

Конспект лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

группы 320–325, 327, 328 (III поток)
осенний семестр 2018/19 уч. года

Лектор *С. И. Гуров*

ассистент *Д. А. Кропотов*

(кафедра *Математических методов
прогнозирования*)

2018

Читать и не понимать — то же, что совсем не читать.

Ян Амос Коменский.

Добавим: ... и не запоминать ...

Предисловие

Данный конспект лекций был подготовлен для студентов III-го («программистского») потока студентов-бакалавров факультета ВМК МГУ изучающих в 5-м семестре указанную дисциплину. В ней рассматриваются приложения конечных алгебраических структур к задаче кодирования данных в целях коррекции ошибок и обеспечения конфиденциальности при передаче информации.

Заметим, что стиль изложения в учебнике и конспекте лекций различен. Последний более свободный, «разговорный», и содержит, в основном, лишь формулировки определений и теорем (возможно, с доказательствами). В учебнике же данный материал обычно предваряется и завершается пояснениями, указываются его связи с другими понятиями и др. С другой стороны, автор счёл необходимым оставить в данном конспекте некоторый материал, обычно неиспользуемый непосредственно на лекциях, но полезный при самостоятельной проработке материала.

В связи со спецификой преподавания курса, в текст конспекта включено достаточное количество примеров и задач с решениями.

Глава 3 написана совместно с Д. А. Кропотовым.

Оглавление

1	Группы, кольца, поля (компендиум)	5
1.1	Группы	5
1.2	Кольца и поля	14
1.3	Задачи	22
2	Конечные кольца и поля	26
2.1	Поля Галуа	26
2.2	Вычисления в конечных кольцах и полях	36
2.3	Алгебра векторов над конечным полем	43
2.4	Корни многочленов над конечным полем	47
2.5	Циклические подпространства колец вычетов	59
2.6	Задачи	64
3	Коды, исправляющие ошибки	70
3.1	Блочное кодирование: основные понятия	70
3.2	Линейные коды	78
3.3	Синдромное декодирование линейных кодов	87
3.4	Циклические коды	90
3.5	Коды БЧХ	96
3.6	Декодирование кодов БЧХ	103
3.7	Задачи	113
4	Алгебраические основы криптографии	116
4.1	Основные понятия	116
4.2	Система шифрования RSA	127
4.3	Простота и факторизация натуральных чисел	128

4.4	Задача дискретного логарифмирования	136
4.5	Задачи	145
	Решения задач	146
	Список литературы	187

Глава 1

Группы, кольца, поля (компендиум)

1.1 Группы

Определение 1.1. *Группой* называется тройка $\langle G, \circ, e \rangle$, где G — непустое множество (*носитель*), $e \in G$ — *нейтральный элемент группы*, а \circ — такая бинарная операция на носителе, что для любых его элементов x, y, z выполняются следующие *законы* или *аксиомы группы*:

- [0) $x \circ y \in G$ — *устойчивость* носителя;]
- 1) $(x \circ y) \circ z = x \circ (y \circ z)$ — *ассоциативность*;
 - 2) $e \circ x = x \circ e = x$ — *свойство нейтрального элемента*;
 - 3) $\forall x \exists ! y : y \circ x = x \circ y = e$ — *существование обратного элемента к x* .

При отсутствии неясностей, группы обозначают $\langle G, \circ \rangle$ или просто символом носителя G .

Вместо \circ часто пишут \cdot или просто этот символ опускают (*мультипликативная запись групповой операции*) и нейтральный элемент называют единицей 1, а обратный к x — x^{-1} .

Степень элемента при мультипликативной записи:

$$a^0 = e, \quad a^n = \underbrace{a \cdot \dots \cdot a}_n, \quad n \in \mathbb{N},$$

n символов a

при которой справедливы обычные свойства степени:

$$a^{m+n} = a^m \cdot a^n, \quad (a^m)^n = a^{mn}, \quad a^{-n} = (a^{-1})^n = (a^n)^{-1}.$$

Если $|G| = n$, то G — конечная группа и n — её порядок. В конечной группе небольшого порядка операцию \circ удобно задавать *таблицей умножения* (таблицей Кэли).

Пример 1.1 (Таблица умножения группы Клейна V_4).

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

— четверная группа Клейна
 $V_4 = \{e, a, b, c\}$

Группы со свойством $x \circ y = y \circ x$ называются *коммутативными* или *абелевыми*. Для них используют *аддитивную запись* $x + y$ групповой операции, нейтральный элемент называют *нулем* (0), а обратный к элементу x — *противоположным* ($-x$).

Пример 1.2. 1. Четверная группа Клейна абелева.

2. Числовые группы — все они абелевы:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ — группы относительно сложения.
- Ненулевые элементы множеств $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — группы относительно умножения.

3. *Бинарные наборы* $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n) \in B^n$ (единичный куб) относительно покомпонентной суммы по mod 2: $\tilde{\alpha} \oplus \tilde{\beta} = (\alpha_1 \oplus \beta_1, \dots, \alpha_n \oplus \beta_n)$ — абелева группа, её нуль — $\tilde{0} = (0, \dots, 0)$.

3. *Симметрическая группа* S_n : все перестановки n -элементного множества $X = \{1, \dots, n\}$ относительно их композиции $*$. Нейтральный элемент симметрической группы — единичная перестановка 1_X . Ясно, что $|S_n| = n!$ и S_n не абелева при $n \geq 3$.

Перестановки можно записывать в виде:

а) таблицы —

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ t_1 & t_2 & \dots & t_i & \dots & t_n \end{pmatrix},$$

б) разложения на циклы —

$$\pi = (t_1^1 t_2^1 t_3^1 \dots t_{k_1}^1) (t_1^2 t_2^2 t_3^2 \dots t_{k_2}^2) \dots (t_1^m t_2^m t_3^m \dots t_{k_m}^m).$$

Внутри каждой пары скобок числа переставляются циклически: $\pi(t_1) = t_2$, $\pi(t_2) = t_3$, \dots , $\pi(t_k) = t_1$ и перестановка π содержит m циклов.

