА

СПбГУТ)))

**САНКТ-ПЕТЕРБУРГ
2017**

УДК 621.391.254(076.5)
ББК 388-01я73
О92

Рецензент
доктор технических наук, профессор *Н. В. Савищенко* (ВАС)

Рекомендовано к печати
редакционно-издательским советом университета

Охорзин В. М.
О92 Математические методы теории сетей связи и передачи данных (Циклические коды): контрольная работа / *В. М. Охорзин.* – СПб. : Изд-во «Теледом» ГОУВПО СПбГУТ, 2017. – 58 с.

Содержатся теоретический материал по алгебраическим основам циклических кодов и вопросы, выносимые на упражнения по дисциплине «Математические методы теории сетей связи и передачи данных». Приводятся задачи и примеры решения типовых задач, контрольные вопросы, а также необходимая литература. Предназначается для бакалавров по направлению 11.03.02 и студентов, обучающихся по всем техническим специальностям.

УДК 621.391.254(076.5)
ББК 388-01я73

1. АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ПОСТРОЕНИЯ И АНАЛИЗА СВОЙСТВ ГРУППОВЫХ КОДОВ

1.1. Основные определения

В дискретных каналах связи информация передается с помощью некоторого числа символов q, составляющих ограниченный набор, называемым полем. Поля с конечным числом символов q называют полями Галуа и обозначают GF(q). Число q выбирают как степень некоторого простого числа p: $q=p^m$.

При этом поле для m=1 – GF(p) – называют простым, а для m>1 – GF(p^m) – расширенным или расширением степени m основного поля $GF(p)$. В случае q=2 имеет место двоичный канал с символами «0» и «1».

Для передачи сообщений источника элементы поля объединяют в кодовые комбинации длины n, называемые также n-последовательностями. Совокупность всех n-последовательностей образует линейное векторное пространство, в котором отдельная n-последовательность рассматривается как вектор.

Некоторое множество векторов называется *линейным кодом*, если оно является подпространством всех n-последовательностей.

Для двоичных линейных кодов, у которых n-последовательности содержат в качестве символов «0» и «1», общепринято название *групповой код*. Такое название обусловлено тем, что совокупность векторов линейного векторного пространства образует алгебраическую систему, называемую группой.

Кроме группы и связанных с нею разделов теории векторных пространств и матриц для описания и анализа свойств групповых кодов применяют элементы теории колец и конечных полей.

Алгебраические системы – это абстрактные системы, которые подчиняются определенным правилам и законам, формулируемым в виде аксиом [1–3].

Применительно к двоичному каналу *группа* – это система, в которой задана одна из двух возможных операций – сложение (аддитивная группа) или умножение (мультипликативная группа) по модулю 2 и выполняются аксиомы А1–А4.

В *кольце* и *поле* определены две операции – сложение и умножение. При этом элементы *кольца* по операции сложения должны удовлетворять всем групповым аксиомам А1–А5, т. е. образуют абелеву группу, а по операции умножения – А1 и А2; в *поле* все элементы образуют абелеву группу по сложению, а все ненулевые элементы – абелеву группу по умножению. В кольце и поле элементы можно складывать и умножать, значит, в этих системах должна удовлетворяться аксиома А6.

***Аксиомы, определяющие алгебраические системы* [1]**

А1. Замкнутость. Операция может быть применена к любым двум элементам группы, в результате чего получаются также элементы группы.

А2. Ассоциативный закон. Для любых трех элементов a, b и c группы $(a+b)+c=a+(b+c)$, если заданная операция – сложение, или $a\cdot(bc)=(ab)\cdot c$, если заданная операция – умножение.

А3. Наличие единичного элемента. Если задана операция сложения, то единичный элемент есть 0 и определяется из уравнения $0+a=a+0=a$, где a – любой элемент группы. При операции умножения, единичный элемент есть 1 и определяется из уравнения $1\cdot a=a\cdot 1=a$.

А4. Существование обратных элементов. Для каждого элемента группы a существует обратный элемент. Обратный элемент для операции сложения $(-a)$ определяется из уравнения $a+(-a)= (-a)+a=0$. При операции умножения обратный элемент (a^{-1}) определяется уравнением $aa^{-1}=a^{-1}a=1$.

А5. Коммутативный закон. Если для элементов группы по заданной операции удовлетворяется $a+b = b+a$ или $ab=ba$ для операций сложения и умножения соответственно, то группа называется абелевой или коммутативной.

А6. Дистрибутивный закон. Правило раскрытия скобок: $a(b+c) = ab+ac$.

Кольцо называется коммутативным, если коммутативна операция умножения, то есть для любых двух элементов кольца a и b выполняется $ab=ba$.

Полем называется коммутативное кольцо, в котором по операции умножения имеются единичный элемент и обратные элементы для всех ненулевых элементов.

Содержание определений группы, кольца и поля отображается табл. 1.1.

Таблица 1.1

Аксиома	Система				
	группа	кольцо		поле	
Операции	« + » или « × »	« + » и « × »		« + » и « × »	
А1. Замкнутость	+	+	+	+	+
А2. Ассоциативность	+	+	+	+	+
А3. Единичный элемент	+		+	+	+
А4. Обратный элемент	+		+	+	+
А5. Коммутативность	Абелева группа	+		+	+
А6. Дистрибутивность	–	+		+	

Наименьшее число элементов, образующих поле, равно 2, так как в поле должно быть 2 единичных элемента, а именно: 0 – относительно операции сложения и 1 – относительно операции умножения. Такое поле является двоичным, т. е. GF(2).

Правила сложения и умножения определены как действия по модулю 2 и в GF(2) однозначно задаются следующими таблицами – сложения и умножения.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Поле GF(2) является простым. Расширенное двоичное поле GF(2^m) в качестве своих элементов содержит все m-разрядные двоичные последовательности. Например, GF(2^2) содержит следующие элементы: 00, 10, 01, 11. Операция сложения последовательностей в этом поле осуществляется поразрядным сложением символов, стоящих на одинаковых позициях суммируемых последовательностей с использованием указанной выше таблицы. Например, 00+11=11, 10+11=01 и т. д.

Операция умножения выполняется по правилам умножения многочленов, для этого двоичные последовательности представляются в виде многочленов от формальной переменной α:

$$00=0,\ 10=1,\ 01=\alpha,\ 11=1+\alpha.$$

Для сохранения разрядности элементов поля GF(2^m) умножение элементов поля производится по модулю некоторого неприводимого многочлена $\pi(\alpha)$ степени m. Для поля GF(2^2) таким неприводимым многочленом является $\pi(\alpha)=1+\alpha+\alpha^2$. Это единственный неприводимый многочлен степени 2 над полем GF(2).

Таблицы сложения и умножения для поля GF(2^2)

+	0	1	α	1+α
0	0	1	α	1+α
1	1	0	1+α	α
α	α	1+α	0	1
1+α	1+α	α	1	0

×	0	1	α	1+α
0	0	0	0	0
1	0	1	α	1+α
α	0	α	1+α	1
1+α	0	1+α	1	α

Приведенные таблицы для GF(2) и GF(2^2) подтверждают выполнение в этих полях всех аксиом поля, в том числе единственность единичных и обратных элементов. Кроме того, можно сделать вывод, что расширенное поле содержит основное поле. Как для основного поля 2=0, так и для расширенного поля $\pi(\alpha)=1+\alpha+\alpha^2=0$, т. е. α является корнем $\pi(x)=1+x+x^2$. Вторым корнем $\pi(x)$ является 1+α, что можно проверить прямой подстановкой. Очевидно, что $1+\alpha=\alpha^2$. Значит, все ненулевые элементы GF(2^2) есть степени корня α многочлена $\pi(x)$, поэтому говорят, что расширение поля образуется присоединением корней $\pi(x)$ к основному полю.

1.2. Группа, подгруппа и смежные классы

Подмножество H элементов группы G, удовлетворяющее всем групповым аксиомам, называется *подгруппой.*

Обозначим элементы группы G через g_1, g_2, g_3, … , а подгруппы через h_1, h_2, h_3, … . Рассмотрим следующую таблицу. Первая строка состоит из элементов подгруппы H, взятых по одному разу, с единичным элементом в начале строки. Первым элементом второй строки может быть любой элемент G, не вошедший в первую строку, а все остальные элементы получаются применением групповой операции (например, сложения) первого элемента второй строки с элементами подгруппы.

Аналогично образуются последующие строки, каждая с неиспользованным прежде элементом группы в начале строки до тех пор, пока все элементы G не войдут в таблицу.

h_1=0,	h_2,	h_3,	…..,	h_l
g_1,	g_1+h_2,	g_1+h_3,	…..,	g_1+h_l
g_2,	g_2+h_2,	g_2+h_3,	…..,	g_2+h_l
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
g_m,	g_m+h_2,	g_m+h_3,	…..,	g_m+h_l

Каждая строка в полученной таблице называется *смежным классом*, а элемент группы в начале строки называется *образующим смежного класса.*

Представленное разложение группы G по подгруппе H на смежные классы, независимо от групповой операции, обладает следующими свойствами.

1. В таблице содержатся все элементы группы, и каждый элемент группы появляется в таблице только один раз.

2. Состав смежного класса не зависит от выбора образующего элемента смежного класса.

3. По введенной в группе операции можно ввести операцию над смежными классами, и по введенной операции смежные классы образуют новую группу, элементами которой являются смежные классы $\{g_i\}$ (в фигурных скобках указывается образующий смежного класса), а единичным элементом – сама подгруппа $\{h_j\}$.

Действие над смежными классами выполняется следующим образом:

сложение $\{g_i\}+\{g_j\}=\{g_z\}$ означает, что сумма любого элемента из смежного класса $\{g_j\}$ с любым элементом смежного класса $\{g_i\}$ находится в классе $\{g_z\}$;

умножение $\{g_i\}\cdot\{g_j\}=\{g_x\}$ означает, что произведение любого элемента из $\{g_i\}$ с любым элементом $\{g_j\}$ находится в $\{g_x\}$.

Пример 1.2.1. Пусть G – группа по сложению из всех целых положительных, отрицательных чисел и нуля и H – подгруппа, состоящая из всех чисел, кратных двум.

Тогда таблица разложения G по H на смежные классы состоит из двух строк:

{0}	2	–2	4	–4	6	–6, …
{1}	–1	3	–3	5	–5	7, …

где {0} – подгруппа, содержащая все числа, кратные двум, т. е. четные числа положительные и отрицательные;

{1} – смежный класс, содержащий все нечетные положительные и отрицательные числа.

Таблица сложения для смежных классов

+	{0}	{1}
{0}	{0}	{1}
{1}	{1}	{0}

В этой таблице легко узнается таблица сложения по модулю 2. Число элементов группы называется *порядком группы.*

Пример 1.2.2. Показать, что множество всех двоичных последовательностей длины 3: 000, 001, 010, 011, 100,101, 110, 111, состоящее из всех возможных трехразрядных двоичных чисел, является группой по операции поразрядного сложения по модулю 2.

Проверим выполнение групповых аксиом для заданной совокупности двоичных последовательностей и заданной операции.

А1. *Замкнутость*. Поразрядное сложение по модулю 2 дает для суммы любых чисел из заданной совокупности также число из этой совокупности, так как других трехразрядных двоичных чисел не существует.

А2. *Ассоциативность*. Для введенной операции результат сложения не зависит от очередности выбора суммируемых элементов из некоторой ассоциации, поэтому для нее ассоциативный и коммутативный законы всегда выполняются.

А3. *Наличие единичного элемента*. Единичным элементом является чисто нулевая последовательность 000, так как сложение именно этой последовательности с любой другой в любом порядке не изменяет значения последней.

А4. *Существование обратных элементов*. Для любой двоичной последовательности только сумма с точно такой же последовательностью даст в результате чисто нулевую последовательность, т. е. каждая двоичная последовательность является для себя обратной.

А5. *Коммутативный закон*. Выполнение коммутативного закона подтверждается пояснениями в А2.

На основе проведенного анализа можно сделать следующий вывод.

При проверке выполнения групповых свойств некоторого множества двоичных последовательностей по введенным операциям достаточно выявить их замкнутость и наличие единичного элемента.

1.3. Кольцо, идеал и классы вычетов

В теории колец роль, аналогичную подгруппе в группе, играет понятие идеала.

Идеалом I называется подмножество элементов кольца R, обладающее следующими двумя свойствами:

● является подгруппой аддитивной группы кольца R;

● для любого элемента a из I и любого элемента r из R произведение ar и ra принадлежит I.

Поскольку идеал является подгруппой, могут быть образованы смежные классы. В случае кольца смежные классы называют *классами вычетов*. Их построение аналогично рассмотренному выше. Идеал образует первую строку с нулевым элементом в начале строки. Любой элемент кольца, не принадлежащий идеалу, может быть выбран в качестве образующего первого класса вычетов, а остальные элементы класса вычетов получают сложением образующего с каждым элементом идеала и т. д. Первыми элементами в каждой строке являются элементы, не использованные в предыдущих классах.

Все свойства смежных классов верны и для классов вычетов, т. е. их можно складывать и умножать в рассмотренном выше смысле. Легко проверить, что по операции сложения классы вычетов образуют коммутативную группу, в которой идеал играет роль нулевого элемента, а по операции умножения классов вычетов выполняется замкнутость, ассоциативный и дистрибутивный законы, т. е. классы вычетов по идеалу в некотором кольце образуют кольцо, называемое *кольцом классов вычетов.*

Понятие кольца и кольца классов вычетов одинаково справедливо как целых чисел, так и для многочленов от одного переменного с коэффициентами из некоторого поля. Эти понятия позволяют определить структуру конечных полей простых и расширенных соответственно. Идеал кольца классов вычетов многочленов используется для определения и характеристики свойств циклических кодов. Из определения идеала вытекает, что идеал может быть образован всеми кратными некоторого его элемента.

Для целых чисел структура идеала и классов вычетов формируется следующим образом:

● совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу;

● идеал, состоящий из всех целых чисел кратных m и самого m, лежит в основе кольца класса вычетов, называемого *кольцом целых чисел по модулю* m;

● каждый класс вычетов по модулю m содержит либо 0, либо целое положительное число, не превосходящее m. Нуль является элементом идеала, а все целые положительные числа, не превосходящие m, принадлежат различным классам вычетов.

Рассмотрим кольцо целых чисел. Оно имеет бесконечное число элементов. В кольце целых чисел используются обычные операции сложения и умножения.

Построим кольцо классов вычетов по модулю m=5, идеал которого содержит числа:

$\{0\}$: 0, 5 , – 5, ,10, – 10, 15, – 15, …

В качестве образующего первого класса вычетов выберем минимальное число, не вошедшее в $\{0\}$:

$\{1\}$: 1, 6, – 4, 11, – 9, 16, – 14, …

В качестве образующих следующих классов вычетов возьмем числа 2, 3, 4, при этом состав классов вычетов будет иметь вид:

$\{2\}$: 2, 7, – 3, 12, – 8, 17, – 13, …
$\{3\}$: 3, 8, – 2, 13, – 7, 18, – 12, …
$\{4\}$: 4, 9, – 1, 14, – 6, 19, – 11, …

Идеал $\{0\}$ и классы вычетов $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$ образуют кольцо классов вычетов по модулю 5.

Сложение и умножение чисел в этом новом кольце будут производиться по модулю 5.

Таблицы сложения и умножения чисел по модулю

+	{0}	{1}	{2}	{3}	{4}
{0}	{0}	{1}	{2}	{3}	{4}
{1}	{1}	{2}	{3}	{4}	{0}
{2}	{2}	{3}	{4}	{0}	{1}
{3}	{3}	{4}	{0}	{1}	{2}
{4}	{4}	{0}	{1}	{2}	{3}

×	{0}	{1}	{2}	{3}	{4}
{0}	{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{2}	{3}	{4}
{2}	{0}	{2}	{4}	{1}	{3}
{3}	{0}	{3}	{1}	{4}	{2}
{4}	{0}	{4}	{3}	{2}	{1}

Аналогично можно охарактеризовать структуру идеала и классов вычетов кольца многочленов, заменяя слова «целое число» на «многочлен».

Будем рассматривать многочлены с коэффициентами из двоичного поля:

$$f(x)=f_0+f_1x+f_2x^2+\ldots+f_n x^n,$$

где f_i = 0,1.

Степенью многочлена называют наибольшую степень x в слагаемом с ненулевым коэффициентом. Степень нулевого многочлена равна 0. Многочлен называют нормированным, если коэффициент при наивысшей степени x равен 1 (в двоичном поле все ненулевые многочлены нормированные).

В двоичном случае многочлены можно складывать, умножать и делить в общепринятом смысле с использованием таблицы сложения по модулю 2 при сложении коэффициентов равностепенных слагаемых и приведении подобных членов при умножении и делении многочленов. Легко показать, что множество всех многочленов с коэффициентами из двоичного поля по введенным над этим полем операциями сложения и умножения многочленов образуют кольцо.

Порядок такого кольца бесконечен оно имеет следующую структуру:

1) совокупность многочленов образует идеал тогда и только тогда, когда она содержит все многочлены, кратные некоторому многочлену;

2) идеал, состоящий из всех многочленов, кратных некоторому многочлену $f(x)$, лежит в основе кольца классов вычетов, называемого кольцом многочленов по модулю многочлена $f(x)$;

3) каждый класс вычетов по модулю многочлена $f(x)$ степени n содержит либо 0, либо многочлен степени меньшей, чем n. Нуль является элементом идеала, а все многочлены степеней меньших, чем n, принадлежат различным классам вычетов.

В качестве примера рассмотрим кольцо многочленов по модулю $f(x)=x^2+1$.

Идеал этого кольца и классы вычетов по модулю $f(x)=x^2+1$ имеют вид:

$\{0\}$	x^2+1	$(x^2+1)x$	$(x^2+1)(x+1)$	…
$\{1\}$	x^2	x^3+x+1	x^3+x^2+x	…
$\{x\}$	x^2+x+1	x^3	x^3+x^2+1	…
$\{1+x\}$	x^2+x	x^3+1	x^3+x^2	…

Составим таблицы сложения и умножения для этого кольца.

+	$\{0\}$	$\{1\}$	$\{x\}$	$\{1+x\}$
$\{0\}$	$\{0\}$	$\{1\}$	$\{x\}$	$\{1+x\}$
$\{1\}$	$\{1\}$	$\{0\}$	$\{1+x\}$	$\{x\}$
$\{x\}$	$\{x\}$	$\{1+x\}$	$\{0\}$	$\{1\}$
$\{1+x\}$	$\{1+x\}$	$\{x\}$	$\{1\}$	$\{0\}$

×	$\{0\}$	$\{1\}$	$\{x\}$	$\{1+x\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
$\{1\}$	$\{0\}$	$\{1\}$	$\{x\}$	$\{1+x\}$
$\{x\}$	$\{0\}$	$\{x\}$	$\{1\}$	$\{1+x\}$
$\{1+x\}$	$\{0\}$	$\{1+x\}$	$\{1+x\}$	$\{0\}$

Обратим внимание, что по сложению рассматриваемое кольцо удовлетворяет всем групповым аксиомам.

При операции умножения для элемента $\{1+x\}$ отсутствует обратный, что допустимо для кольца. Сравнение элементов кольца многочленов по модулю $f(x)=x^2+1$ с элементами расширенного поля $GF(2^2)$ из п. 1.1 показывает их полное совпадение. Можно сделать вывод, что отличие в свойствах сравниваемых систем зависит от структуры идеала, т. е. выбора модуля, по которому сформировано кольцо классов вычетов.

Классы вычетов кольца многочленов по модулю многочлена $f(x)$ степени n образуют кольцо многочленов по модулю $f(x)$.Порядок этого кольца при выборе коэффициентов многочлена из поля GF(q) равен q^n. При $q=2$ число классов вычетов многочленов по модулю многочлена степени n равно 2^n.

При выборе в качестве образующего класса вычетов многочлена минимальной степени в своем классе, как это сделано в примере, поясняющем кольцо многочленов по модулю x^2+1, образующими классов вычетов будут все возможные многочлены степеней от нулевой (единица) до n–1.

В кольце, которое образуют классы вычетов, также может быть найден идеал как множество классов вычетов с образующими, кратными некоторому многочлену $g(x)$, степень которого, естественно, меньше n.

Многочлен g(x) минимальной степени, отличный от нуля, такой, что класс вычетов {g(x)} образует идеал I, содержащий все классы вычетов, кратные {g(x)}, в кольце многочленов по модулю f(x) тогда и только тогда, когда g(x) является делителем f(x).

Действительно, в соответствии с алгоритмом деления

$$\{f(x)\}=\{0\}=\{g(x)\}\{q(x)\}+\{r(x)\},$$

где $q(x)$ – частное от деления $f(x)$ на $g(x)$, $r(x)$ – остаток от деления.

В соответствии с представленной записью $\{r(x)\}$ принадлежит идеалу$\{0\}$, и при этом $r(x)$ имеет степень меньшую, чем степень $g(x)$, что возможно лишь в том случае, когда $r(x)=0$.

Определим размерность идеала в кольце многочленов по модулю многочлена $f(x)$ степени n, если идеал образован всеми кратными некоторого многочлена $g(x)$, являющегося делителем $f(x)$.

Пусть $f(x)=g(x)h(x)$, где $h(x)$ – многочлен степени κ, а $f(x)$ имеет степень n.

Многочлены вида $x^0g(x), x^1g(x), ..., x^{\kappa-1}g(x)$ линейно независимы и принадлежат идеалу, а их линейная комбинация

$$s(x) = (a_0 x^0+\ldots+a_{\kappa-1} x^{\kappa-1})\, g(x),$$

где a_i – элемент основного поля, отлична от нуля, так как имеет степень, меньшую n, и также принадлежит идеалу.

Значит, идеал, порожденный многочленом g(x) степени n–k, являющийся делителем f(x) степени n, в кольце многочленов по модулю f(x) имеет размерность, равную k.

Пример 1.3.1. Рассмотрим кольцо многочленов по модулю $f(x) = x^3+1= =(x+1)(x^2+x+1)$.

Это кольцо содержит следующие классы вычетов:

$$\{0\}, \{1\}, \{x\}, \{1+x\}, \{x^2\}, \{1+x^2\}, \{x+x^2\}, \{1+x+x^2\}$$

или {000}, {100}, {010}, {110}, {001}, {101}, {011}, {111} .

В данном кольце возможны два идеала.

I_1, порожденный $\{x+1\}$; общий вид элемента идеала:

$\{(a_0 x^0+a_1 x^1)(x+1)\}$; размерность 2; при подстановке a_i=0 или 1 имеем $\{0\}, \{1+x\}, \{1+x^2\}, \{x+x^2\}$ или {000}, {110}, {101} и {011}.

I_2, порожденный $\{x^2+x+1\}$. Размерность 1. Включает классы вычетов $\{0\}$ и $\{1+x+x^2\}$ или $\{000\}$ и $\{111\}$ в двоичном представлении.

1.4. Поля Галуа. Мультипликативная группа поля Галуа

В п. 1.1 дано аксиоматическое определение поля, введены понятия и приведены примеры простого и расширенного полей. Обобщением сказанного в п. 1.1 и 1.3 являются следующие определения [1, 2].

Для простых полей – *кольцо классов вычетов по модулю m является полем тогда и только тогда, когда m – простое число.*

Для расширенных полей – *кольцо многочленов по модулю некоторого неприводимого в поле GF(p) многочлена $\pi(x)$ степени m является полем GF(p^m).*

К многочлену $\pi(x)$ кроме требования неприводимости предъявляется еще одно принципиальное требование – ненулевые элементы поля являются степенями корня α многочлена $\pi(x)$.

Если ненулевые элементы поля GF*(m)* могут быть представлены как степени некоторого элемента α, то α называют примитивным элементом этого поля.

Неприводимый многочлен степени m над полем GF(p) называется примитивным, если его корнем является примитивный элемент GF(p^m).

В п. 1.1 было показано, что поле GF(2^2) в качестве ненулевых элементов имеет 1, α, $1+\alpha$, где α – корень $\pi(x)=1+x+x^2$, т. е. $1+\alpha+\alpha^2=0$. Поскольку $1=\alpha^0$, а $1+\alpha=\alpha^2$, все ненулевые элементы GF(2^2) представляются степенями корня $\pi(x)$.Элемент α является примитивным элементом GF(2^2), а $\pi(x)=1+x+x^2$ является примитивным неприводимым многочленом.

Рассмотрим поле GF(5). Поскольку 5 – простое число, то кольцо классов вычетов по модулю 5 образует поле GF(5).Таблицы сложения и умножения по модулю 5 приведены в п. 1.3. Для этого поля также существует примитивный элемент, степени которого дают все ненулевые элементы поля, например $2^0=1$; $2^1=2$; $2^2=4$; $2^3=8=3$; $2^4=16=1$; $2^5=32=2$.

Эти примеры могут быть обобщены следующим образом. В любой конечной мультипликативной группе можно рассмотреть совокупность элементов, образованную некоторым элементом g и его степенями g^2, g^3 и т. д. Группа имеет конечное число элементов, поэтому неизбежно появится повторение, т. е. для некоторых i и j будет $g^i = g^j$.

Если наблюдается $g^i=g^j$, то $g^{j-i}=1$. Следовательно, некоторая степень элемента g равна 1. Пусть e – наименьшее положительное число, при котором g^e=1. Совокупность элементов 1, g, g^2, ..., g^{e-1} образует подгруппу по операции умножения, так как налицо единичный элемент 1, замкнутость, наличие обратных элементов: для g^i обратный элемент g^{e-i}.

Группа, состоящая из всех степеней одного из ее элементов, получила название *циклической группы*. Число ***e*** называется порядком элемента ***g***.

Обобщением изложенного выше является следующее.

В поле GF(q) *существует примитивный элемент α, т.е. элемент порядка q–1. Каждый ненулевой элемент поля* GF(q) *может быть представлен как некоторая степень* α*, т. е. мультипликативная группа поля Галуа* GF(q) *является циклической.*

Если мультипликативная группа порядка q содержит циклическую подгруппу из e элементов, порожденную некоторым элементом g, то число смежных классов в разложении группы по циклической подгруппе будет равно q/e, и каждый смежный класс также будет содержать e элементов.

Значит справедливо следующее утверждение.

Порядок е любого элемента группы является делителем порядка группы. Число элементов поля GF(q^m)*, имеющих порядок е, определяется выражением: Ne =* φ*(е),*

где φ(e) – *функция Эйлера* [3], равная числу чисел взаимно простых с e и меньших e.

Функция Эйлера может быть вычислена следующим образом.

Если e – составное число вида $e=\prod_{i=1}^{t} p_i^{l_i}$, где $p_i > 1$ – простое, а l_i – натуральное число и i = 1,2, ..., t,

то φ(e) = $\varphi(e)=\prod_{i=1}^{t} p_i^{l_i-1}(p_i-1)=\mathring{a}(1-\frac{1}{p_1})...(1-\frac{1}{p_t})$.

В частности, для простого p и целого a

$$\varphi(p^a)= p^a - p^{a-1},\ \varphi(p) = p - 1.$$

Кроме того, $\varphi(a_1\times a_2) = \varphi(a_1)\varphi(a_2)$, если a_1 и a_2 взаимно просты.

Например:

φ(1) = 1	φ(4) = 2
φ(2) = 1	φ(5) = 4
φ(3) = 2	φ(6) = 2

Пример 1.4.1. Определить число элементов N_i поля GF(2^6) порядка i = 1, 3, 7, 9, 21, 63.

Решение: $N_i = \varphi(i)$, где $\varphi(i)$ – функция Эйлера, для вычисления которой необходимо знать каноническое разложение числа i: 1=1, 3=3, 7=7, $9=3^2$, $21=3\times7$, $63=3^2\times7$.

Теперь находим: $N_1 = \varphi(1) = 1$, $N_3 = \varphi(3) = 2$, $N_7 = \varphi(7) = 6$, $N_9 = \varphi(9) = 9(1-1/3) = 9\times2/3 = 6$, $N_{21} = \varphi(21) = 21(1-1/3)(1-1/7) = 21\times2/3\times6/7 = 12$, или $\varphi(21)=\varphi(3)\varphi(7)=2\times6=12$, $N_{63} = \varphi(63) = 63(1-1/3)(1-1/7) = 63\times2/3\times6/7 = 36$.

Рассмотренные числа 1, 3, 7, 9, 21, 63 являются делителями числа 63 и поэтому определяют все возможные порядки элементов мультипликативной группы поля GF(2^6).

Полученный результат может быть обобщен следующим образом.

Сумма всех ненулевых элементов поля GF(q) *с различными порядками равна порядку его мультипликативной группы* q–1.

Важным следствием из рассмотренного является следующее.

Пусть α – примитивный элемент GF(p^m), порядок которого равен p^m-1, т. е. $\alpha^{p^m-1}=1$.

Если среди элементов поля GF(p^m) есть элемент β порядка p^{r-1}, где $r < m$, т. е. $\beta=\alpha^{\frac{p^m-1}{p^r-1}}$, то последовательность элементов β^1, β^2, …, $\beta^{p^r-1}=\alpha^{p^m-1}$ образует циклическую подгруппу мультипликативной группы GF(p^m), т. е. содержит все ненулевые элементы нового поля GF(p^r), являющегося подполем GF(p^m).

Итак, GF(p^m) *содержит подполе* GF(p^r)*, если* p^r*–1 делит* p^m*–1.*

В п. 2.1 будет показано, что p^r-1 делит p^m-1, если r делит m.

Таким образом, окончательно

GF(p^m) *содержит подполе* GF(p^r)*, если* r *делит* m*.*

Пример 1.4.2. Рассмотрим подполя поля GF(2^{12}). Число 12 делится на числа 6, 4, 3 и 2, т. е. в составе поля GF(2^{12}) существуют в качестве подполей поля GF(2^6), GF(2^4), GF(2^3), GF(2^2).

Любое расширенное поле содержит основное поле, поэтому в каждом из указанных полей содержится поле GF(2). Найдем циклические группы рассматриваемых полей. Обозначим примитивные элементы полей:

$$\mathrm{GF}(2^{12})\to\alpha,\ \mathrm{GF}(2^6)\to\beta,$$
$$\mathrm{GF}(2^4)\to\gamma,\ \mathrm{GF}(2^3)\to\delta,$$
$$\mathrm{GF}(2^2)\to\varepsilon,\ \mathrm{GF}(2)\to\zeta.$$

Выразим ненулевые элементы полей через степени примитивных элементов:

$GF(2^{12})$: $\alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{4095}$	$\alpha^{2^{12-1}} = 1$, e = 4095
$GF(2^6)$: $\beta^1, \beta^2, \beta^3, \ldots, \beta^{63}$	$\beta^{2^{6-1}} = 1$, e = 63
$GF(2^4)$: $\gamma^1, \gamma^2, \gamma^3, \ldots, \gamma^{15}$	$\gamma^{2^{4-1}} = 1$, e = 15
$GF(2^3)$: $\delta^1, \delta^2, \delta^3, \ldots, \delta^7$	$\delta^{2^{3-1}} = 1$, e = 7
$GF(2^2)$: $\varepsilon^1, \varepsilon^2, \varepsilon^3$	$\varepsilon^{2^{2-1}} = 1$, e = 3
$GF(2)$: ζ^1	$\zeta^{2^{1-1}} = 1$, e = 1

Элементы полей $GF(2^6)$, $GF(2^4)$, $GF(2^3)$, $GF(2^2)$ и $GF(2)$ входят в состав $GF(2^{12})$, при этом $\beta = \alpha^{65}$, так как $\beta^{63} = \alpha^{4095} = 1 = (\alpha^{65})^{63}$. Аналогично $\gamma = \alpha^{273}$, $\delta = \alpha^{585}$, $\varepsilon = \alpha^{1365}$, $\zeta = \alpha^{4095}$.

Связь между рассмотренными полями иллюстрирует рис. 1.1 [2, 4].