Циклы длины 1, то есть вида (t) , обычно опускают:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix} \leftrightarrow (154)(26)$$

Каноническое представление цикла $(t_1 t_2 \dots t_k)$: t_1 — наименьшее из чисел $\{t_1, t_2, \dots, t_k\}$.

Например, для композиции перестановок:

$$(123) * (23) = (12) \neq (13) = (23) * (123).$$

4. Группы симметрии (самосовмещений) объекта — совокупность преобразований, совмещающих объект с самим собой.

4.1. Группы симметрии правильного n -угольника — группы диэдра D_n

а) У группы D_{2k+1} , $k \in \mathbb{N}$ — две образующих:
 (1) вращение вокруг центра на $\frac{360^\circ}{2k+1}$ в выбранном направлении,
 (2) симметрия относительно оси, проходящей через данную вершину и центр многоугольника.

Например: группа симметрии правильного треугольника — перестановка его вершин A , B и C

$$D_3 = \langle t, r \rangle = \{ e, (ABC), (ACB), (A)(BC), (B)(AC), (C)(AB) \} = S_3.$$

t — вращение на 120° вокруг центра в выбранном направлении (по или против часовой стрелки),
 r — осевая симметрия относительно выбранной оси.

б) У группы D_{2k} , $k \in \mathbb{N}$ — три образующих:
 (1) вращение вокруг центра (в выбранном направлении) на $\frac{360^\circ}{2k}$ и две осевых симметрий — относительно фиксированных осей, проходящих через середины противоположных (2) сторон и (3) вершин.

Пример: группа симметрии квадрата с вершинами A , B , C и C .

$$D_4 = \langle t, r, f \rangle.$$

t — вращение на 90° вокруг центра в выбранном направлении,

r — симметрия относительно некоторой оси, проходящей через центры противоположных сторон,
 f — симметрия относительно некоторой оси, проходящей через противоположные вершины.

Легко видеть, что $|D_n| = 2n$.

4.2. Группы *вращений* правильных многогранников — это не все симметрии многогранника, а только повороты, т. е. зеркальные отражения исключены.

Пять *платоновых тел* и соответствующие группы их вращений: T — группа *вращения тетраэдра*, $|T| = 12$; O — группа *октаэдра*, вращения октаэдра и куба, $|O| = 24$; Y группа *икосаэдра*, вращения икосаэдра и додекаэдра, $|Y| = 60$.

Подгруппы и смежные классы. Если $\langle G, \circ, e \rangle$ — группа, а H — подмножество G , само являющееся группой относительно \circ , то $\langle H, \circ, e \rangle$ — *подгруппа* G , символически $H \leq G$.

Единичная $E = \{e\}$ и вся группа — *тривиальные* подгруппы любой группы. Ясно, что нейтральный элемент e входит в любую группу.

Определение левого xH и правого Hx *смежных классов* по подгруппе H (с представителем x) соответственно:

$$\begin{aligned} H \leq G, x \in G &\Rightarrow xH = \{xh \mid h \in H\}, \\ Hx &= \{hx \mid h \in H\}. \end{aligned}$$

Утверждение 1.1 (о смежных классах). *Левые смежные классы с разными представителями либо не пе-*

ресекаются, либо совпадают и вместе составляют всю группу.

То же справедливо и для правых смежных классов.

Если $\forall x \in G : xH = Hx$, то подгруппа H — нормальная. Нормальность — ослабленное условие коммутативности: в абелевой группе все подгруппы нормальны.

Определение 1.2. Множество смежных классов группы $\langle G, \circ \rangle$ по её нормальной подгруппе H снабжённое операцией \bullet :

$$(aN) \bullet (bN) = (a \circ b)N.$$

называется *факторгруппой*, символически G/H .

Легко видеть, что результат $x \circ y$ находится в aN независимо от выбора элементов $x \in aN$ и $y \in bN$.

Определение 1.3. Для групп $\langle G, \circ, e \rangle$ и $\langle G', \cdot, e' \rangle$ отображение $\varphi : G \rightarrow G'$ называется *изоморфизмом*, если оно

- 1) взаимно-однозначно (биективно);
- 2) сохраняет групповую операцию: для любых $a, b \in G$ справедливо $\varphi(a \circ b) = \varphi(a) \cdot \varphi(b)$,

а такие группы — *изоморфными*, символически $G \cong G'$.

Из определения следует, что для изоморфизма φ имеет место $\varphi(a^{-1}) = \varphi(a)^{-1}$ и $\varphi(e) = e'$.

Иногда, когда это не приводит к недоразумениям, вместо $G \cong G'$ пишут просто $G = G'$.

Теорема 1.1 (Кэли). Любая группа порядка n изоморфна некоторой подгруппе симметрической группы S_n .

Если в определении изоморфизма снять требование биективности φ , то получим определение *гомоморфизма групп*. Например, всегда существует гомоморфизм произвольной группы в единичную E .

Циклические группы. Если в коммутативной группе $\langle C, \cdot, 1 \rangle$ каждый элемент есть степень некоторого элемента c , то такая группа называется *циклической*, а элемент c — *порождающим (образующим, генератором)*. То есть C — циклическая группа, если

$$\exists c \underset{C}{\forall} a \exists k \underset{\mathbb{Z}}{=} : c^k = a, \quad \text{символически } \langle c \rangle = C.$$

Ясно, что циклическая группа абелева и любая её подгруппа — циклическая и абелева.