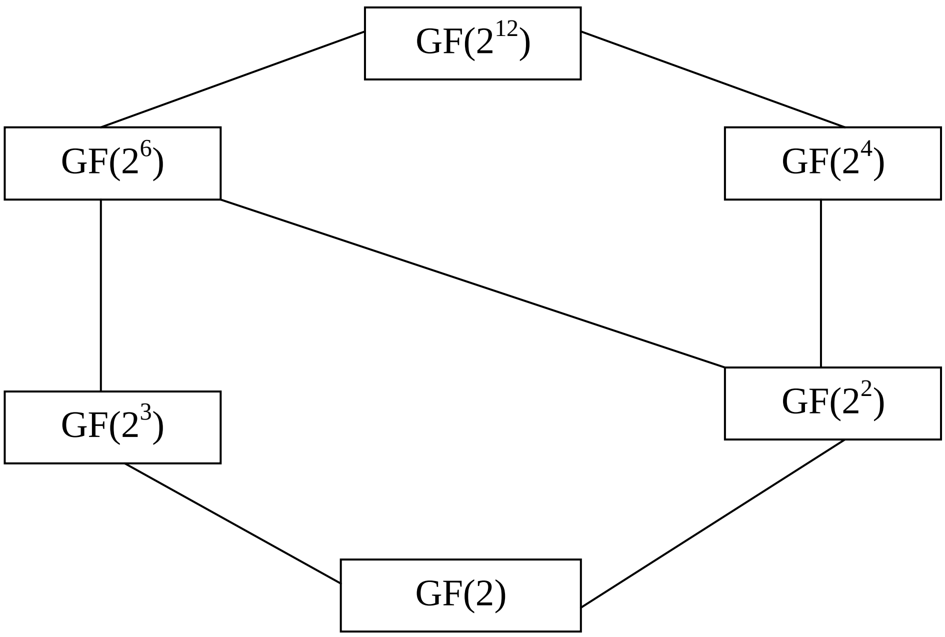


Рис.1.1. Поле $GF(2^{12})$ и его подполя

2. МНОГОЧЛЕН $x^n - 1$, ЕГО КОРНИ И НЕПРИВОДИМЫЕ СОМНОЖИТЕЛИ

2.1. Связь между корнями x^n–1 и элементами поля GF(q)

Многочлен x^n–1, его неприводимые сомножители и их корни играют существенную роль в построении важнейшего класса групповых кодов – циклических кодов. Знание корней сомножителей x^n-1 позволяет решить задачу выбора требуемого кода для конкретного дискретного канала.

Рассмотрим общий случай. Пусть x^n–1 задан над полем GF(q). Известно, что GF(q) имеет циклическую группу из q–1 своих ненулевых элементов.

Порядок каждого ненулевого элемента GF(q) не может быть выше q–1, а это означает, что α^{q-1}=1 для любого ненулевого элемента α из GF(q), т. е. любой ненулевой элемент GF(q) обращает x^{q-1}–1 в нуль, а значит, является его корнем. Поскольку x^{q-1}–1 имеет ровно q–1 корней, следовательно, все ненулевые элементы GF(q) являются корнями x^{q-1}–1.

Таким образом, *имеется однозначное соответствие между корнями x^{q-1}–1 и ненулевыми элементами* GF(q).

В случае двоичных циклических кодов интересны многочлены с корнями из расширенных полей Галуа GF(2^m).

В соответствии с полученным результатом справедливо утверждение – *все ненулевые элементы GF(2^m) являются корнями $x^{2^m-1}-1$.*

Важно уметь сопоставлять совокупности элементов GF(q), в частном случае GF(2^m), с корнями неприводимых сомножителей x^{q-1}–1 (в двоичном случае с корнями $x^{2^m-1}-1$), ровно как и с корнями x^n-1 при произвольном n.

При выявлении сомножителей x^n-1 полезны следующие свойства, характеризующие связи между элементами GF(q), и многочленами, являющимися делителями x^n-1.

Свойство 1. Наличие в двучлене x^n-1 сомножителей вида x^m-1, где $m<n$. Пусть $n=m\times d$, где n, m и d – целые положительные числа. Рассмотрим двучлен y^d-1. Очевидно, что при y=1, он обращается в нуль, и 1 является корнем y^d-1.

Тогда по теореме Безу y^d-1 делится на y–1. Положим, что $y=x^m$. Тогда, очевидно, $x^{md}-1$ делится на x^m-1.

Таким образом, справедливо следующее: *многочлен x^n-1 делится на многочлен x^m-1, если m делит n.*

Свойство 2. Поля Галуа GF(p^m), образованные классами вычетов многочленов по модулю примитивного неприводимого над полем GF(p) многочлена $\pi(x)$ степени m, называют полями *характеристики* p при любом выборе m. В поле GF(p) элемент p=0.

В поле характеристики p для любых чисел a и b справедлива биномиальная теорема:

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + C_p^2 a^{p-2} b^2 + \ldots b^p,$$

где $\tilde{N}_p^i = \dfrac{p!}{i!(p-i)!}$ – биномиальные коэффициенты.

Поэтому справедливо: *в поле характеристики p имеет место равенство* $(a+b)^p = a^p + b^p$.

Свойство 3. Пусть многочлен $f(x)=a_0 + a_1 x + \ldots + a_m x^m$ степени m неприводим в поле GF(p). Рассмотрим $(f(x))^p$.

По предыдущему свойству:

$$(f(x))^p = (a_0)^p + (a_1 x^1)^p + \ldots + (a_m x^m)^p = a_0^p + a_1^p (x^p) + \ldots + a_m^p (x^p)^m =$$
$$= a_0 + a_1 (x)^p + \ldots + a_m (x^p)^m = f(x^p).$$

Этот результат получен в силу того, что для любого элемента a_i из GF(p) справедливо: $a_i^{p-1} = 1$ и $a_i^p = a_i$.

Пусть β − корень $f(x)$, тогда $f(\beta) = 0$.

В силу полученного результата $(f(\beta))^p = f(\beta^p) = 0$, т. е. для любого корня β многочлена $f(x)$ справедливо утверждение, что β^p также является корнем $f(x)$. Так как неприводимый многочлен $f(x)$ степени m имеет всего m корней и один из его корней есть β, то m степеней β от p^0=1 до p^{m-1} являются корнями $f(x)$.

Таким образом, справедливо: *если f(x) – многочлен степени m с коэффициентами из поля* GF(p)*, неприводимый в этом поле, и* β *– корень f(x), то* β, β^p, *…,* $\beta^{p^{m-1}}$ *– все корни f(x).*

Свойство 4. Прямым следствием из свойства 3 является следующее.

Все корни неприводимого многочлена имеют один и тот же порядок.

Для доказательства этого свойства предположим, что корнями некоторого неприводимого многочлена $f(x)$ степени m являются β, имеющий порядок e, и $\beta^{p^{m-1}}$, имеющий порядок l. Тогда $((\beta^{p^j})^e = (\beta^e)^{p^j} = 1^{p^j}$, и поэтому e делится на l. Аналогично, $\beta^l = (\beta^{p^m})^l = \beta^{p^j p^{m-j} l} = ((\beta^{p^j})^l)^{p^{m-j}} = 1p^{m-j} = 1$, так что l делится на e. Поскольку e и l – целые положительные числа, значит $e = l$, что и доказывает свойство 4.

Свойство 5. Выше показано однозначное соответствие между ненулевыми элементами GF(p^m) и корнями двучлена x^{p^m-1}. Определим вид многочлена, корнями которого являются все элементы поля GF(p^m). Пусть α – произвольный элемент поля порядка p^m–1.

Тогда справедливо: $\alpha^{p^m} = \alpha$, т. е. α является корнем уравнения $x^{p^m} - x = 0$.

Данный результат известен в литературе как теорема Ферма: ***любой элемент*** **α** ***поля*** **GF(*p^m*)** ***удовлетворяет тождеству*** $\alpha^{p^m} = \alpha$ ***или эквивалентно является корнем уравнения*** $x^{p^m} - x = 0$.

Следствием теоремы Ферма является тот факт, что двучлен $x^{p^m} - x$ может быть представлен в виде произведения p^m сомножителей следующим образом:

$$x^{p^m} - x = \prod_{i=1}^{p^m} (x - a_i),$$

где a_i= GF(p^m), т. е. все элементы a_i или GF(p^m) являются корнями двучлена $x^{p^m} - x$, причем каждый корень встречается только один раз.

Элемент поля GF(p^m) α порядка p^m –1 называется примитивным и любой ненулевой элемент поля является степенью α, т. е. для ненулевых элементов a_i справедливо $a_i = \alpha^i$, где i принимает значение от 1 до p^m –1.

Свойство 6. Свойство 3 устанавливает связь между корнями неприводимого многочлена $f(x)$. Естественно считать, что корень $f(x)$ – элемент расширенного поля GF(p^m). Какой может быть максимальная степень неприводимого многочлена с корнями из GF(p^m) или что то же самое – какова максимальная степень неприводимого сомножителя $x^{p^m} - x$?

Ответ на этот вопрос дает анализ возможной максимальной степени в последовательности корней:

$$\beta, \quad \beta^p, \quad \beta^{p^2}, \quad \beta^{p^{m-1}}.$$

Удобно рассматривать последовательность степеней в выражении корня через примитивный элемент поля $\alpha \in$GF(p^m), тогда приведенная выше последовательность корней однозначно соответствует последовательности степеней примитивного элемента:

$$\{s, \quad ps, \quad p^2 s, \quad p^3 s, \ldots, \quad p^{m_s - 1} s\},$$

где m_s – наименьшее положительное число такое, что $p^{m_s} \times s = s$ по модулю p –1.

Модуль p^m–1 отражает порядок примитивного элемента поля. В последовательности степеней корней следующая степень $\beta^{p^m} = \beta$.

Максимальная степень неприводимого многочлена в разложении $x^{p^m-1}-1$, равно как и в разложении многочлена x^{p^m} равна m.

Последовательность, взятая в фигурные скобки, получившая название циклотомического класса, в зависимости от значения s может содержать $m_s \le m$ элементов. Число s, стоящее в начале циклотомического класса, получило название образующего или представителя циклотомического класса. Ниже будет показано, что число элементов в циклотомическом классе m_s должно быть делителем числа m.

Справедливо следующее: *множество целых чисел, отображающих степени примитивного элемента* α *поля* GF(p^m) *в представлении ненулевых элементов поля в виде циклической группы, распадается на подмножества, называемые циклотомическими классами по модулю p^m–1. Каждый циклотомический класс однозначно соответствует одному из неприводимых сомножителей $x^{p^m-1}-1$.*

Понятно, что: *полное число циклотомических классов для поля* GF(p^m) *совпадает с числом неприводимых сомножителей многочлена $x^{p^m-1}-1$, и множество элементов, охватываемых циклотомическими классами, отображает все ненулевые элементы поля GF(p^m).*

Например, циклотомическими классами по модулю 15 для p=2 являются:

$C_{0(15)}$ ={0}, $C_{1(15)}$={1,2,4,8}, $C_{3(15)}$={3,6,12,9}, $C_{5(15)}$={5,10}, $C_{7(15)}$={7,14,13,11},

здесь $C_{s(15)}$ обозначает циклотомический класс по модулю 15, начинающийся с числа s.

Анализ приведенных последовательностей означает, что двучлен $x^{15}+1$ над полем GF(2) состоит из 5 неприводимых сомножителей: одного сомножителя 1-й степени с корнем порядка 1, одного сомножителя 2-й степени с корнем порядка 3 и трех сомножителей степени 4, два из которых имеют порядок корней 15, а один – имеет порядок корней 5.

Результаты этого анализа показывают, что последовательность $C_{0(15)}$ соответствует многочлену x+1; последовательность $C_{5(15)}$ соответствует многочлену 2-й степени с корнями порядка 3 – это многочлен x^2+x+1 – неприводимый сомножитель двучлена x^3+1; последовательность $C_{3(15)}$ соответствует неприводимому сомножителю 4-й степени двучлена $x^5+1=(x+1)(x^4+x^3+x^2+x+1)$, отсюда и порядок корней, равный пяти.

Многочлены, соответствующие последовательностям $C_{1(15)}$ и $C_{7(15)}$, могут быть найдены на основе теоремы Безу:

$$f_1(x)=(x+\alpha))(x+\alpha^2))(x+\alpha^4))(x+\alpha^8),$$
$$f_7(x)=(x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13}))(x+\alpha^{14}).$$

Анализ многочленов $f_1(x)$ и $f_7(x)$ будет выполнен далее.

Свойство 7. Анализ неприводимых многочленов, входящих в разложение $x^{2^4-1}+1$, имеющих корни среди элементов GF(2^4) показывает, что степени всех неприводимых многочленов: 1, 2, 4 являются делителями числа 4. Обобщим этот результат следующими рассуждениями.

Пусть $f(x)$ – неприводимый сомножитель степени $d \leq m$ многочлена $x^{p^m}-x$ и пусть β элемент порядка p^d–1 поля GF(p^m), являющийся примитивным элементом подполя GF(p^d) поля GF(p^m), принадлежит циклической группе GF(p^m) порядка p^m–1. Следовательно, p^d–1 делит p^m–1, а это возможно только в том случае, когда d делит m.

Значит, справедливо: *для простого числа p многочлен* $x^{p^m}-x$ *равен произведению всех нормированных неприводимых над* GF(*p*) *многочленов, степени которых делят m.*

Свойство 8. Аналогичные рассуждения приводят к следующему утверждению: *для любого поля* GF(*q*)*, где q=p^m (степень простого числа) имеет место равенство:* $x^{p^m}-x$ *равно произведению всех нормированных неприводимых над* GF(*p*) *многочленов, степени которых делят m.*

Свойство 9. Рассмотрим подробнее многочлены над GF(2):

$$f_1(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8),$$
$$f_7(x) = (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14}).$$

Корни этих многочленов являются элементами поля GF(2^4), с учетом правил сложения и умножения в этом поле простым умножением находим:

$$f_1(x) = 1+x+x^4,$$
$$f_7(x) = 1+x^3+x^4.$$

Многочлены $f_1(x)$ и $f_7(x)$ относятся к двойственным (взаимным) многочленам.

Многочлен $f^*(x)$, двойственный некоторому многочлену $f(x)$, определяется как $f^*(x) = x^m f(1/x)$, где m – степень $f(x)$.

Для двойственных многочленов $f^*(x)$ и $f(x)$ справедливо:

1) корни $f^*(x)$ обратны корням $f(x)$;

2) многочлен $f^*(x)$ неприводим тогда и только тогда, когда неприводим $f(x)$;

3) если многочлен $f(x)$ неприводим, то $f(x)$ и $f^*(x)$ принадлежат к одному и тому же показателю.

Порядок корней неприводимого многочлена называется показателем, которому этот многочлен принадлежит. Если неприводимый многочлен принадлежит показателю e, то он является делителем многочлена $x^e–1$, но не является делителем никакого многочлена $x^n–1$ при $n < e$.

Показатель, которому принадлежит многочлен, находится следующим образом. Пусть α *– примитивный элемент* GF(2^m), *тогда прядок e элемента* α^j:

$$e = (2^m - 1)/НОД(2^m - 1, j),$$

с другой стороны, порядок e элемента α^j *указывает минимальную степень многочлена $x^e–1$, делителем которого является неприводимый многочлен, для которого* α^j *есть корень* (НОД – *наибольший общий делитель*);

4) многочлен $f^*(x)$ примитивен тогда и только тогда, когда примитивен $f(x)$.

Возвращаясь к многочленам $f(x) = x^4+x+1$ и $f^*(x) = x^4+x^3+1$, отмечаем, что все сказанное относительно двойственных многочленов справедливо для этих многочленов:

- корни $f(x)$ – α^1, α^2, α^4, α^8 и корни $f^*(x)$ – α^7, α^{11}, α^{13}, α^{14} являются элементами поля GF(2^4), при этом $\alpha^1\,\alpha^{14} = \alpha^{15} = 1$; $\alpha^2\,\alpha^{13} = \alpha^{15} = 1$; $\alpha^4\,\alpha^{11} = \alpha^{15} = 1$; $\alpha^8\,\alpha^7 = \alpha^{15} = 1$;

- $f(x)$ и $f^*(x)$ – неприводимые многочлены, при этом

$$f_7(x) = x^4 f_1(1/x) = x^4\left(1+\frac{1}{x}+\frac{1}{x^4}\right) = x^4 + x^3 + 1;$$

- f_1(x) и f_7(x) принадлежат одному показателю 15, так как не являются делителями никакого двучлена меньшей степени.

Проверить этот факт можно непосредственным делением x^5+1, x^6+1 и т. д. на многочлены $f_1(x)$ и $f_7(x)$.

Найдем двучлен минимальной степени, делителем которого является

$$f_1(x)f_7(x) = f_{17}(x) = (x^4+x+1)(x^4+x^3+1) = x^8+x^7+x^5+x^4+x^3+x+1.$$

Воспользуемся приемом [5], который эффективнее, чем последовательное деление x^9+1, $x^{10}+1$ и т. д. на $f_{17}(x)$. Будем искать одночлен x^n, остаток от деления которого на $f_{17}(x)$ равен 1.

Остаток от деления x^8 на $f_{17}(x)$:

$$x^8 = x^7+x^5+x^4+x^3+x+1 \pmod{f_{17}(x)};$$
$$x^9 = x^8+x^6+x^5+x^4+x^2+x =$$

$x^7+x^5+x^4+x^3+x+1+x^6+x^5+x^4+x^2+x =$
$= x^7+x^6+x^3+x^2+1 \pmod{f_{17}(x)};$
$x^{10} = x^8+x^7+x^4+x^3+x =$
$= x^7+x^5+x^4+x^3+x+1+x^7+x^4+x^3+x =$
$= x^5+1 \pmod{f_{17}(x)};$
$x^{11} = x^6+x \pmod{f_{17}(x)};$
$x^{12} = x^7+x^2 \pmod{f_{17}(x)};$
$x^{13} = x^8+x^3 = x^7+x^5+x^4+x^3+x+1+x^3 =$
$= x^7+x^5+x^4+x+1 \pmod{f_{17}(x)};$
$x^{14} = x^8+x^6+x^5+x^2+x =$
$= x^7+x^5+x^4+x^3+x+1+x^6+x^5+x^2+x =$
$= x^7+x^6+x^4+x^3+x^2+1 \pmod{f_{17}(x)};$
$x^{15} = x^8+x^7+x^5+x^4+x^3+x =$
$=x^7+x^5+x^4+x^3+x+1+x^7+x^5+x^4+x^3+x = 1 \pmod{f_{17}(x)}.$

Итак, $x^{15}+1$ – двучлен минимальной степени, сомножителем которого является $(x^4+x+1)(x^4+x^3+1)$.

2.2. Минимальные многочлены и их свойства

Выше было показано, что между корнями $x^q–x$ и элементами GF(q), где $q=p^m$ существует однозначное соответствие, заключающееся в том, что каждый элемент β из GF(q) является корнем $x^q–x$.

При этом коэффициенты многочлена $x^q–x$ и его неприводимых сомножителей являются элементами поля GF(q). Элемент β, являясь корнем $x^q–x$, является корнем одного из его сомножителей.

Минимальным многочленом элемента β *из поля* GF(p^m) *называют нормированный многочлен минимальной степени m(x) с коэффициентами из поля* GF(p)*, такой, что m*(β)*=0.*

Пример 2.2.1. Минимальные многочлены для элементов поля GF(2^4):

Элемент	Минимальный многочлен
0	x
1	$x+1$
α	x^4+x+1
$\alpha^{-1} = \alpha^{14}$	x^4+x^3+1
α^3	$x^4+x^3+x^2+x+1$
α^5	x^2+x+1

Процесс нахождения минимальных многочленов будет обобщен в п. 2.4.

2.3. Свойства минимальных многочленов над полем GF(p)

1. *Минимальный многочлен неприводим.*

Действительно, если $m(x) = m_1(x)m_2(x)$, то $m(\beta) = m_1(\beta)\ m_2(\beta) = 0$, то либо $m_1(\beta) = 0$, либо $m_2(\beta) = 0$, что противоречит определению.

2. *Если некоторый многочлен $f(x)$ с коэффициентами из* GF(p) *такой, что $f(\beta) = 0$, то минимальный многочлен $m(x)$ для* β *делит $f(x)$.*

Из свойства 2 имеем:

3. *Минимальный многочлен $m(x)$ степени m является делителем $x^{p^m} - x$.*

Из свойства 3 следует:

4. *Степени минимальных многочленов $m(x)$ для элементов поля* GF(p^m) *не превышают m.*

С учетом сказанного, справедливо

5. *Если корень* β *является примитивным элементом* GF(p^m), *то $m(x)$ для* β *имеет степень, равную m.*

Как найти $m^{(i)}(x)$ минимальный многочлен для $\beta = \alpha^i$ из GF(p^m)?

Если i лежит в циклотомическом классе $C_{s(p^m-1)}$, то

6. $m^{(i)}(x) = \prod\limits_{j \in C_{s(p^m-1)}} (x - \alpha^j)$.

Из свойства 3 непосредственно вытекает:

7. $x^{p^m-1} - 1 = \prod\limits_{s} m^{(s)}(x)$,

где s пробегает все множество представителей циклотомических классов по модулю p^m–1.

Полученный результат конкретизирует свойство 5.

Пример 2.3.1. В соответствии с данными примера 2.2.1 произведение всех минимальных многочленов для элементов поля GF(2^4) равно

$$x(x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)=x^{16}+x, \text{ откуда}$$

$$(x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)=x^{15}+1.$$

2.4. Разложение x^n–1 на неприводимые сомножители

Ранее циклотомические классы были определены по модулю p^m–1. В более общем случае можно определить циклотомический класс по модулю n над GF(p) как множество

$$C_{s(n)} = \{s, sp, sp^2, sp^{m_s-1}\},$$

где $sp^{m_s} = s(\text{mod } n)$.

При этом множество всех чисел по модулю n разбивается на циклотомические классы

$$\{0\}, \{1\}, \{l\}, \ldots, \{n–1\} = \bigcup_s C_{s(p^m-1)}.$$

Значение числа m_s было определено выше. Связь между циклотомическими классами по модулю $p^m–1$ и n определяется следующим образом: *число чисел m_1 в классе $C_{1(n)}$ равно степени расширения поля, для которого многочлен степени m_1, является примитивным, т. е. $\bigcup_s C_{s(n)}$, является составной частью $\bigcup_s C_{s(p^m-1)}$, где $m = m_1$.*

Например, для $n = 9$ и $p = 2$ имеем 3 циклотомических класса:

$$C_{0(9)} = \{0\}, C_{1(9)} = \{1, 2, 3, 4, 8, 7, 5\}, C_{3(9)} = \{3, 6\}.$$

Это значит, что x^9+1 над двоичным полем разлагается на 3 неприводимых сомножителя: 1-й степени (x+1), 2-й степени (x^2+x+1) и многочлен 6-й степени. При этом порядок корней многочлена 2-й степени равен 3,так как x^2+x+1 принадлежит показателю 3, а порядок корней неприводимого многочлена 6-й степени равен 9 (принадлежит показателю 9).

В соответствии с сформулированными выше правилами $x^9 + 1$ является сомножителем $x^{2^6-1}+1$, так как класс $C_{1(9)}$ содержит 6 чисел, и корни x^9+1 могут быть выражены в виде степеней примитивного элемента поля GF(2^6).

Определим порядок пересчета корней $x^{n_j}-1$ в элементы поля GF(p^m), т. е. найдем, какие корни $x^{n=p^m-1}-1$ являются корнями $x^{n_j}-1$, при условии, конечно, что n_j меньше n и является его сомножителем .

Если порядок корней x^n-1 есть e, а порядок корней его сомножителей, принадлежащих показателю n_j, т. е. входящих в разложение $x^{n_j}-1$, где $n_j < n$, равен $\frac{e}{n/n_j}$, то, очевидно, *образующий циклотомического класса неприводимого многочлена f(x) по модулю $n=p^m–1$, большего n_j и делящегося на него, в $j = n/n_j$ раз больше образующего циклотомического класса того же неприводимого многочлена.*

Следовательно, циклотомическому классу по модулю 9 $C_{1(9)} = \{1, 2, 4, 8, 7, 5\}$ соответствует по модулю 63 циклотомический класс

$C_{7(63)}$ = {7,14,28,56, 49, 35}, так как = $\frac{63}{9}$ = 7, а циклотомичекому классу $C_{3(9)}$ = {3,6} соответствует циклотомический класс $C_{21(63)}$ = {21, 42}.

Как и ранее, подстрочный индекс в скобках в обозначении циклотомического класса указывает модуль $n_j \le n$, по которому найдены последовательности корней, отображаемых числами, входящими в циклотомический класс, а число перед ним – образующий циклотомического класса.

Минимальное число n_j в обозначении циклотомического класса данного набора корней равно показателю, которому принадлежит многочлен с данными корнями, т. е. порядку этих корней.

Заметим, что неприводимый многочлен, соответствующий некоторому циклотомическому классу, является минимальным многочленом для корней, отображаемых этим циклотомическим классом.

Таким образом, разложение $x^n - 1$ на неприводимые сомножители сводится к поиску минимальных многочленов для корней $x^n - 1$.

Число корней, имеющих порядок *e*, определяется функцией Эйлера φ(*e*).

Если *s* − число, указывающее первый подстрочный индекс в обозначении циклотомического класса, то при модуле n=2^m–1 порядок корней циклотомического класса определяется следующим выражением:

$$e = \frac{2^m - 1}{\text{НОÄ}(2^m - 1, s)}.$$

Проиллюстрируем все отмеченное рассмотрением следующего примера.

*Пример 2.4.1***.** Разложим x^{63}+1 на неприводимые сомножители над двоичным полем.

В соответствии с теоремой Ферма над полем GF(2)

$$x^{63} + 1 = \prod_{i=0}^{63} (x + \alpha^i), \text{ где } \alpha^i \in \mathrm{GF}(2^6).$$

Таким образом, поиск неприводимых сомножителей x^{63}+1 сводится к распределению элементов поля GF(2^6) α^i по неприводимым сомножителям x^{63}+1 в соответствии с циклотомическими классами по модулю 63 и синтезу минимальных многочленов, соответствующих каждому циклотомическому классу.

Распределение элементов поля GF(2^6) α^i по неприводимым сомножителям x^{63}+1 в соответствии с циклотомическими классами по модулю 63 имеет вид:

$C_{0(63)}$ = {0}
$C_{1(63)}$ = {1, 2, 4, 8, 16,32}
$C_{3(63)}$ = {3, 6, 12, 24, 48, 33}
$C_{5(63)}$ = {5, 10, 20, 40, 17, 34}
$C_{7(63)}$ = {7, 14, 28, 56, 49, 35}
$C_{9(63)}$ = {9, 18, 36}
$C_{11(63)}$ = {11, 22, 44, 25, 50, 37}
$C_{13(63)}$ = {13,26, 52, 41, 19, 38}
$C_{15(63)}$ = {15, 30, 60, 57, 51, 39}
$C_{21(63)}$ = {21,42}
$C_{23(63)}$ = {23,46, 29, 58, 53, 43}
$C_{27(63)}$ = {27, 54, 45}
$C_{31(63)}$ = {31,62, 61 ,59, 55,47}

В табл. 2.4.1 приведены многочлены, соответствующие найденным циклотомическим классам, и порядок их корней.

Таблица 2.4.1

Циклото-мический класс	Состав циклотомического класса	Минимальный многочлен	Порядок корней многочлена $e = \dfrac{63}{\text{НОÄ}(s, 63)}$
$C_{0(63)}$	{0 = 63}	x+1	1
$C_{1(63)}$	{1, 2, 4, 8, 16, 32}	x^6+x+1	63
$C_{3(63)}$	{3, 6, 12, 24, 48, 33}	$x^6+x^4+x^2+x+1$	21
$C_{5(63)}$	{5, 10, 20, 40, 17, 34}	$x^6+x^5+x^2+x+1$	63
$C_{7(63)}$	{7, 14, 28, 56 49, 35}	x^6+x^3+1	9
$C_{9(63)}$	{9, 18, 36}	x^3+x^2+1	7
$C_{11(63)}$	{11, 22, 44, 25, 50, 37}	$x^6+x^5+x^3+x^2+1$	63
$C_{13(63)}$	{13, 26, 52, 41, 19, 38}	$x^6+x^4+x^3+x+1$	63
$C_{15(63)}$	{15, 30, 60, 57, 51, 39}	$x^6+x^5+x^4+x^2+1$	21
$C_{21(63)}$	{21,42}	x^2+x+1	3
$C_{23(63)}$	{23, 46, 29, 58, 53, 43}	$x^6+x^5+x^4+x+1$	63
$C_{27(63)}$	{27, 54, 45}	x^3+x+1	7
$C_{31(63)}$	{31, 62, 61, 59, 55, 47}	x^6+x^5+1	63

Многочлены получены из таблиц, приведенных в [1] и помещенных в приложении. Правила пользования таблицами приводятся ниже.

Анализ приведенных в табл. 2.4.1 многочленов показывает, что в разложение $x^{63}+1=x^{2^6-1}+1$ входят многочлены 1, 2, 3 и 6-й степеней. Эти числа представляют все делители числа 6. Порядок корней многочленов указывает, какому показателю принадлежат многочлены.

Если воспользоваться функцией Эйлера, можно определить число элементов поля $GF(2^6)$, принадлежащих указанным в таблице порядкам 1, 3, 7, 9, 21, 63:

$\varphi(1) = 1$ − это один корень $x+1$,

$\varphi(3) = 2$ − это два корня x^2+x^3+1,

$\varphi(7) = 6$ − это корни двойственных многочленов x^3+x^2+1 и x^3+x+1,

$\varphi(9) = 6$ − это корни самодвойственного многочлена x^6+x^3+1,

$\varphi(21) = 12$ – это корни двойственных многочленов: $x^6+x^4+x^2+x+1$ и $x^6+x^5+x^4+x^2+1$,

$\varphi(63) = 32$ − это корни 6 примитивных попарно двойственных многочленов x^6+x+1 и x^6+x^5+1, $x^6+x^5+x^2+x+1$ и $x^6+x^5+x^4+x+1$, $x^6+x^5+x^3+x^2+1$ и $x^6+x^4+x^3+x+1$.

На этом процесс разложения $x^{63}+1$ на неприводимые сомножители завершен.

Пример 2.4.2. Построить циклотомические классы по модулю степеней двучленов, делящих $x^{63}+1$.

$x+1$, $j = 63$	$C_{0(1)} = \{0 = 1\}$	$C_{0(63)} = \{0 = 63\}$
x^3+1, $j = 21$	$C_{0(3)} = \{0 = 3\}$	$C_{0(63)} = \{0 = 63\}$
	$C_{1(3)} = \{1, 2\}$	$C_{21(63)} = \{21, 42\}$
x^7+1, $j = 9$	$C_{0(7)} = \{0 =7\}$	$C_{0(63)} = \{0 = 63\}$
	$C_{1(7)} = \{1, 2, 4\}$	$C_{9(63)} = \{9, 18, 36\}$
	$C_{3(7)} = \{3, 6, 5\}$	$C_{27(63)} = \{27, 54, 45\}$
x^9+1, $j = 7$	$C_{0(9)} = \{0 = 9\}$	$C_{0(63)} = \{0 = 63\}$
	$C_{1(9)} = \{1, 2, 4, 8, 7, 5\}$	$C_{7(63)} = \{7, 14, 28, 56, 49, 35\}$
	$C_{3(9)} = \{3, 6\}$	$C_{21(63)} = \{21, 42\}$
$x^{21}+1$, $j = 3$	$C_{0(21)} = \{0 = 21\}$	$C_{0(63)} = \{0 = 63\}$
	$C_{1(21)} = \{1, 2, 4, 8, 16, 11\}$	$C_{3(63)} = \{3, 6, 12, 24, 48, 33\}$
	$C_{3(21)} = \{3, 6, 12\}$	$C_{9(63)} = \{9, 18, 36\}$
	$C_{5(21)} = \{5, 10, 20, 19, 17, 13\}$	$C_{15(63)} = \{15, 30, 60, 57, 51, 39\}$
	$C_{7(21)} = \{7, 14\}$	$C_{21(63)} = \{21, 42\}$
	$C_{9(21)} = \{9, 18, 15\}$	$C_{27(63)} = \{27, 54, 45\}$

Таким образом, найдены все неприводимые многочлены, входящие в разложение $x^{63}+1$ с порядком корней, меньшим 63.

В качестве представителей циклотомических классов s используют наименьшие числа в классе. При построении циклотомических классов они выбираются как минимальные числа, не вошедшие в предыдущие классы. Представители циклотомических классов используются в качестве первого подстрочного индекса в обозначении класса.

Вид многочленов, соответствующих циклотомическим классам, в рассмотренном примере взят из таблиц неприводимых многочленов над полем GF(2), представленных в [1] (таблицы в усеченном виде даны в приложении). Неприводимые многочлены расположены по степеням m.

Число m определяет степень расширения поля GF(2^m), элементами которого являются корни представленных многочленов. Под числом m показаны все неприводимые многочлены со степенями, делящими m, кроме многочлена $x+1$.

Для многочлена указана характеристика в виде цифры, являющейся представителем циклотомического класса, соответствующего указанному многочлену по модулю 2^m–1, и латинской буквы (только для многочленов степени m), несущей следующую информацию о многочлене:

A, B, C, D	–	непримитивный
E, F, G, H	–	примитивный
A, B, E, F	–	корни линейно зависимы
C, D, G, H	–	корни линейно независимы
A, C, E, G	–	корни двойственного многочлена линейно зависимы
B, D, F, H	–	корни двойственного многочлена линейно независимы.

Из двойственных многочленов в таблице (см. приложение) представлен лишь тот, у которого представитель циклотомического класса меньше по величине. Многочлены даны в двоично-восьмеричном представлении. Каждый символ в таблице обозначает три двоичных знака в соответствии со следующим кодом: 0 = 000, 1 = 001, 2 = 010, 3 = 011, 4 = 100, 5 = 101, 6 = 110, 7 = 111.