Пример циклической группы: группа $\langle \frac{2\pi}{n} \rangle$ поворотов n -угольника вокруг центра на указанный угол с совпадением исходного и полученного положения.

Для циклических групп возможны два случая.

1. *Все степени порождающего элемента различны* — тогда группа бесконечна и состоит из элементов

$$\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots,$$

то есть она изоморфна группе $\langle \mathbb{Z}, +, 0 \rangle$ целых чисел по сложению. Ясно, что это единственная с точностью до изоморфизма бесконечная циклическая группа.

Сколько в ней генераторов? Два: -1 и $+1$.

2. Две различные степени порождающего элемента совпадают: $a^{k+n} = a^k a^n = a^k \Rightarrow a^n = e$.

Определение 1.4. Порядком элемента a циклической группы C , символически $\text{ord } a$, называют число

$$\text{ord } a = \arg \min_{m \in \mathbb{N}} \{ a^m = e \}.$$

В рассматриваемом случае получаем конечную группу

$$\mathbb{Z}_n = \langle \{0, 1, \dots, n-1\}, +_{\text{mod } n}, 0 \rangle, \quad n = \text{ord } a$$

(подробнее см. далее).

Любая циклическая группа является гомоморфным образом группы \mathbb{Z} .

Рассмотрим группу $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Её нетривиальные подгруппы суть

$$\{0, 2, 4\} \cong \mathbb{Z}_3 \quad \text{и} \quad \{0, 3\} \cong \mathbb{Z}_2,$$

а порождающие элементы — 1 и 5, взаимно простые с 6, не входящие ни в одну из них.

Определение 1.5. Значение функции Эйлера $\varphi(n)$ — количество чисел из интервала $[1, \dots, n-1]$, взаимно простых с n и, по определению $\varphi(1) = 1$.

$$\text{Например, } \varphi(6) = |\{1, 5\}| = 2.$$

Свойства функции Эйлера (p — простое):

- $\varphi(p) = p - 1$;
- $\varphi(n^k) = n^{k-1} \varphi(n)$, откуда $\varphi(p^k) = p^{k-1}(p - 1)$,

- если m и n взаимно просты, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
- $\sum_{d|n} \varphi(d) = n$.

Иллюстрация свойств:

$$\varphi(12) = \varphi(2^2 \cdot 3) = 2^1 \cdot 1 \cdot 2 = 4,$$

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8,$$

$$\varphi(16) = \varphi(2^4) = 2^3 \cdot 1 = 8,$$

$$n = 12, D(12) = \{1, 2, 3, 4, 6, 12\},$$

$$\underbrace{\varphi(1)}_{=1} + \underbrace{\varphi(2)}_{=1} + \underbrace{\varphi(3)}_{=2} + \underbrace{\varphi(4)}_{=2} + \underbrace{\varphi(6)}_{=2} + \underbrace{\varphi(12)}_{=4} = 12.$$

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Рис. 1.1. Первые 99 значений функции Эйлера

Ясно, что циклическая группа порядка n имеет ровно $\varphi(n)$ порождающих элементов: элемент $a \in \mathbb{Z}_n$ обратим, если и только если он взаимно прост с n .

Теорема Лагранжа и следствия из неё

Теорема 1.2 (Лагранж). Порядок подгруппы конечной группы делит порядок самой группы:

$$|G| = |H| \cdot [G : H].$$

Число $[G : H]$ называется *индексом подгруппы H по группе G* .

Следствие. Порядок любого элемента конечной группы делит порядок группы.

Например, для \mathbb{Z}_6 : $\text{ord } 0 = 1$, $\text{ord } 1 = \text{ord } 5 = 6$, $\text{ord } 2 = \text{ord } 4 = 3$, $\text{ord } 3 = 2$ и порядки всех элементов делят 6.

1.2 Кольца и поля

Кольца: определение, основные свойства

Определение 1.6. Абелева группа $\langle R, +, 0 \rangle$ называется *кольцом*, символически $\langle R, +, \cdot, 0 \rangle$, если на ней определена бинарная операция *умножения* \cdot , связанная со сложением $+$ *дистрибутивными законами*

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{и} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

- Обычно рассматривают *ассоциативные кольца* с ассоциативной операцией умножения.
- Важный случай — *коммутативные кольца* с коммутативной операцией умножения.

- Если в кольце имеется единичный элемент 1 по умножению ($x \cdot 1 = 1 \cdot x = x$), то кольцо называется *кольцом с единицей* или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$.
- *Тривиальное кольцо* — $\{0\}$, в нём и только в нём $0 = 1$.
- Кольцо R — *без делителей нуля*, если для любых $a, b \in R$ из $a \cdot b = 0$ следует $a = 0$ или $b = 0$.

Определение 1.7. *Целостным кольцом* называют нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля.

- Пример 1.3.*
1. Классический пример кольца — кольцо целых чисел \mathbb{Z} с обычными операциями сложения и умножения. Это кольцо целостно и имеет два обратимых элемента: $+1$ и -1 .
 2. Кольцо чётных $2\mathbb{Z}$ — кольцо без единицы.
 3. \mathbb{Z}_n — *кольцо классов вычетов*¹⁾ по модулю n , результаты операций $(+)$ и (\cdot) по $\text{mod } n$.

Целые числа a и b *сравнимы по модулю натурального n* , символически $a = b \pmod{n}$ или $a \equiv_n b$, если при делении на n они имеют одинаковые остатки, или, что то же, $a - b$ делится на n .

Класс вычетов числа a по модулю n — множество всех целых чисел, сравнимых с a по модулю

¹⁾ вычет (лат. residum) — остаток

n , символически $[a]$ или \bar{a} (число n считается заданным):

$$[a] = \{b \in \mathbb{Z} : a \equiv_n b\} = \{a, a \pm n, a \pm 2n, \dots\}.$$

Если нет опасности разночтений, вместо $[a]$ или \bar{a} пишут просто a .

Сложение и умножение классов вычетов определяется формулами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [a \cdot b].$$

Кольцо \mathbb{Z}_n содержит ровно n элементов:

$$[0], [1], \dots, [n-1] \text{ или просто } \{0, 1, \dots, n-1\}.$$

Это кольцо нецелостно при составном n : например в \mathbb{Z}_6 получим $3 \cdot 2 = 0$.

Элемент a *унитального* кольца называется *обратимым*, если существует элемент b такой, что

$$a \cdot b = b \cdot a = 1$$

(ясно, что тогда и элемент b обратим).

Например, в кольце \mathbb{Z}_6 обратимы элементы 1 и 5: $1 \cdot 1 = 5 \cdot 5 = 1$. Если p — простое число, то все ненулевые элементы кольца \mathbb{Z}_p обратимы: например, в $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$: $1 \cdot 1 = 1$, $2 \cdot 3 \equiv_5 1$, $4 \cdot 4 \equiv_5 1$.

Элемент $p \neq 0$ *целостного* кольца называется *неприводимым* или *неразложимым*, если он не является произведением двух необратимых элементов. Например, в кольце \mathbb{Z} обратимы только элементы ± 1 , а неразложимы — простые числа и противоположные к ним.

Определение 1.8. Целостное кольцо, в котором каждый ненулевой элемент либо обратим, либо однозначно с точностью до перестановки сомножителей и умножения на обратимый элемент представляется в виде произведения *неразложимых* элементов, называется *факториальным* или *гауссовым*.

- \mathbb{Z} — факториальное кольцо: для любого целого n справедливо *примарное разложение* (по простым) — $n = \pm 1 \cdot p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$.
- Кольцо $\{a \pm i\sqrt{3} \mid a \in \mathbb{R}\}$ не факториально, т. к., например, число 4 имеет два представления в виде произведения неразложимых:

$$4 = 2 \cdot 2 = (1 + i\sqrt{3}) \cdot (1 - i\sqrt{3}).$$

Определение 1.9. Непустое подмножество S носителя R кольца $\langle R, +, \cdot, 0 \rangle$ называется его *подкольцом*, если оно само является кольцом, относительно операций $+$ и \cdot . Подкольцо *собственное*²⁾, если $S \neq R$.

Идеалы колец и факторкóльца

Определение 1.10. Подкольцо I коммутативного³⁾ кольца $\langle R, +, \cdot, 0 \rangle$ называется его (*двусторонним*)

²⁾ Кстати, термин *собственный* — неудачный перевод английского слова *proper*; следовало бы говорить *правильный* или *настоящий*, но так уж исторически сложилось и не исправить...

³⁾ Для некоммутативного кольца вводят понятия *правых* и *левых идеалов*, но они нам не понадобятся. Пример правого неглавного идеала в кольце матриц порядка n : совокупность матриц, у которых все столбцы, кроме первого — нулевые.

идеалом, символически $I \triangleleft R$, если оно устойчиво относительно относительно умножения на элементы R , т. е. для любых $i \in I$ и $r \in R$ справедливо $i \cdot r \in I$.

Пример идеала в кольце целых: все чётные числа.

Само кольцо и его нуль 0 — *тривиальные идеалы* кольца. Идеалы, не совпадающие со всем кольцом — *собственные*; 0 принадлежит любому идеалу.

Можно определить сумму и произведение идеалов и работать с ними как с «идеальными числами».

Определение 1.11. Идеал I унитарного коммутативного кольца R называется *главным порождённым элементом* $a \in R$, если

$$I = \{ a \cdot r \mid r \in R \} = (a).$$

Целостные кольца, в которых все идеалы главные, называются *кольцами главных идеалов КГИ*.

Примеры КГИ:

- кольцо целых \mathbb{Z} — все его идеалы имеют вид $(n) = n\mathbb{Z} = \{ 0, \pm n, \pm 2n, \dots \}$.
- кольцо \mathbb{Z}_n — так как вместе с любыми элементами идеал всегда содержит их НОД.

Например, для \mathbb{Z}_6 : $(0) = 0$, $(1) = (5) = \mathbb{Z}_6$,
 $(2) = (4) = \{0, 2, 4\}$, $(3) = \{0, 3\}$.

Все КГИ факториальны.

Определение 1.12. *Классом вычетов по модулю идеала* I кольца $\langle R, +, \cdot, 0 \rangle$ с представителем $r \in R$, называют множество

$$\bar{r}_I = \{ r + i \mid i \in I \}.$$

Если идеал фиксирован, пишут просто \bar{r} . Классы вычетов разных представителей по модулю данного идеала —

- либо совпадают, либо не пересекаются;
- в объединении дают R ;
- порождаются любым своим элементом:

$$a \in \bar{r} \Rightarrow \bar{a} = \bar{r}.$$

В кольце целых \mathbb{Z} класс вычетов по идеалу (n) с представителем $0 \leq r \leq n - 1$ есть

$$\bar{r} = \{r, r \pm n, r \pm 2n, \dots\}$$

— все целые, дающие при делении на n остаток r . Далее, как правило, будем опускать черту над символом представителем класса.

На классах вычетов определены операции сложения и умножения, индуцированные операциями над представителями. При этом совокупность всех классов вычетов кольца R по модулю идеала I образуют *факторкольцо*, символически R/I .

Понятно, что ранее рассмотренное кольцо \mathbb{Z}_n есть факторкольцо \mathbb{Z} по идеалу (n) : $\mathbb{Z}_n \cong \mathbb{Z}/(n)$.