Коэффициенты многочленов расположены в порядке убывания, т. е. коэффициент при старшей степени расположен слева.

Например, первый многочлен при степени 6 записан в виде: 1 103 F. В двоичной записи числу 103 эквивалентно число 001000011, и соответствующий многочлен равен x^6+x+1. Буква F означает, что многочлен примитивный, его корни линейно зависимы, а корни двойственного многочлена линейно независимы. Цифра, стоящая перед двоично-восьмеричным представлением многочлена (в приведенном примере это 1), есть представитель циклотомического класса этого многочлена по модулю $x^{2^m-1}-1$ (в примере по модулю $x^{63}+1$).

При вычислении порядка корней e неприводимого многочлена или, что то же самое – показателя, к которому принадлежит данный многочлен, полезны данные табл. 2.4.2.

Таблица 2.4.2

Разложение 2^m-1 на простые сомножители	
$2^3-1=7$	$2^{19}-1=524287$
$2^4-1=3\times5$	$2^{20}-1=3\times5\times5\times11\times31\times41$
$2^5-1=31$	$2^{21}-1=7\times7\times127\times337$
$2^6-1=3\times3\times7$	$2^{22}-1=3\times23\times89\times683$
$2^7-1=127$	$2^{23}-1=47\times178481$
$2^8-1=3\times5\times17$	$2^{24}-1=3\times3\times5\times7\times13\times17\times241$
$2^9-1=7\times73$	$2^{25}-1=31\times601\times1801$
$2^{10}-1-=3\times11\times31$	$2^{26}-1=3\times2731\times8191$
$2^{11}-1=23\times89$	$2^{27}-1=7\times73\times262657$
$2^{12}-1=3\times3\times5\times7\times13$	$2^{28}-1=3\times5\times29\times43\times113\times127$
$2^{13}-1=8191$	$2^{29}-1=233\times1103\times2089$
$2^{14}-1=3\times43\times127$	$2^{30}-1=3\times3\times7\times11\times31\times151\times331$
$2^{15}-1=7\times31\times151$	$2^{31}-1=2147483647$
$2^{16}-1=3\times5\times17\times257$	$2^{32}-1=3\times5\times17\times257\times65537$
$2^{17}-1=131071$	$2^{33}-1=7\times23\times89\times599479$
$2^{18}-1=3\times3\times3\times7\times19\times73$	$2^{34}-1=3\times43691\times131071$

2.5. Алгоритм разложения x^n+1 на неприводимые сомножители

Обобщением вышеизложенного в отношении разложения двучлена вида x^n+1 на неприводимые над двоичным полем сомножители представлено в виде приведенного алгоритма, применение которого проиллюстрируем двумя примерами.

Пример 2.5.1. Разложить $x^{21}+1$ на неприводимые сомножители над GF(2).

Шаг 1. Задано значение степени двучлена $n=21$.

Шаг 2. Заданное значение $n=21$ не может быть представлено в виде $n=2^m-1$.

Шаг 3. Из табл. 2.4.2 находим ближайшее к 21 число, которое делится на 21 и может быть представлено в виде 2^m-1. Таким числом является 63, т. е. $\eta=63$ и $m=6$.

Шаг 4. Неприводимые сомножители $x^{21}+1$ были рассмотрены в примере 2.4.1. Как они были определены? Число 21=3×7. Это означает, что в разложение $x^{21}+1$ входят неприводимые сомножители двучленов x^3+1 и x^7+1. Порядок их корней – 3 и 7 соответственно. Кроме того, $x^{21}+1$, безусловно, имеет корни порядка 21.

Шаг 5. Число корней порядка 3 равно $\varphi(3) = 2$, порядка 7 – $\varphi(7) = 6$ и порядка 21– $\varphi(21)=\varphi(3)\times\varphi(7) =2\times6= 12$.

Шаг 6. Итак, двучлен $x^{21}+1$ имеет корни различного порядка.

Шаг 7. Помимо $x+1$ в разложение $x^{21}+1$ входят:

- многочлен степени 2 с корнями порядка 3,
- 2 многочлена степени 3 с корнями порядка 7.

Новое значение $\eta=2^6-1$ позволяет определить, что 12 корней порядка 21 принадлежат двум многочленам степени 6.

Итак, в разложение $x^{21}+1$ входят следующие неприводимые сомножители: по одному степеней 1 и 2 и по два – 3 и 6.

Шаг 8. Строим циклотомические классы по модулю 21 и преобразуем их представителей по модулю $\eta=2^6-1$:

$\{1, 2, 4, 8, 16, 11\} \rightarrow \{3,\ldots\}$,
$\{3, 6, 12\} \rightarrow \{9,\ldots\}$,
$\{5, 10, 20, 19, 17, 13\} \rightarrow \{15,\ldots\}$,
$\{7, 14\} \rightarrow \{21,\ldots\}$,
$\{9, 18, 15\} \rightarrow \{27, \ldots\}$.

Шаг 9. В разложение $x^{21}+1$ входят двойственные многочлены степеней 3 и 6.


Начальные условия:
задано n
$n=2^m-1$?
Нет
Нахождение
нового $n = \eta$
Да
Определение порядка корней
неприводимых сомножителей x^n+1
Определение числа корней
каждого порядка
Корни имеют
один порядок?
Да
Нет
Вычисление степеней
неприводимых сомножителей
и их числа с корнями каждого порядка
Построение циклотомических классов
и нахождение их представителей
Нахождение двойственных многочленов
для неприводимых сомножителей
Нахождение неприводимых
сомножителей по их корням
или по таблицам
Все неприводимые
сомножители найдены?
Нет
Да
Конец

Шаг 10. Из таблиц приложения для степени 6 находим по представителям циклотомических классов многочлены:

3 127 B $\to x^6 + x^4 + x^2 + x + 1$ и двойственный ему $x^6 + x^5 + x^4 + x^2 + 1$,

9 015 $\to x^3 + x^2 + 1$ и двойственный ему $x^3 + x + 1$,

21 007 $\to x^2 + x + 1$.

Найденные пять неприводимых многочленов совместно с многочленом $x+1$ представляют все неприводимые сомножители двучлена $x^{21}+1$.

Пример 2.5.2. Найти неприводимые сомножители $x^{13}+1$ над GF(2)**.**

Шаг 1. Степень разлагаемого двучлена равна 13.

Шаг 2. Число 13 не может быть представлено в виде $2^m - 1$.

Шаг 3. Ближайшее целое число, большее числа 13, которое может быть представлено в виде $2^m - 1$ и делится на 13, есть $\eta = 2^{12} - 1$ (табл. 2.4.2).

Шаг 4. Порядок корней двучлена $x^{13}+1$ равен $\varphi(13) = 12$.

Шаг 5. Все корни двучлена $x^{13}+1$ кроме корня $x = 1$, имеют порядок 12.

Шаг 6. См. шаг 5.

Шаг 7. Может быть пропущен.

Шаг 8. Циклотомический класс по модулю 13:
{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7}, т. е. в разложение двучлена $x^{13}+1$ входит неприводимый многочлен степени 12, принадлежащий показателю 13. По модулю $\eta = 2^{12} - 1$ этому многочлену соответствует циклотомический класс с представителем $s = (2^{12} - 1)/13 = 315$.

Шаг 9. Может быть пропущен.

Шаг 10. Из таблиц приложения для степени 12 определяем, что искомый многочлен – 315 17777 D. Этот результат вполне ожидаем и мог быть определен еще на шаге 4.

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ

В каждом из 6 разделов студент должен ответить на 1 вопрос или решить одну задачу, в зависимости от задания. Студент должен решить в итоге 6 заданий, которые выбирает самостоятельно из перечня, приведенного в каждой теме.

1. Основные алгебраические системы, используемые в теории кодирования

Линейные коды и математический аппарат, используемый для их описания и построения.

Группа, кольцо, поле. Примеры использования в теории кодирования.

Подгруппы и смежные классы.

Действия над смежными классами.

Литература: см. 1.1 и 1.2.

Цель. Изучить основные алгебраические системы, используемые в теории помехоустойчивого кодирования. Получить навыки в решении задач, связанных с понятиями группа, кольцо, поле.

Контрольные вопросы

1.1. Показать, что множество всех целых чисел (положительных, отрицательных и нуля) является группой по операциям:

а) обычного сложения G_+,

б) обычного умножения $G_\times$.

В группе G_+ по операции сложения выделить подгруппу, состоящую из чисел:

а) кратных 3,
б) кратных 4,
в) кратных 5.

Построить смежные классы для каждой из этих подгрупп.

1.2. Проверить, обладают ли полученные в п. 1.1 смежные классы групповыми свойствами:

а) по операции сложения,
б) по операции умножения.

1.3. Являются ли образованные в п. 1.2 смежные классы кольцом? Почему?

1.4. Являются ли образованные в п. 1.2 смежные классы полем? Почему?

1.5. Построить все возможные двоичные последовательности длины 5. Являются ли они группой по операции поразрядного сложения по mod 2? Доказать.

1.6. Образовать все возможные подгруппы в группе двоичных последовательностей длины 5 по операции, введенной в п. 1.5.

(Рассмотреть элементы группы как вектора и воспользоваться понятием базиса векторного пространства. Для каждой подгруппы указать ее порядок).

1.7. Для каждой найденной подгруппы в п. 1.6 найти подгруппу из этого же множества с ортогональными векторами. Ортогональности векторов соответствует равенство нулю их скалярного произведения.

1.8. Что нужно сделать, чтобы все последовательности длины 5 из п. 1.5 стали кольцом?

1.9. Является ли кольцо из п. 1.8 полем?

1.10. Какие подполя существуют в поле из всех двоичных последовательностей длины 5?

1.11. Проверить, что элементы поля $GF(2^2)$ α и $1+\alpha$ являются корнями многочлена $\pi(x)=1+x+x^2$ в двоичном поле.

Примеры решения задач и дополнительные задачи

1.12. Перечислить групповые аксиомы и привести примеры по их выполнению для операций сложения и умножения.

Решение

I. Замкнутость:

$a, b \in G$; $a \square b=c \in G$.

II. Ассоциативность:

$(a \square b) \square c=a \square (b \square c)$, где $a, b, c \in G$.

III. Наличие единичного элемента e:

$a \square e=e \square a$, где $e, a \in G$.

IV. Наличие обратных элементов a':

$a \square a' = a' \square a=e$, где $a, a', e \in G$.

V. Коммутативность:

$a \square b=b \square a$, где $a, b \in G$.

VI. Дистрибутивность:

$(a + b)\, c=ac+bc$, где $a, b, c \in G$.

В I–V $\square$ означает либо + (операция сложения), либо × (операция умножения).

1.13. Число p – простое число. Дать определение простого поля, указать число элементов и сформировать таблицы сложения и умножения для $p = 2$ и 3.

Решение

а) $p = 2$:

GF(2) – совокупность классов вычетов по mod 2, удовлетворяющая групповым аксиомам по операциям сложения и умножения:

- замкнутость,
- ассоциативность,
- наличие единичного элемента,
- наличие обратных элементов,
- коммутативность,
- дистрибутивность.

Сформируем классы вычетов:

…	–10	–8	–6	–4	–2	{0}	2	4	6	8	10	…
…	–9	–7	–5	–3	–1	{1}	3	5	7	9	11	…

Поле GF(2) содержит 2 элемента 0 и 1; 0={0}, 1={1}.

Таблицы сложения и умножения:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

б) p = 3:

GF(3) – совокупность классов вычетов по mod 3:

…	–12	–9	–6	–3	{0}	3	6	9	12	…
…	–11	–8	–5	–2	{1}	4	7	10	13	…
…	–10	–7	–4	–1	{2}	5	8	11	14	…

Классы вычетов удовлетворяют групповым аксиомам по операциям сложения и умножения (см. п. а)

Поле содержит 3 элемента 0, 1, 2; 0 ={0}, 1={1}=1, 2={2}.

Таблицы сложения и умножения:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

1.14. Задана совокупность всех двоичных последовательностей длины 3: **000 , 001 , 010 , 011 , 100 , 101 , 110 , 111.** Найти последовательности, ортогональные каждой из перечисленных.

Решение

Последовательности ортогональны, если их скалярное произведение равно 0.

Умножение двоичных последовательностей выполняется по правилам скалярного произведения векторов над двоичным полем, т.е. с использованием таблиц сложения и умножения по mod 2.

000 – ортогональна всем последовательностям,
так как $(000)\times(e_1e_2e_3) = 0\times e_1 + 0\times e_2 + 0\times e_3 = 0$ для любого $e_i = 0$ или 1.

001 – ортогональна всем последовательностям, содержащим 0 в крайнем справа разряде: 000, 100, 010, 110.

010 – ортогональна всем последовательностям, содержащим 0 в среднем разряде: 000, 001, 100, 101.

011 – ортогональна всем последовательностям, содержащим только нули или только единицы в двух крайних справа разрядах: 000, 011, 100, 111.

Для остальных последовательностей приведем ортогональные последовательности без пояснений (проверить самостоятельно):

100 – 000, 001, 010, 011.
101 – 000, 010, 101, 111.
110 – 000, 001, 110, 111.
111 – 000, 011, 101, 110.

Отметим, что двоичные последовательности с четным числом единиц (в рассмотренном примере – 000, 011, 101 и 110) являются самоортогональными.

1.15. Задана совокупность двоичных последовательностей длины 3: 000, 001, 010, 011. Показать, что данная совокупность является подгруппой всех возможных двоичных последовательностей длины 3. Найти совокупность двоичных последовательностей, ортогональных заданной. Показать, что найденная совокупность также является подгруппой всех двоичных последовательностей длины 3. Найти базисы заданной совокупности и ортогональной ей. Показать, что произведение найденных базисов по правилам умножения матриц дает чисто нулевую матрицу.

Решение

1. Для того чтобы показать, что совокупность 000, 001, 010, 011 является подгруппой всех восьми двоичных последовательностей длины 3, необходимо установить, что эта совокупность удовлетворяет групповым аксиомам. Проверка выполнения групповых аксиом сводится к проверке замкнутости элементов совокупности по операции поразрядного сложения по mod 2 при наличии среди элементов совокупности нулевой последовательности.

Легко убедиться, что и то, и другое имеет место; при этом порядок подгруппы равен 4, т. е. делит порядок группы.

2. Ортогональными к заданным последовательностям являются последовательности 000 и 100, которые также образуют подгруппу размерности 2 всех двоичных последовательностей длины 3.

3. Базис последовательностей 000, 001, 010, 011 представляется матрицей: $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Действительно, все последовательности заданной совокупности могут быть получены как линейная комбинация строк базисной матрицы:

$$W = c_1\,(010) + c_2(001), \text{ где } c_i \text{ – элементы GF(2).}$$

4. Базис совокупности ортогональных последовательностей представляется матрицей: $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$.

5. Умножение матриц $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ и $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$ возможно только в том случае, когда одна из них транспонирована: $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ или $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Выполнить умножение матриц самостоятельно и убедиться в ортогональности рассмотренных подгрупп.

1.16. Используя таблицы сложения и умножения для полей GF(2) и GF(3), приведенные в 1.13, определить, чему равны суммы и произведения пар чисел 1 и 2, 2 и 3, 3 и 4, 4 и 5, 5 и 6, 6 и 7 по mod 2 и по mod 3.

1.17. Показать, что пространство строк матрицы $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ содержит последовательности 000, 001, 010, 011.

2. Кольца многочленов и поля Галуа

Идеал кольца и классы вычетов кольца целых чисел – по модулю m и многочленов – по модулю многочлена $f(x)$.

Размерность идеала кольца классов вычетов многочленов по модулю многочлена $f(x)=g(x)h(x)$, где $f(x)$ имеет степень n, $g(x)$ – степень $n–k$, $h(x)$ – степень k.

Простые и расширенные поля Галуа, подполя.

Циклическая группа расширенного поля Галуа, порядок элементов поля (группы), число элементов некоторого порядка.

Примитивные элементы поля и примитивные многочлены.

Литература: см. 1.3 и 1.4.

Цель. Изучить структуру числовых колец и колец многочленов, способы формирования идеалов колец, связь между кольцами классов вычетов многочленов и конечными полями. Получить навыки формирования идеалов заданного порядка.

Контрольные вопросы

2.1. Над полем GF(2) заданы многочлены $p_1(x)=x^3+1$ и $p_2(x)=x^4+x^3+x+1$:

а) найти наибольший общий делитель этих многочленов НОД $[p_1(x), p_2(x)]$ (указание: использовать алгоритм Евклида);

б) найти многочлены A(x) и B(x), удовлетворяющие равенству:

$$\text{НОД}\,[p_1(x), p_2(x)] = \mathrm{A}(x)\, p_1(x) + \mathrm{B}(x)\, p_2(x).$$

2.2. Сколько различных многочленов второй степени вида x^2+ax+b, где a и b – элементы GF(2) имеется над полем GF(2)?