Пример 1.4. $I = (6) \triangleleft \mathbb{Z}$, $\mathbb{Z}/(6) \cong \mathbb{Z}_6 = \{0, 1, \dots, 5\}$,

$$2 + 5 = 1, \quad 2 \cdot 3 = 0, \quad 2 \cdot 5 = 4 \text{ и т. д.}$$

Определение 1.13. *Максимальным идеалом* коммутативного кольца называется всякий его собственный идеал, не содержащийся ни в каком другом собственном идеале.

В нетривиальном коммутативном кольце всегда существует максимальный идеал.

Пример 1.5. В кольце \mathbb{Z}

- идеалы (2) и (3) максимальны;
- идеал (6) не максимален, т. к. он содержится и в идеале (2), и в идеале (3): любое число, делящееся на 6 делится также и на 2, и на 3.
- максимальные идеалы имеют вид (p) , где p — простое число.

Евклидовы кольца

Определение 1.14. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$ называется *евклидовым*, если для каждого его элемента a определена норма $N(a) \in \mathbb{N}_0$ со свойством: для любого элемента $b \neq 0$:

- 1) существуют такие элементы q и r , что $a = q \cdot b + r$ и либо $r = 0$, либо $N(r) < N(b)$;
- 2) $N(a) \leq N(ab)$.

Наличие нормы даёт возможность производить деление элементов кольца друг на друга с остатком.

Пример 1.6. • Классический пример евклидова кольца — кольцо целых чисел \mathbb{Z} ; норма — абсолютная величина числа.

- Кольцо $\mathbb{R}[x]$ многочленов с действительными коэффициентами евклидово, норма — степень многочлена.

Все евклидовы кольца — КГИ.

Поле

Определение 1.15. Целостное кольцо $\langle K, +, \cdot, 0, 1 \rangle$, в котором все элементы, кроме 0, обратимы, называется *полем*.

Поле также можно определить как такую пятёрку $\langle K, +, \cdot, 0, 1 \rangle$, что $\langle K, +, 0 \rangle$ — абелева группа по сложению, $\langle \{K \setminus \{0\}, \cdot, 1 \rangle$ — абелева группа по умножению, связанные дистрибутивным законом $x \cdot (y + z) = x \cdot y + x \cdot z$ для всех $x, y, z \in K$.

Для нас важны следующие свойства поля:

- 1) ненулевые элементы поля образуют группу относительно умножения, её называют *мультипликативной группой* данного поля;
- 2) факторкольцо R/I является полем если и только если идеал I кольца R *максимальный*.
- 3) Конечное коммутативное унитарное кольцо без делителей нуля является полем.

Подмножество поля K , само являющееся полем и устойчивое относительно сужения на него операций из K , называется *подполем*. Примеры бесконечных полей и их подполей — числовые поля $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; конечного поля — \mathbb{Z}_p , p — простое число.

Поле, не обладающее никаким собственным подполем, называется *простым*. Поля \mathbb{Q} и \mathbb{Z}_p — простые.

Взаимнооднозначное отображение φ поля K на поле K' называется *изоморфным отображением* или *изоморфизмом*, если для любых a, b из K

- 1) $\varphi(a + b) = \varphi(a) + \varphi(b)$;

$$2) \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Утверждение 1.2. В каждом поле содержится только одно простое подполе, которое изоморфно либо \mathbb{Q} , либо \mathbb{Z}_p , p — простое.

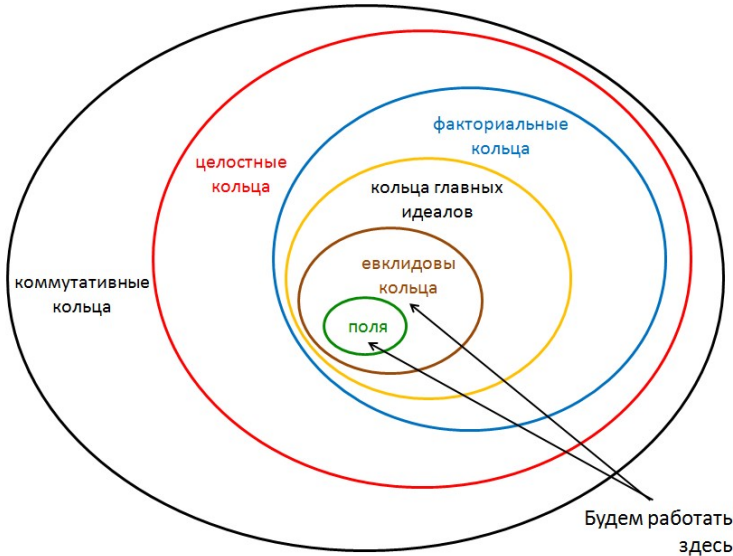


Рис. 1.2. От ассоциативных колец к полям

1.3 Задачи

1.1. Выяснить, образуют ли группы следующие множества при указанной операции над элементами:

- 1) Целые числа, кратные данному натуральному числу n , относительно сложения?
- 2) Неотрицательные целые числа относительно сложения?

- 3) Нечетные целые числа относительно сложения?
- 4) Целые числа относительно вычитания?
- 5) Рациональные числа относительно умножения?
- 6) Рациональные числа, отличные от нуля, относительно умножения?
- 7) Положительные рациональные числа относительно умножения?
- 8) Положительные рациональные числа относительно деления?
- 9) Корни n -й степени из единицы (как действительные, так и комплексные) относительно умножения?
- 10) Матрицы порядка n с действительными элементами относительно умножения?
- 11) Невырожденные матрицы порядка n с действительными элементами относительно умножения?
- 12) Перестановки чисел $1, 2, \dots, n$ относительно композиции перестановок?
- 13) Преобразования множества M , то есть взаимнооднозначные отображения этого множества на себя, относительно композиции отображений?
- 14) Элементы n -мерного векторного пространства \mathbb{R}^n относительно сложения?
- 15) Параллельные переносы трехмерного пространства \mathbb{R}^3 относительно композиции движений?
- 16) Повороты трехмерного пространства \mathbb{R}^3 вокруг прямых, проходящих через данную точку O относительно композиции движений?