2.3. Сколько различных многочленов вида $(x–\alpha)(x–\beta)$, где α и β не равны 0, имеется над полем $GF(2^4)$, сколько из них неприводимых над этим полем? Сколько из них неприводимо над полем GF(2)?

2.4. Используя алгоритм Евклида, найти НОД (1573,308) и целые числа А и В, удовлетворяющие равенству НОД (1573,308) = 1573A+308B.

2.5. Доказать, что в кольце целых чисел по модулю 15 многочлен $p(x)=x^2–1$ имеет более двух корней, а в поле $GF(2^3)$ – один. Чему равно значение этих корней?

2.6. Сколько различных многочленов над GF(2) делят многочлен $x^6–1$?

2.7. Построить поле GF(5), выписав для него таблицы сложения и умножения. Определить порядок ненулевых элементов поля.

2.8. Определить возможные порядки ненулевых элементов GF(7). Сколько элементов каждого порядка имеется? Указать порядок каждого ненулевого элемента из этого поля.

2.9. Вычислить 3^{100} (mod 5).

2.10. Доказать, что многочлен x^2+x+1 неприводим над GF(2). В каком поле корни этого многочлена являются примитивными элементами? Построить это поле.

2.11. Доказать, что многочлен x^3+x+1 неприводим над GF(2). В каком поле корни этого многочлена являются примитивными элементами? Построить это поле.

2.12. Сколько примитивных элементов имеет поле $GF(2^3)$? Корнями каких многочленов они являются?

2.13. Построить поле $GF(2^4)$:

а) по модулю многочлена $\pi(x)=1+ x+x^4$;

б) по модулю многочлена $\pi(x)=1+ x^3+x^4$;

в) каков порядок корней этих многочленов?

г) каков порядок остальных ненулевых элементов $GF(2^4)$?

д) каким многочленом (указать степень) принадлежат в качестве корней ненулевые элементы $GF(2^4)$ из п. б?

2.14. Показать, что поле $GF(2^2)$ является подполем $GF(2^4)$.

2.15. Какие подполя содержит $GF(2^8)$?

2.16. Сколько идеалов существует в кольце многочленов по модулю многочлена $f(x)$ над полем GF(2), если идеалы образуют все многочлены, кратные каждому неприводимому сомножителю многочлена $f(x)$? Какова размерность идеалов:

а) $f(x) = x^3+1$;

б) $f(x) = x^7+1$.

Примеры решения задач и дополнительные задачи

2.17. Показать, что для p = 4 поле целых чисел GF(p) не существует.

Решение

Элементы GF(4): {0}, {1}, {2}, {3}.

Составим таблицы сложения и умножения:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Из анализа таблиц сложения и умножения делаем выводы:

1) по операции сложения существует единичный элемент 0 и для каждого элемента поля есть обратный: для 0 – это 0, для 1 – это 3, для 2 – это 2, для 3 – это 1;

2) по операции умножения существует единичный элемент 1, а обратные элементы существуют для 1 – это 1, и для 3 – это 3, но для элемента 2 обратного элемента не существует.

Общий вывод: для целых чисел простое поле GF(4) не существует.

2.18. Что называют примитивным элементом поля?

Что является примитивным элементом поля:

а) GF(2),

б) GF(3),

в) GF(5)?

Ответ: Примитивным элементом поля называют ненулевой элемент поля, последовательные степени которого дают все ненулевые элементы поля.

Обозначим примитивный элемент поля через α.

а) для GF(2) α=1;

б) для GF(3) α=2; остальные ненулевые элементы GF(3): $\alpha^2=1$; $\alpha^3=2$;

в) для GF(5) α=2; остальные ненулевые элементы GF(5): $\alpha^2=4$; $\alpha^3=3$; $\alpha^4=1$.

2.19**.** Что называют порядком поля? Группы?

Ответ: Порядком поля (группы) называют число элементов поля (группы).

2.20. Чему равен порядок поля:

а) GF(2)?

б) GF(3)?

в) GF(5)?

г) GF(p)?

Ответ**:** а) 2; б) 3; в) 5; г) p.

2.21. Построить поле GF(2^2).

Решение

Поле – кольцо классов вычетов многочленов по модулю неприводимого примитивного многочлена, т. е. такого неприводимого многочлена, корни которого являются примитивными элементами поля. Для поля GF(2^m) это должен быть неприводимый многочлен над полем GF(2) степени m, принадлежащий максимальному показателю, т. е. $e = 2^m - 1$.

В рассматриваемом случае $e = 3$, т. е. это должен быть неприводимый многочлен 2-й степени, входящий в разложение двучлена x^3+1 и не входящий в разложение двучлена меньшей степени. Этим свойством обладает единственный многочлен x^2+x+1, так как $x^3+1= (x+1)(x^2+x+1)$. Все корни x^3+1 являются ненулевыми элементами поля GF(2^2): α^0, α^1, α^2. При этом $\alpha^0=1$ есть корень $x+1$, а α и α^2 – корни x^2+x+1.

Для получения их в двоичном представлении необходимо разделить α^i, где i=1,2, на многочлен $\pi(\alpha)=1+\alpha+\alpha^2$, по модулю которого строится поле, и взять в качестве α^i остаток от деления α^i на $\pi(\alpha)$, тогда получим:

$$\alpha^0=1 \quad = 10,$$
$$\alpha^1= \quad \alpha = 01,$$
$$\alpha^2=1 + \alpha = 11.$$

Таким образом, последовательность степеней корня многочлена x^2+x+1 образует мультипликативную группу GF(2^2). Если к этим элементам добавить 0=00, то получим все элементы поля GF(2^2)=GF(4).

2.22. Доказать, что последовательность чисел 0=00, 1=10, α=01, α^2=11 образует поле GF(2^2).

Решение

Необходимо проверить наличие единичных элементов по операциям сложения и умножения и обратных элементов по этим операциям для всех элементов поля, так как ассоциативность, коммутативность и дистрибутивность выполняются при введении операций над элементами поля как над двоичными векторами.

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

×	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Таблица сложения проверяется сложением соответствующих векторов, а таблица умножения строится с учетом двух соотношений: $\pi(\alpha)=1+\alpha+\alpha^2=0$ и $\alpha^3=1$ (см. пояснения к решению задачи 2.17).

Из анализа таблиц вытекает, что в поле существует единичный элемент по сложению «0» и единичный элемент по умножению «1». Эти два элемента образуют простое поле GF(2), т. е. в состав расширенного поля в качестве подполя входит простое поле.

Для каждого элемента поля существует обратный элемент. По операции сложения обратными элементами являются те, на пересечении которых в таблице сложения располагаются «0», а по операции умножения обратными элементами являются ненулевые элементы, на пересечении которых в таблице умножения располагаются «1». Сравните с решением задачи 2.17.

2.23. Построить поле GF(2^3).

Решение

Для построения поля GF(2^3) необходимо знать примитивный многочлен 3-й степени. Таких многочленов известно два: x^3+x+1 и x^3+x^2+1.

Построим поле по модулю каждого из этих многочленов:

$\pi_1(\alpha)=\alpha^3+\alpha+1$	$\pi_2(\alpha)=\alpha^3+\alpha^2+1$
$\alpha^1= \quad \alpha \quad =010$	$\alpha^1= \quad \alpha \quad =010$
$\alpha^2= \quad \alpha^2=001$	$\alpha^2= \quad \alpha^2=001$
$\alpha^3=1+\alpha \quad =110$	$\alpha^3=1 \quad +\alpha^2=101$
$\alpha^4= \quad \alpha+\alpha^2=011$	$\alpha^4=1+\alpha+\alpha^2=111$
$\alpha^5=1+\alpha+\alpha^2=111$	$\alpha^5=1+\alpha \quad =110$
$\alpha^6=1 \quad +\alpha^2=101$	$\alpha^6= \quad \alpha+\alpha^2=011$
$\alpha^7=1 \quad =100$	$\alpha^7=1 \quad =100$

Получили два различных представления ненулевых элементов GF(2^3); дополним каждое из них нулевым элементом 0=(000). Получим два представления GF(2^3). Для первого из них первообразным корнем является корень $\pi_1(\alpha)$, а для второго − $\pi_2(\alpha)$.

2.24. Построить поле GF(2^4) на основе мультипликативной группы порядка 2^4-1. Проверить прямой подстановкой справедливость распределения элементов поля GF(2^4) в качестве корней по неприводимым многочленам, входящим в разложение $x^{15}+1$.

Решить самостоятельно (использовать материалы см. 2.1).

2.25. Построить поле GF(2^5) по модулю $\pi(\alpha)=1+\alpha^2+\alpha^5$.

Решить самостоятельно.

2.26. Найти наибольший общий делитель (НОД) чисел 186 и 66, т. е. НОД(186,66) =?

Решение

Воспользуемся алгоритмом Евклида и найдем:

1-й шаг:186−2·66=54,

2-й шаг: 66−1·54=12,

3-й шаг: 54−4·12=6,

4-й шаг: 12−2·6=0.

Итак, НОД(186,66)=6.

Представим полученный результат в виде: $fa+gb = d$, где a=186, b=66, d=6.

В этих целях преобразуем полученные выше равенства.

Значение для 54 из 1-го шага подставим в равенство 2-го шага: −186+3·66 =12.

Подставляя значения для 54 и 12 в равенство 3-го шага, получаем 5·186 −14·66 = 6, что соответствует искомому.

Сделаем еще одно преобразование: найденные значения для 6 и 12 подставим в равенство 4-го шага: −11·186+31·66=0.

Анализируя полученные равенства, приходим к выводу, что алгоритм Евклида пошагово находит значение f и g, т. е. процесс решения задачи нахождения НОД сводится к преобразованию выражения $f_ia+g_ib=d_i$ в $fa+gb=d$.

При этом значения f_i, g_i и d_i зависят от их значений на двух предыдущих шагах алгоритма. Найдем общие выражения для значений f_i, g_i, d_i.

Для этого перепишем последовательно найденные равенства, дополнив их двумя формальными равенствами в качестве исходных:

1·186+0·66=186,

0·186+1·66=66,

1·186−2·66=54,

−1·186+3·66=12,

5·186-14·66=6,

−11·186+31·66=0.

Определим $q_i=[d_{i-2}/d_{i-1}]$, где [ ] означает целую часть дроби d_{i-2}/d_{i-1}.

Теперь общее выражение для f_i, g_i и d_i может быть представлено в следующем виде: $E_i = E_{i-2} - q_iE_{i-1}$.

Для подтверждения этого представим процесс нахождения НОД(186,66) в виде таблицы.

Шаг i	f_i	g_i	d_i	q_i	$f_i \cdot a+g_i \cdot b=d_i$
−1	1	0	186	–	1·186 + 0·66 = 186
0	0	1	66	–	0·186 + 1·66 = 66
1	1	−2	54	[186/66]=2	1·186 − 2·66 = 54
2	−1	3	12	[66/54]=1	−1·186 + 3·66 = 12
3	5	−14	6	[54/12]=4	5·186 − 14·66 = 6
4	−11	31	0	[12/6]=2	−11·186 + 31·66 = 0

Выполненные преобразования используются при быстром декодировании кодов БЧХ для решения ключевого уравнения по алгоритму Евклида.

2.27. Вычислить 2^{19} (mod 5).

Число 2 является примитивным элементом поля GF(5) и 2^4=1. Число 2^{19} может быть представлено: $2^{19}=2^{4\cdot 4}\cdot 2^3$(mod 5)=$1^4\cdot 2^3$ (mod 5)=2^3(mod 5) =3.

Ответ: 2^{19}(mod 5) =3.

3. Теорема Ферма и циклотомические классы

Теорема Ферма.

Признаки делимости двучленов.

Корни неприводимых многочленов и циклотомические классы многочленов вида $x^n - 1$ для случаев:

а) $n = p^m-1$;

б) n – любое целое число.

Степени неприводимых многочленов в разложении x^n-1 на неприводимые сомножители.

Минимальные и двойственные многочлены.

Литература: см. 2.1–2.3.

Цель. Научиться вычислять число неприводимых сомножителей многочленов вида x^n-1, их степени и последовательности их корней. Получить навыки в формировании циклотомических классов, определении показателей, которым принадлежат неприводимые многочлены, представлении их корней в виде элементов расширенного поля Галуа.

Контрольные вопросы

3.1. Перечислить все многочлены степени n над полем GF(2), представить их в виде неприводимых сомножителей и определить показатели, к которым эти многочлены принадлежат в следующих случаях:

а) n=2, б) n=3, в) n=4, г) n=5.

3.2. Определить показатели, которым принадлежат следующие многочлены над полем GF(2):

а) $x^8+x^7+x^5+x^4+x^3+x+1$,

б) x^7+x^3+x+1,

в) $x^6+x^5+x^4+x^3+x^2+x+1$

и указать их неприводимые сомножители.

3.3. Определить число и степени неприводимых сомножителей многочленов над полем GF(2):

x^8+1, x^9+1, $x^{10}+1$, $x^{11}+1$, $x^{12}+1$, $x^{13}+1$, $x^{14}+1$, $x^{15}+1$, $x^{16}+1$, $x^{17}+1$, $x^{18}+1$, $x^{19}+1$, $x^{20}+1$, $x^{21}+1$, $x^{22}+1$, $x^{23}+1$.

3.4. Определить все неприводимые сомножители следующих двучленов:

а) $x^{30}+1$,

б) $x^{31}+1$,

в) $x^{32}+1$.

3.5. Используя результат решения задачи 2.13, а, прямым умножением показать, что многочлены из примера п. 2.1 равны: $f_1(x)=x^4+x+1=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$ и $f_2(x) = x^4+x^3+1= (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14})$.

3.6. Найти двойственные многочлены для следующих многочленов: x^2+x+1, x^3+x+1, x^5+x+1, x^6+x^3+1, x^9+x^4+1.

Примеры решения задач и дополнительные задачи

3.6. Доказать, что многочлен x^2+x+1 неприводим над полем GF(2).

Решение

Для доказательства достаточно показать, что данный многочлен не имеет сомножителей, содержащих x в первой степени, т. е. что x или $x+1$ не делят многочлен x^2+x+1 в двоичном поле.

Этот результат может быть получен тремя способами.

1. Непосредственным делением – предоставляется выполнить читателю.

2. Подстановкой корней x и $x+1$ в многочлен x^2+x+1.

Действительно: корень x равен 0, корень $x+1$ равен 1.

Проверяем: $f(x=0)=0^2+0+1=1$, т. е. 0 не является корнем x^2+x+1,

$f(x=1)=1^2+1+1=1$, т. е. 1 также не является корнем x^2+x+1.

3. Определением, к какому показателю принадлежит x^2+x+1, т. е. определением, какой порядок имеют его корни. Для этого представляем $x^2+x+1=0$, откуда $x^2=x+1$. Умножаем обе части равенства на x: $x^3=x^2+x$, но $x^2=x+1$, значит $x^3=x+1+x=1$. Следовательно, корни x^2+x+1 являются и корнями x^3+1, т. е. x^2+x+1 принадлежит показателю 3.

Этот результат не является неожиданным, так как многочлен вида $x^n+x^{n-1}+x^{n-2}+\ldots+x+1$, содержащий все степени x от n до 0 в качестве слагаемых, является сомножителем двучлена вида $x^{n+1}+1$ наряду с сомножителем $x+1$.

Кроме того, применение функции Эйлера позволяет определить число корней x^3+1, имеющих порядок 3: $\varphi(3)=2$. Значит, из трех корней x^3+1 два корня имеют порядок 3, а это корни именно многочлена x^2+x+1, так как порядок корня многочлена $x+1$ равен 1.

3.7. Найти корни многочлена x^2+x+1.

Решение

Решение предыдущей задачи показало, что x^2+x+1 входит в разложение x^3+1. По теореме Ферма корни x^3+1 являются элементами поля GF(2^2).

Найдем циклотомический класс по модулю 3: $C_{1(3)}=\{1,2\}$.

Следовательно, x^2+x+1 имеет корнями элементы α и α^2 поля GF(2^2).

Напомним состав поля GF(2) по модулю $\pi(\alpha)=1+\alpha+\alpha^2$:

$0=00$, $1=\alpha^0=10=\alpha^3$, $\alpha^1=01$, $\alpha^2=11$.

Таким образом, корнями $f(x)= x^2+x+1$ являются последовательности 01 и 11.

Действительно: $11+01+10 = 00$, т. е. $f(x=\alpha) = 0$ и $01+11+10=00$, т. е. $f(x=\alpha^2)=0$.

3.8. Построить многочлен $f(x)$ второй степени над полем GF(2), корнями которого являются элементы $\alpha^1=10$ и $\alpha^2=11$ поля GF(2^2).

Решение

В соответствии с теоремой Безу: $f(x) = (x+\alpha^1)(x+\alpha^2) = x^2+\alpha^2x+\alpha^1x+\alpha^3 = x^2+(\alpha^1+\alpha^2)x+\alpha^3=x^2+x+1$, так как $\alpha^1+\alpha^2= (01)+(11)=(10)=\alpha^0=1$, $\alpha^3=1$ (см. предыдущую задачу и таблицы задачи 2.22).

Тот же самый результат можно получить используя формулы Виета, в соответствии с которыми для нормированного многочлена 2-й степени $f(x) = f_2x^2+f_1x+f_0$ над полем GF(2) справедливо: $f_2=1$, $f_1= \alpha^1+\alpha^2=1$, $f_0= \alpha^1\alpha^2=1$.

Обратить внимание на то, что многочлен, неприводимый над полем GF(2), разлагается на сомножители над полем GF(2^2), т. е. над полем своих корней.

3.9. Найти все неприводимые многочлены степени 3 над полем GF(2).

Решение

Перечислим все многочлены степени 3 с коэффициентами из двоичного поля: x^3+x^2+x+1, x^3+x^2+x, x^3+x^2+1, x^3+x+1, x^3+1, x^3+x, x^3+x^2, x^3.

Второй и четыре последних многочлена явно не могут быть неприводимыми, так как имеют известные сомножители. Осталось проверить первый, третий и четвертый многочлены. Для проверки достаточно убедиться, что проверяемый многочлен не имеет в качестве сомножителя $x+1$, т. е. «1» не должна быть корнем проверяемого многочлена. Непосредственной подстановкой проверяем.

Для x^3+x^2+x+1: $1^3+1^2+1+1=0$, т. е. этот многочлен имеет сомножителем $x+1$, и, действительно, $x^3+x^2+x+1=(x+1)(x^2+1)=(x+1)^3$.

Для x^3+x^2+1: $1^3+1^2+1=1$.

Для x^3+x+1: $1^3+1+1=1$.

Многочлен третей степени может содержать в качестве сомножителей только многочлены 1-й или 2-й и 1-й степеней, поэтому делаем вывод, что многочлены x^3+x^2+1 и x^3+x+1 являются неприводимыми.

Ко всему они являются двойственными, поскольку $x^3(x^{-3}+x^{-1}+1)=$
$= 1+x^2+x^3$.

3.10. Определить, к какому показателю принадлежат многочлены x^3+x+1 и x^3+x^2+1.

Решение

По своей степени эти многочлены могут входить в разложение двучлена $x^{2^3-1}+1=x^7+1$. Достаточно проверить принадлежность к показателю 7 одного из них, например, x^3+x+1.

Полагаем $x^3=x+1$:

$x^4=x^2+x$

$x^5=x^3+x^2=x^2+x+1$

$x^6=x^3+x^2+x=x^2+1$

$x^7=x^3+x=x+1+x=1$.

Этим доказана принадлежность x^3+x+1 и x^3+x^2+1 к показателю 7. А это в свою очередь означает, что корни этих многочленов примитивные. Действительно, найдем функцию Эйлера от числа 7: $\varphi(7)=6$, т. е. среди ненулевых элементов поля GF(2^3) шесть элементов являются примитивными – это все ненулевые элементы, исключая $\alpha^0=1$, а именно: α^1, α^2, α^3, α^4, α^5, α^6. Они распределяются по двум циклотомическим классам: $C_{1(7)}=\{1,2,4\}$, $C_{3(7)}=\{3,6,5\}$.

При этом α^1, α^2 и α^4 – корни x^3+x+1, а α^3, α^5, α^6 – корни x^3+x^2+1. Проверить это можно прямой подстановкой.

3.11. Проверить применением теоремы Безу справедливость найденных в п. 2.1 неприводимых сомножителей $x^{15}+1$. Использовать результаты решения задач 2.13 и 2.24.

3.12. Определить, является ли многочлен x^5+x+1 неприводимым над полем GF(2).

Решение

Для решения этой задачи достаточно проверить имеет ли многочлен x^5+x+1 в качестве сомножителей неприводимые многочлены первой и второй степени, т. е. $x+1$ и x^2+x+1.

Многочлен $x+1$ имеет корнем «1». Подставим $x=1$ в x^5+x+1, получаем $x^5+x+1=1^5+1+1=1$, т. е. $x+1$ не делит x^5+x+1.

Для корней x^2+x+1 справедливо $x^2+x+1=0$ или $x^2=x+1$. Подставляем это значение в x^5+x+1: $x(x+1)(x+1)+x+1=x(x^2+1)+x+1=x^3+x+x+1=x^3+1=$
$= (x+1)(x^2+x+1)=0$, т. е. корни x^2+x+1 являются и корнями x^5+x+1.

Значит, x^5+x+1 имеет одним из своих сомножителей x^2+x+1. Выполняя деление x^5+x+1 на x^2+x+1, находим $x^5+x+1=(x^2+x+1)(x^3+x^2+1)$.

Ответ: Многочлен x^5+x+1 не является неприводимым над полем GF(2).

3.13. Проверить делимость многочлена x^5+x+1 на многочлен x^3+x^2+1. Решить самостоятельно методом проверки общих корней.

3.14. Найти все неприводимые многочлены пятой степени над полем GF(2).

Рекомендации по решению

1) выписать все двоичные приведенные многочлены 5-й степени с коэффициентом 1 при x^0;

2) определить методом проверки общих корней делимость рассматриваемых многочленов на многочлены $x+1$ и x^2+x+1 и выявить неприводимые;

3) правильность решения проверить по приложению.

3.15. Найти последовательности корней неприводимых двоичных многочленов 5-й степени из предыдущей задачи.

Рекомендации по решению

1) построить циклотомические классы по модулю $2^5–1=31$. Поскольку 31 – простое число, все ненулевые элементы поля GF(2^5), являющиеся искомыми корнями, имеют порядок 31, и их число равно 30, т. е. всего существует 6 неприводимых двоичных многочленов 5-й степени, а следовательно, и 6 циклотомических классов по модулю 31. Все эти многочлены являются примитивными;

2) по составу циклотомических классов найти пары двойственных многочленов;

3) используя результаты решения задач 2.25 и 3.14, установить соответствие между найденными неприводимыми многочленами и последовательностями их корней;

4) правильность решения проверить по приложению.

4. Разложение $x^n–1$ на неприводимые сомножители

Методика определения неприводимых сомножителей двучленов вида $x^n–1$.

Методика определения порядка корней сомножителей двучленов вида $x^n–1$.

Методика использования таблиц неприводимых многочленов для нахождения неприводимых сомножителей двучленов вида $x^n–1$ по их корням.

Решение задач по разложению двучленов $x^n–1$ на неприводимые сомножители с использованием таблиц неприводимых многочленов.

Литература: см. 2.4.

Цель. Привить студентам навыки нахождения неприводимых сомножителей двучленов вида x^n-1, определения значения и порядка корней многочленов.

Контрольные вопросы

4.1. Найти все неприводимые сомножители двучленов следующих степеней: 23, 51, 73, 85, 127.

4.2. Указать, какие из найденных в п. 4.1 многочленов являются примитивными (см. [1] и приложение).

4.3. Определить максимальную степень неприводимых в двоичном поле многочленов в разложении двучленов степеней 255 и 511. Каким показателям принадлежат эти многочлены?

4.4. Написать в общепринятом виде многочлены, заданные в двоично-восьмеричном представлении: 7, 13, 23, 45, 103, 211, 435, 1021, 2011, 4005.

4.5. Написать в двоично-восьмеричном представлении многочлены, найденные в п. 4.1.

Примеры решения задач и дополнительные задачи

4.6. Определить степени, число и вид неприводимых над GF(2) многочленов, входящих в разложение двучленов $x^{127}+1$ и $x^{255}+1$.

Решение

1. Многочлен $x^{127}+1 = x^{2^7-1}+1$. Поскольку 7 – простое число, в разложение на неприводимые сомножители $x^{127}+1$ над GF(2) входят только $x+1$ и неприводимые многочлены 7-й степени. Их число равно $\frac{\varphi(127)}{7}=\frac{126}{7}=18$.

Все эти 18 многочленов принадлежат показателю 127. Из приложения найдем вид девяти неприводимых двоичных многочленов степени 7 в двоично-восьмеричном представлении: 211, 217, 235, 367, 277, 325, 203, 313, 345. Дополнив эти многочлены двойственными им 221, 361, 271, 357, 375, 253, 301, 323, 247, завершаем решение первой части задачи.

2. Многочлен $x^{255}+1=x^{2^8-1}+1$. Поскольку 8 делится на числа 2 и 4, в разложение $x^{255}+1$ на неприводимые сомножители входят, кроме неприводимых многочленов 8-й степени, неприводимые многочлены 4-й и 2-й степеней. Определим число многочленов каждой из этих степеней, входящих в разложение $x^{255}+1$.

Для этого представим 255 в виде простых сомножителей: $255=3\cdot5\cdot17$. Это значит, что $x^{255}+1$ делят x^3+1, x^5+1, $x^{15}+1$, $x^{17}+1$, $x^{51}+1$ и $x^{85}+1$. Из этого делаем вывод, что в разложение $x^{255}+1$ входят некоторые неприводимые многочлены, не принадлежащие показателю 255:

$x+1$ – принадлежит показателю 1,

x^2+x+1 – принадлежит показателю 3,

$x^4+x^3+x^2+x+1$ – принадлежит показателю 5,

x^4+x+1, x^4+x^3+1 – принадлежат показателю 15,

два многочлена 8-й степени, принадлежащие показателю 17: $\frac{\varphi(17)}{8}=\frac{16}{8}=2$,

четыре многочлена 8-й степени, принадлежащие показателю 51: $\frac{\varphi(51)}{8}=\frac{32}{8}=4$,

восемь многочленов 8-й степени, принадлежащие показателю 85: $\frac{\varphi(85)}{8}=\frac{64}{8}=8$.

Кроме того, в разложение $x^{255}+1$ входят $\frac{\varphi(255)}{8}=\frac{128}{8}=16$ многочленов 8-й степени, принадлежащих показателю 255. Многочлены 8-й степени найдем из приложения. Для этого необходимо определить образующие соответствующих циклотомических классов.

Значения образующих:

- для многочленов, принадлежащих к показателю 17: $s=\frac{255}{17}=15$; этому числу соответствует многочлен 15 727 D: $x^8+x^7+x^6+x^4+x^2+x+1$. Это самодвойственный многочлен. Значит, должен быть еще один многочлен, принадлежащий показателю 17; таковым является многочлен 45 471 A: $x^8+x^5+x^4+x^3+1$ также самодвойственный;

- для многочленов, принадлежащих показателю 51, числа s равны 5 и 25. Это многочлены 5 763 D: $x^8+x^7+x^6+x^5+x^4+x+1$ и $x^8+x^7+x^4+x^3+x^2+x+1$ и 25 433 B: $x^8+x^4+x^3+x+1$ и $x^8+x^7+x^5+x^4+1$;

- для многочленов, принадлежащих к показателю 85, числа s=3, 9, 21 и 27.

Вид многочленов 8-й степени, принадлежащих к показателям 85 и 255, предлагается найти самостоятельно.

4.7. Найти неприводимые многочлены степени 9, принадлежащие показателю, меньшему 511.

Решение

Число 511 можно представить в виде 511=7×73. Из этого следует, что многочлены 9-й степени могут принадлежать помимо показателя 511 к показателю 73.

Число неприводимых многочленов 9-й степени, принадлежащих показателю 73: $\frac{\varphi(73)}{9}=\frac{72}{9}=8$.

Образующие циклотомических классов, соответствующих корням этих многочленов, составляют числа, кратные j = 7.

Из приложения находим, что им соответствуют следующие многочлены 9-й степени:

7 1231 A и двойственный многочлен 1145,
21 1027 A и двойственный многочлен 1641,
35 1401 C и двойственный многочлен 1003,
77 1511 C и двойственный многочлен 1113.

Записать эти многочлены в обычном виде предлагается самостоятельно.

5. Декодер Меггита

Структурная схема декодера Меггита.

Алгоритм исправления ошибки по методу Меггита.

Расчет комбинации, на которую настраивается дешифратор.

Расчет эффективности исправления ошибок в канале с группированием ошибок.

Оценка выигрыша от декорреляции ошибок.

Литература: [6].

Цель. Изучить принцип построения и алгоритм работы декодера Меггита для циклических кодов, исправляющих однократную ошибку. Привить студентам навыки вычисления значения синдрома ошибки, соответствующего моменту исправления ошибки.

Контрольные вопросы

5.1. Нарисовать схему декодера Меггита для исправления однократных ошибок укороченными циклическими кодами Хемминга:

а) (10,5) с $g(x) = 1+x^2+x^5$;
б) (11,5) с $g(x) = 1+x+x^6$;
в) (12,5) с $g(x) = 1+x+x^7$.

5.2. Для каждого кода из предыдущей задачи определить комбинацию, на которую должен быть настроен дешифратор, и показать по тактам работу синдромного регистра при выводе информационных разрядов принятой комбинации из буферного регистра, начиная с того момента, когда в нем сформировался синдром, до момента исправления ошибки. Считать, что ошибка произошла в символе кодовой комбинации, соответствующем коэффициенту при x^7.

Примеры решения задач и дополнительные задачи

5.3. Построить порождающую и проверочную матрицы укороченного циклического кода (10,5) с порождающим многочленом $g(x) = 1+ x^2+ x^5$.

Решение

Код (10,5) с порождающим многочленом $g(x)=1+x^2+x^5$ является укороченным кодом Хемминга, так как многочлен $1+x^2+x^5$ – примитивный многочлен, принадлежащий показателю 31.

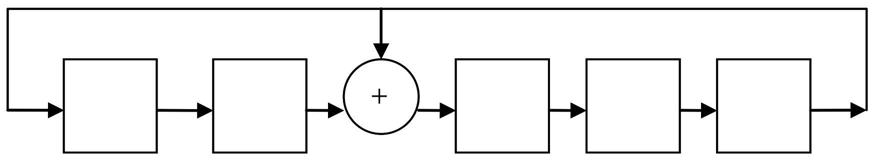
В таблице неприводимых многочленов он указан условной записью 1 45 Е.

Наиболее простое решение задачи состоит в построении генератора элементов поля GF(2^5) и нахождении десяти первых значений степеней примитивного корня. Их двоичное представление даст столбцы проверочной матрицы в канонической форме:

$H_{(10,5)}=[\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9]$, где α^i – элемент поля GF(2^5).

Затем по проверочной матрице и известным правилам найдем порождающую матрицу. Она также получится в канонической форме.

Генератор элементов поля GF(2^5), построенный на основе примитивного многочлена $1+x^2+x^5$, содержимое ячеек памяти на 10 тактах работы и матрицы, характеризующие код, представлены на рис. 1.



$$H^T_{(10,5)}=\begin{bmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&1&0&0\\ 0&1&0&1&0\\ 0&0&1&0&1\\ 1&0&1&1&0\\ 0&1&0&1&1 \end{bmatrix}$$

$$G_{(10,5)}=\begin{bmatrix} 1&0&1&0&0&1&0&0&0&0\\ 0&1&0&1&0&0&1&0&0&0\\ 0&0&1&0&1&0&0&1&0&0\\ 1&0&1&1&0&0&0&0&1&0\\ 0&1&0&1&1&0&0&0&0&1 \end{bmatrix}$$

Рис.1

5.4. Построить декодер Меггита для циклического кода (7,5) над полем GF(2^3) с порождающим многочленом $g(x)=x^2+\alpha^4x+\alpha^3$. Код гарантийно справляет однократные ошибки.

Значения элементов поля GF(2^3):

$0 = \quad 000$

$\alpha^0 = 1 \quad = 100$

$\alpha^1 = \quad \alpha \quad = 010$

$\alpha^2 = \quad \alpha^2 = 001$

$\alpha^3 = 1+\alpha \quad = 110$

$\alpha^4 = \quad \alpha+\alpha^2 = 011$

$\alpha^5 = 1+\alpha+\alpha^2 = 111$

$\alpha^6 = 1 \quad +\alpha^2 = 101$

$\alpha^7 = 1 \quad = 100$

Решить самостоятельно.