1.2. Найти степени и порядки всех элементов циклической группы 6-го порядка. Какие из них являются порождающими?

1.3. Найти все подгруппы и порождающие элементы циклической группы порядка 24.

1.4. Показать, что если $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ — примарное разложение $n \in \mathbb{N}$, то

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right).$$

1.5. Выяснить, какие из следующих множеств являются кольцами, а какие полями относительно естественных операций на них.

- 1) Квадратные матрицы данного порядка с действительными элементами относительно сложения и умножения матриц?
- 2) Многочлены одного неизвестного с целыми коэффициентами относительно обычных операций сложения и умножения?
- 3) Многочлены одного неизвестного с действительными коэффициентами относительно обычных операций?

1.6. Покажите, что для любого элемента r кольца справедливо $0 \cdot r = r \cdot 0 = 0$.

1.7. Пусть $\langle R, +, \cdot \rangle$ и $\langle R', \oplus, \otimes \rangle$ — кольца. Отображение $\varphi : R \rightarrow R'$ называется *гомоморфизмом*, если

$$\varphi(r_1 + r_2) = \varphi(r_1) \oplus \varphi(r_2), \quad \varphi(r_1 \cdot r_2) = \varphi(r_1) \otimes \varphi(r_2).$$

Взаимно-однозначный гомоморфизм колец называется их *изоморфизмом*, символически $R \cong R'$.

Является ли отображение $f : \mathbb{Z} \rightarrow 2\mathbb{Z}$, $f(x) = 2x$ гомоморфизмом колец?

1.8. Показать, что множество векторов V пространства с операциями сложения и векторного умножения является кольцом. Является ли оно ассоциативным? коммутативным?

1.9. Указать классы вычетов кольца \mathbb{Z}_6 по идеалу (3).

1.10. Является ли 2-элементное поле подполем 5-элементного?

Глава 2

Конечные кольца и поля

2.1 Поля Галуа

Простые поля Галуа — поля вычетов

- \mathbb{Z} — кольцо целых чисел.
- p — простое число.
- $(p) = p\mathbb{Z} = \{0, \pm p, \pm 2p, \dots\}$ — идеал, порождённый числом p .
- $\mathbb{Z}/(p) = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ — p -элементное кольцо вычетов по модулю этого идеала, то есть классы остатков от деления целых чисел на p :

$$\left. \begin{array}{l} \bar{0} = 0 + (p), \\ \bar{1} = 1 + (p), \\ \dots \dots\dots \\ \overline{p-1} = p-1 + (p) \end{array} \right\} \Rightarrow \mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят, заменяя класс его представителем — наименьшим по модулю положительным элементом.

Поскольку p — простое, то идеал (p) — максимальный и $\mathbb{Z}/(p)$ — поле. Его называют *простым полем Галуа* и обозначают \mathbb{F}_p или $GF(p)^1$. Любое конечное

¹⁾ В честь Эвариста Галуа (1811–1832); первым обозначением обычно пользуются математики, а вторым — специалисты по информатике.

поле называют также полем Галуа.

Примеры: таблицы сложения и умножения в поле \mathbb{F}_3 и факторкольце $\mathbb{Z}/(4)$ —

$\mathbb{F}_3 :$	$\begin{array}{c ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$	$\begin{array}{c ccc} \times & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$
$\mathbb{Z}/(4):$	$\begin{array}{c cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$	$\begin{array}{c cccc} \times & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$

В факторкольце $\mathbb{Z}/(4) \cong \mathbb{Z}_2$: $2 \times 2 = 0$ (!)
Однако поле из 4-х элементов существует...

Характеристика поля. Пусть K — произвольное поле. Будем складывать его единицы: $1 + 1 = 2$, $1 + 1 + 1 = 3$, ...

В конечном поле всегда найдётся первое k такое, что

$$\underbrace{1 + \dots + 1}_{p \text{ единиц}} = 0.$$

Это значение p — порядок аддитивной группы поля K называют *характеристикой поля*, символически $\text{char } K$.

Ясно, что $\text{char } K$ — простое число: иначе, если $\text{char } K = u \cdot v$, то получим $(u \cdot 1) \cdot v = 0$, т. е. наличие в K делителей нуля.

Если все суммы вида $1 + \dots + 1$ различны, то полагают $\text{char } K = 0$ (а не ∞). Числовые поля \mathbb{Q} , \mathbb{R} , \mathbb{C} — нулевой характеристики.

$\{0, 1, \dots, \text{char } K - 1\} \cong \mathbb{Z}_{\text{char } K}$ — минимальное подполе любого поля K положительной характеристики.

Существуют и бесконечные поля положительной характеристики. Таким будет, например, поле $K(x)$ рациональных функций над конечным полем K , элементами которого являются “дроби” P/Q (если $Q \neq 0$), где P и Q — многочлены от формальной переменной x с коэффициентами из K . На множестве данных “дробей” вводятся отношение эквивалентности, операции сложения, умножения и деления, аналогично как это делается для рациональных чисел в форме простых дробей.

В конечном поле возможно сильное упрощение вычисления степеней сумм.