6. Быстрое декодирование кодов БЧХ

Коды Рида–Соломона. Определение, построение порождающего многочлена для кодов с требуемыми свойствами.

Ключевое уравнение. Алгоритм Форни.

Методы решения ключевого уравнения по алгоритмам Берлекемпа–Месси и Евклида.

Решение задач по исправлению ошибок на основе алгоритмов Берлекемпа–Месси и Евклида.

Литература: [7,8].

Цель. Изучить методы быстрого декодирования кодов БЧХ применительно к кодам Рида–Соломона, приобрести навыки использования методов быстрого декодирования для исправления ошибок в декодере и нахождения избыточных элементов в кодере.

Контрольные вопросы

6.1. Вычислить порождающий многочлен для кода Рида–Соломона (7,5).

6.2. Методом быстрого декодирования закодировать кодом Рида–Соломона (7,5) свой порядковый номер в журнале группы.

6.3. Для кода Рида–Соломона (7,5) построить кодер на основе регистра сдвига с обратными связями и закодировать комбинацию из предыдущей задачи. Сравнить результаты кодирования.

6.4. С помощью кодера предыдущей задачи построить порождающую и проверочную матрицы кода Рида–Соломона (7,5) в канонической форме.

6.5. Вычислить порождающий многочлен для кода Рида–Соломона (7,3).

Примеры решения задач и дополнительные задачи

6.6. Построить код Рида–Соломона (7,4) над полем $GF(2^3)$.

Решение

Находим порождающий многочлен по теореме Безу:

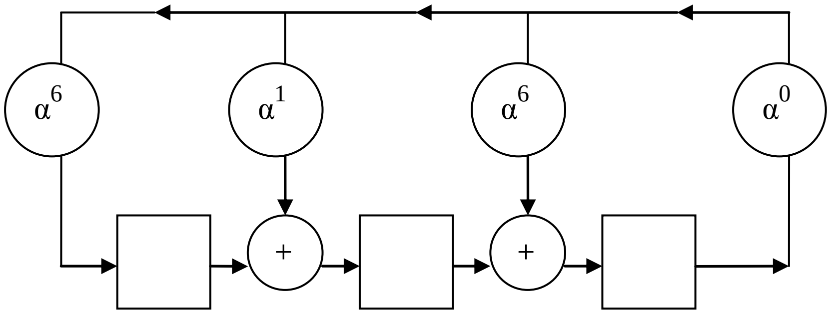
$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3) = (x^2+\alpha^2x+\alpha x+\alpha^3)(x+\alpha^3) =$$
$$=x^3+\alpha^2x^2+\alpha x^2+\alpha^3x+\alpha^3x^2+\alpha^5x+ \alpha^4x +\alpha^6 =$$
$$= x^3+(\alpha+\alpha^2+\alpha^3)x+(\alpha^3+\alpha^4+\alpha^5)x +\alpha^6 =x^3+\alpha^6x^2+\alpha x+\alpha^6$$

и по формуле Виета:

$$g_3=1,\ g_2= \alpha+\alpha^2+\alpha^3= \alpha^6,\ g_1 = \alpha\alpha^2 + \alpha\alpha^3+\alpha^2\alpha^3=\alpha^3+\alpha^4+\alpha^5=\alpha,\ g_0=\alpha\alpha^2\alpha^3=\alpha^6.$$

Итак, $g(x) = x^3+\alpha^6x^2+\alpha x+\alpha^6$.

Для построения порождающей и проверочной матриц воспользуемся приемом, примененным в п. 5.3. Строим генератор элементов GF(2^3) по виду $g(x)$ (рис. 2). Записав в крайнюю слева ячейку памяти «1», выполним 7 сдвигов до получения в ячейках регистра исходной последовательности 1 0 0. Содержимое ячеек памяти регистра на первых 7 тактах работы схемы соответствует строкам транспонированной проверочной матрицы кода. Последние четыре строки данной матрицы соответствуют столбцам порождающей матрицы этого кода, расположенных на местах избыточных элементов в канонической форме. Приписав к ним справа единичную матрицу размером 4×4, получаем всю порождающую матрицу кода (7,4) в канонической форме.



$$H^{T}_{(7,4)}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha^6 & \alpha^1 & \alpha^6 \\ \alpha^5 & \alpha^2 & \alpha^6 \\ \alpha^5 & \alpha^4 & \alpha^3 \\ \alpha^2 & \alpha^0 & \alpha^1 \end{bmatrix}$$

$$G_{(7,4)}=\begin{bmatrix} \alpha^6 & \alpha^1 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^5 & \alpha^2 & \alpha^6 & 0 & 1 & 0 & 0 \\ \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha^2 & \alpha^0 & \alpha^1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

1 0 0

Рис. 2

ПРИЛОЖЕНИЕ

(фрагмент табл.В.2. из[1])

Таблица В.2. Неприводимые многочлены степени, не превосходящей 34, над полем GF (2)

Степень 2	1 7H				
Степень 3	1 13F				
Степень 4	1 23F	3 37D	5 07		
Степень 5	1 45E	3 75G	5 67H		
Степень 6	1 103F	3 127B	5 147H	7 111A	9 015
11 155E	21 007				
Степень 7	1 211E	3 217E	5 235E	7 367H	9 277E
11 325G	13 203F	19 313H	21 345G		
Степень 8	1 435E	3 567B	5 763D	7 551E	9 675C
11 747H	13 453F	15 727D	17 023	19 545E	21 613D
23 543F	25 433B	27 477B	37 537F	43 703H	45 471A
51 037	85 007				
Степень 9	1 1021E	3 1131E	5 1461G	7 1231A	9 1423G
11 1055E	13 1167F	15 1541E	17 1333F	19 1605G	21 1027A
23 1751E	25 1743H	27 1617H	29 1553H	35 1401C	37 1157F
39 1715E	41 1563H	43 1713H	45 1175E	51 1725G	53 1225E
55 1275E	73 0013	75 1773G	77 1511C	83 1425G	85 1267E
Степень 10	1 2011E	3 2017B	5 2415E	7 3771G	9 2257B
11 2065A	13 2157F	15 2653B	17 3515G	19 2773F	21 3753D
23 2033F	25 2443F	27 3573D	29 2461E	31 3043D	33 0075C
35 3023H	37 3543F	39 2107B	41 2745E	43 2431E	45 3061C
47 3177H	49 3525G	51 2547B	53 2617F	55 3453D	57 3121C
59 3471G	69 2701A	71 3323H	73 3507H	75 2437B	77 2413B
83 3623H	85 2707E	87 2311A	89 2327F	91 3265G	93 3777D
99 0067	101 2055E	103 3575G	105 3607C	107 3171G	109 2047F
147 2355A	149 3025G	155 2251A	165 0051	171 3315C	173 3337H
179 3211G	341 0007				
Степень 11	1 4005E	3 4445E	5 4215E	7 4055E	9 6015G
11 7413H	13 4143F	15 4563F	17 4053F	19 5023F	21 5623F
23 4757B	25 4577F	27 6233H	29 6673H	31 7237H	33 7335G
35 4505E	37 5337F	39 5263F	41 5361E	43 5171E	45 6637H
47 7173H	49 5711E	51 5221E	53 6307H	55 6211G	57 5747F
59 4533F	61 4341E	67 6711G	69 6777D	71 7715G	73 6343H
75 6227H	77 6263H	79 5235E	81 7431G	83 6455G	85 5247F
87 5265E	89 5343B	91 4767F	93 5607F	99 4603F	101 6561G
103 7107H	105 7041G	107 4251E	109 5675E	111 4173F	113 4707F
115 7311C	117 5463F	119 5755E	137 6675G	139 7655G	141 5531E
147 7243H	149 7621G	151 7161G	153 4731E	155 4451E	157 6557H
163 7745G	165 7317H	167 5205E	169 4565E	171 6765G	173 7535G
179 4653F	181 5411E	183 5545E	185 7565G	199 6543H	201 5613F
203 6013H	205 7647H	211 6507H	213 6037H	215 7363H	217 7201G
219 7273H	293 7723H	299 4303B	301 5007F	307 7555G	309 4261E
331 6447H	333 5141E	339 7461G	341 5253F		
Степень 12	1 10123F	3 12133B	5 10115A	7 12153B	9 11765A
11 15647E	13 12513B	15 13077B	17 16533H	19 16047H	21 10065A
23 11015E	25 13377B	27 14405A	29 14127H	31 17673H	33 13311A
35 10377B	37 13565E	39 13321A	41 15341G	43 15053H	45 15173C
47 15621E	49 17703C	51 10355A	53 15321G	55 10201A	57 12331A
59 11417E	61 13505E	63 10761A	65 00141	67 13275E	69 16663C
71 11471E	73 16237E	75 16267D	77 15115C	79 12515E	81 17545C
83 12255E	85 11673B	87 17361A	89 11271E	91 10011A	93 14755C
95 17705A	97 17121G	99 17323D	101 14227H	103 12117E	105 13617A
107 14135G	109 14711G	111 15415C	113 13131E	115 13223A	117 16475C
119 14315C	121 16521E	123 13475A	133 11433B	135 10571A	137 15437G
139 12067F	141 13571A	143 12111A	145 16535C	147 17657D	149 12147F
151 14717F	153 13517B	155 14241C	157 14675G	163 10663F	165 10621A

Таблица В.2. Неприводимые многочлены степени, не превосходящей 34, над полем GF (2)

Продолжение

Степень 12

167 16115G	169 16547C	171 10213B	173 12247E	175 16757D	177 16017C
179 17675E	181 10151E	183 14111A	185 14037A	187 14613H	189 13535A
195 00165	197 11441E	199 10321E	201 14067D	203 13157B	205 14513D
207 10603A	209 11067F	211 14433F	213 16457D	215 10653B	217 13563B
219 11657B	221 17513C	227 12753F	229 13431E	231 10167B	233 11313F
235 11411A	237 13737B	239 13425E	273 00023	275 14601C	277 16021G
279 16137D	281 17025G	283 15723F	285 17141A	291 15775A	293 11477F
295 11463B	297 17073C	299 16401C	301 12315A	307 14221E	309 11763B
311 12705E	313 14357F	315 17777D	325 00163	327 17233D	329 11637B
331 16407F	333 11703A	339 16003C	341 11561E	343 12673B	345 14537D
347 17711G	349 13701E	355 10467B	357 15347C	359 11075E	361 16363F
363 11045A	365 11265A	371 14043D	397 12727F	403 14373D	405 13003B
407 17057G	409 10437F	411 10077B	421 14271G	423 14313D	425 14155C
427 10245A	429 11073B	435 10743B	437 12623F	439 12007F	441 15353D
455 00111	585 00013	587 14545G	589 16311G	595 13413A	597 12265A
603 14411C	613 15413H	619 17147F	661 10605E	683 10737F	685 16355C
691 15701G	693 12345A	715 00133	717 16571C	819 00037	1365 00007

Степень 13

	1 20033F	3 23261E	5 24623F	7 23517F	9 30741G
11 21643F	13 30171G	15 21277F	17 27777F	19 35051G	21 34723H
23 34047H	25 32535G	27 31425G	29 37505G	31 36515G	33 26077F
35 35673H	37 20635E	39 33763H	41 25745E	43 36575G	45 26653F
47 21133F	49 22441E	51 30417H	53 32517H	55 37335G	57 25327F
59 23231E	61 25511E	63 26533F	65 33343H	67 33727H	69 27271E
71 25017F	73 26041E	75 21103F	77 27263F	79 24513F	81 32311G
83 31743H	85 24037F	87 30711G	89 32641G	91 24657F	93 32437H
95 20213F	97 25633F	99 31303H	101 22525E	103 34627H	105 25775E
107 21607F	109 25363F	111 27217F	113 33741G	115 37611G	117 23077F
119 21263F	121 31011G	123 27051E	125 35477H	131 34151G	133 27405E
135 34641G	137 32445G	139 36375G	141 22675E	143 36073H	145 35121G
147 36501G	149 33057H	151 36403H	153 35567H	155 23167F	157 36217H
159 22233F	161 32333H	163 24703F	165 33163H	167 32757H	169 23761E
171 24031E	173 30025G	175 37145G	177 31327H	179 27221E	181 25577F
183 22203F	185 37437H	187 27537F	189 31035G	195 24763F	197 20245E
199 20503F	201 20761E	203 25555E	205 30357H	207 33037H	209 34401G
211 32715G	213 21447F	215 27421E	217 20363F	219 33501G	221 20425E
223 32347H	225 20677F	227 22307F	229 33441G	231 33643H	233 24165E
235 27427F	237 24601E	239 36721G	241 34363H	243 21673F	245 32167H
247 21661E	265 33357H	267 26341E	269 31653H	271 37511G	273 23003F
275 22657F	277 25035E	279 23267F	281 34005G	283 34555G	285 24205E
291 26611E	293 32671G	295 25245E	297 31407H	299 33471G	301 22613F
303 35645G	305 32371G	307 34517H	309 26225E	311 35561G	313 25663F
315 24043F	317 30643H	323 20157F	325 37151G	327 24667F	329 33325G
331 32467H	333 30667H	335 22631E	337 26617F	339 20275E	341 36625G
343 20341E	345 37527H	347 31333H	349 31071G	355 23353F	357 26243F
359 21453F	361 36015G	363 36667H	365 34767H	367 34341G	369 34547H
371 35465G	373 24421E	375 23563F	377 36037H	391 31267H	393 27133F
395 30705G	397 30465G	399 35315G	401 32231G	403 32207H	405 26101E
407 22567F	409 21755E	411 22455E	413 33705G	419 37621G	421 21405E
423 30117H	425 23021E	427 21525E	429 36465G	431 33013H	433 27531E
435 24675E	437 33133H	439 34261G	441 33405G	443 34655G	453 32173H
455 33455G	457 35165G	459 22705E	461 37123H	463 27111E	465 35455G
467 31457H	469 23055E	471 30777H	473 37653H	475 24325E	477 31251G
547 35163H	549 33433H	551 37243H	553 27515E	555 32137H	557 26743F
563 30277H	565 20627F	567 35057H	569 24315E	571 24727F	581 30331G
583 34273H	585 23207F	587 31113H	589 36023H	595 27373F	597 20737F
599 36235G	601 21575E	603 26215E	605 21211E	611 20311E	613 34003H
615 34027H	617 20065E	619 22051E	621 22127F	627 23621E	629 24465E
651 26457F	653 31201G	659 34035G	661 27227F	663 22561E	665 21615E
667 22013F	669 23365E	675 26213F	677 26775E	679 32635G	681 33631G
683 32743H	685 31767H	691 34413H	693 22037F	695 30651G	697 26565E
711 22141E	713 22471E	715 35271G	717 37445G	723 22717F	725 26505E
727 24411E	729 24575E	731 23707F	733 25173F	739 21367F	741 25161E
743 24147F	793 36307H	795 24417F	805 20237F	807 36771G	809 37327H
811 27735E	813 31223H	819 36373H	821 33121G	823 32751G	825 33523H

ЛИТЕРАТУРА

1. *Питерсон, У.* Коды, исправляющие ошибки / У. Питерсон / Пер. с англ. – М. : Мир, 1964. – 338 с.

2. *Мак-Вильямс, Ф.Дж.* Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн / Пер. с англ. – М. : Связь, 1979. – 744с.

3. *Виноградов, И.М.* Основы теории чисел / И.М. Виноградов. – М. : Наука, 1965. – 172 с.

4. *Кассами, Т.* Теория кодирования / Т. Кассами, Н. Токура, Е. Ивадари, Я. Инагака / Пер. с яп. – М. : Мир, 1978. – 576 с.

5. *Крук, Е.А.* Лекции по теории кодирования / Е.А. Крук, А.А. Овчинников. – СПб. : ГУАП, 2004. – 64с.

6. *Когновицкий, О.С.* Построение циклического (n, k)-кода / О.С. Когновицкий, А.Н. Глухов, М.С. Новодворский, Л.В. Федотова – СПб. : СПбГУТ, 2006. – 34 с.

7. *Охорзин, В.М.* Построение каскадных кодов на основе кодов Рида–Соломона и Боуза–Чоудхури–Хоквингема / В.М. Охорзин, Д.С. Кукунин, М.С. Новодворский – СПб. : СПбГУТ им. проф. М.А. Бонч-Бруевича, 2004. – 60 с.

8. *Кларк, Дж.К.* Кодирование с исправлением ошибок в системах цифровой связи / Дж.К. мл. Кларк, Дж.Б. Кейн. – М. : Радио и связь, 1987. – 392 с.

СОДЕРЖАНИЕ