Лемма 2.1 (тождество Фробениуса). В поле характеристики $p > 0$ выполнено тождество

$$(a + b)^p = a^p + b^p.$$

Доказательство. В любом коммутативном кольце верна формула для степени бинома

$$(a + b)^p = a^p + \underbrace{C_p^1 a^{p-1} b + \dots + C_p^{p-1} a b^{p-1}}_{=0} + b^p,$$

в которой при $i = 1, \dots, p - 1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p , а знаменатель — нет, откуда $C_p^i \equiv_p 0$. □

Следствие. В поле характеристики $p > 0$ для любого натурального n справедливо

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Мультипликативная группа и примитивный элемент конечного поля. Обозначим $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ мультипликативную группу q -элементного поля Галуа \mathbb{F}_q .

Утверждение 2.1. \mathbb{F}_q^* — циклическая по умножению группа порядка $q - 1$.

Порождающие элементы мультипликативной группы поля называют его *примитивными элементами*. Если α — примитивный элемент поля \mathbb{F}_q , то $\text{ord } \alpha = q - 1$ и справедливо представление

$$\mathbb{F}_q = \left\{ 0, \underbrace{\alpha, \alpha^2, \dots, \alpha^{q-2}, \alpha^{q-1} = 1}_{\mathbb{F}_q^*} \right\}.$$

Рассмотрим поле \mathbb{F}_{11} . Его мультипликативная группа есть $\mathbb{F}_{11}^* \cong \langle \{1, 2, \dots, 10\}, \cdot, 1 \rangle$ и она имеет $\varphi(10) = 4$ примитивных элемента.

Попробуем их найти. Проверяем элемент 2:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

— т. е. элемент 2 — примитивный. Проверяем 3:

k	1	2	3	4	5
3^k	3	9	5	4	1

— то есть $\text{ord } 3 = 5 \neq 10$ и 3 — не примитивный, и т. д.

Как ускорить процесс?

Если примарное разложение числа $p - 1$

— известно \Rightarrow элемент $\alpha \in \mathbb{F}_p^*$ примитивен если и только если

$$\alpha^{\frac{p-1}{q}} \neq 1 \text{ для каждого простого } q \mid (p-1).$$

Примеры: 1) $p = 11$ (наш случай), $p - 1 = 10 = 2 \cdot 5$, проверяем степени q из множества $\{2, 5\}$:

$$2^2 = 4 \neq 1, 2^5 = 10 \neq 1 \Rightarrow 2 \text{ — примитивный,}$$

$$3^2 = 9 \neq 1, 3^5 = 1 \Rightarrow 3 \text{ — не примитивный.}$$

2) Для $GF(37)$ $p - 1 = 36 = 2^2 \cdot 3^2$. Находим: $\frac{36}{2} = 18$, $\frac{36}{3} = 12$; поэтому для выяснения, является ли элемент α примитивным, нужно проверить не более двух равенств: $\alpha^{12} = 1$ и $\alpha^{18} = 1$.

— неизвестно \Rightarrow эффективного алгоритма не найдено; используют таблицы, вероятностные алгоритмы...

Если найден один примитивный элемент α поля \mathbb{F}_p , то любой другой его примитивный элемент может быть получен как степень α^k , где k — взаимно просто с $p - 1$. В нашем примере 2 — примитивный элемент \mathbb{F}_{11} , $k \in \{1, 3, 7, 9\}$ — взаимно простые с 10 , получим, что $6, 7$ и 8 — также примитивные элементы \mathbb{F}_{11} :

$$2^1 = 2, 2^3 = 8, 2^7 = 7, 2^9 = 6.$$

Деление в кольце многочленов. Корни многочленов. Поскольку кольцо многочленов над полем евклидово, то многочлены можно делить друг на друга с остатком.

Пример 2.1. В кольце $\mathbb{Z}_2[x]$ разделим «уголком» $f(x) = x^7 + x^4 + x^2 + 1$ на $g(x) = x^3 + x + 1$ с остатком (см. рис. 2.1):

$$\begin{array}{r}
 -x^7 + \quad x^4 + x^2 + 1 \quad | \quad x^3 + x + 1 \\
 \underline{x^7 + x^5 + x^4} \quad | \quad x^4 + x^2 + 1 \\
 \quad -x^5 + \quad x^2 + 1 \\
 \quad \quad \underline{x^5 + x^3 + x^2} \\
 \quad \quad \quad -x^3 + \quad 1 \\
 \quad \quad \quad \quad \underline{x^3 + x + 1} \\
 \quad \quad \quad \quad \quad x
 \end{array}$$

Рис. 2.1. Деление многочленов «уголком»

Получили частное $x^4 + x^2 + 1$ и остаток x .

Корнем многочлена $f(x)$ из кольца многочленов $K[x]$ над полем K называется такой элемент $a \in K$, что $f(a) = 0$. В этом случае бином $x - a$ делит $f(x)$: кольцо $K[x]$ евклидово, при делении $f(x)$ на $x - a$ получаем $f(x) = (x - a)q(x) + r$, r -константа, что при подстановке $x = a$ даёт $0 = f(a) = 0 \cdot q(a) + r$, т. е. $r = 0$.

Неприводимые многочлены. Многочлен над некотором полем называется *неприводимым* или *неразложимым*, если он не является произведением двух многочленов ненулевой степени.

Поскольку евклидовы кольца факториальны, любой многочлен над любым полем однозначно с точностью до перестановок разлагается в произведение неприводимых или сам является таковым.

В кольце многочленов над:

\mathbb{Q} — существуют неприводимые многочлены произвольной степени;

\mathbb{R} — неприводимы линейные многочлены и квадратные с отрицательным дискриминантом;

\mathbb{C} — неприводимы только линейные многочлены.

Далее нас будут интересовать неприводимые многочлены в кольцах $\mathbb{F}_p[x]$ (над простыми полями Гаула), т. е. вида

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_i \in \mathbb{F}_p, \quad i = \overline{0, n-1}.$$

Неприводимые многочлены из $\mathbb{F}_2[x]$ степеней 2...5.

Вторая степень: $x^2 + ax + b$.

Ясно, что $b = 1$, иначе $x^2 + ax = x(x+a) \Rightarrow$ ищем неприводимый многочлен в виде $x^2 + ax + 1$.

Если $a = 0$, то $x^2 + 1 = (x+1)^2$; поэтому $a = 1$ и получаем *единственный* неприводимый многочлен степени 2 над \mathbb{F}_2 : $x^2 + x + 1$.

Третья степень: $x^3 + ax^2 + bx + 1$.

Исключая, как сделано ранее, делимость на $x+1$, получаем условие $a + b = 1$, то есть

$$\text{либо } a = 0, b = 1, \quad \text{либо } a = 1, b = 0.$$

Проверкой устанавливаем, что оба эти варианта дают неприводимые многочлены

$$x^3 + x^2 + 1 \quad \text{и} \quad x^3 + x + 1.$$

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$.

Исключение делимости на $x + 1$ приводит к условию $a + b + c = 1$, то есть остаются к рассмотрению 4 варианта, которые дают 3 неприводимых многочлена:

a	b	c	многочлен
0	0	1	$x^4 + x + 1$
0	1	0	$x^4 + x^2 + 1 = (x^2 + x + 1)^2 - \text{приводимый}$
1	0	0	$x^4 + x^3 + 1$
1	1	1	$x^4 + x^3 + x^2 + x + 1$

Пятая степень: $x^5 + ax^4 + bx^3 + cx^2 + dx + 1$.

Исключение делимости на $x + 1$ приводит к условию $a + b + c + d = 1$ — 8 вариантов. Далее необходимо исключить делимость на многочлены 2 и 3-й степеней; их один и два соответственно и их произведения дают два многочлена. Приведём 6 неприводимых многочленов 5-й степени:

$$\begin{aligned} x^5 + x^2 + 1, & & x^5 + x^3 + 1, \\ x^5 + x^3 + x^2 + x + 1, & & x^5 + x^4 + x^2 + x + 1, \\ x^5 + x^4 + x^3 + x + 1, & & x^5 + x^4 + x^3 + x^2 + 1. \end{aligned}$$

Теорема 2.1 (о существовании неприводимых многочленов). *Для любых простого p и натурального n в $\mathbb{F}_p[x]$ существует неприводимый многочлен степени n .*

— докажем позже.

Итак, в кольцах $\mathbb{F}_p[x]$ есть неприводимые многочлены любой степени, но как их найти?

Для этого *нет эффективных алгоритмов*; известные неприводимые многочлены приводят в таблицах.

Расширения простых полей. С помощью неприводимых многочленов можно строить *новые конечные поля* — *расширения* простых полей аналогично построению самого простого поля:

- 1) выбирая простое p , фиксируем поле \mathbb{F}_p и рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над \mathbb{F}_p ;
- 2) выбираем натуральное n и *неприводимый многочлен* над \mathbb{F}_p —

$$a(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{F}_p[x], \quad a_n \neq 0;$$

- 3) идеал $(a(x))$ порождает факторкольцо $\mathbb{F}_p[x]/(a(x))$, элементы которого суть совокупности $\overline{r(x)}$ многочленов, дающих при делении на $a(x)$ остаток $r(x)$; множество всех таких остатков $\{r(x)\}$ есть совокупность всех многочленов из $\mathbb{F}_p[x]$ степеней от 0 до $n - 1$.

Утверждение 2.2. Множество $\{\overline{r(x)}\}$ является полем Галуа $GF(p^n)$ относительно сложения и умножения вычетов.

Действительно, кольцо многочленов $\mathbb{F}_p[x]$ евклидово, многочлен $a(x)$ неприводим, следовательно ид-

еал $(a(x))$ — максимальный и $\left\{ \overline{r(x)} \right\}$ — поле. Данное поле обозначают \mathbb{F}_p^n и называют *расширением n -й степени* простого поля \mathbb{F}_p .

Пример 2.2. Построим поле \mathbb{F}_3^2 . Для этого выберем в $\mathbb{F}_3[x]$ неприводимый многочлен: пусть это будет $x^2 + 1$. Тогда искомое поле 9-элементное поле есть

$$\begin{aligned} \mathbb{F}_3^2 &\cong \mathbb{F}_3[x]/(x^2 + 1) = \\ &= \left\{ \overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2} \right\}. \end{aligned}$$

Можно составить таблицы сложения и умножения в этом поле с учётом $x^2 = -1 \equiv_3 2$. Например:

$$\begin{aligned} \overline{x+1} + \overline{x+2} &= \overline{2x}, & \overline{x} \cdot \overline{2x} &= \overline{1}, \\ \overline{2x+1} + \overline{x} &= \overline{1}, & \overline{2x+1} \cdot \overline{x} &= \overline{x+1}, \quad \text{и т. д.} \end{aligned}$$

Черту над элементами поля $\mathbb{F}_p[x]/(a(x))$ обычно не ставят и называют их просто «многочленами». Но надо помнить, что это суть *бесконечные совокупности* многочленов, дающих при делении на $a(x)$ один и тот же данный остаток.

Примитивные многочлены. В примере 2.2 построено поле $F = \mathbb{F}_3[x]/(x^2 + 1)$. Определим в F^* порядок корня x неприводимого многочлена $a(x) = (x^2 + 1)$: имеем $x^2 = -1 \equiv_3 2$ и $x^4 = 4 \equiv_3 1$, т. е. $\text{ord } x = 4 \neq 3^2 - 1 = 8$. Это означает, что x не является примитивным элементом построенного поля.

Когда же корень x неприводимого многочлена $a(x) \in \mathbb{F}_p[x]$, $\deg a(x) = n$ будет примитивным элементом поля $\mathbb{F}_p[x]/(a(x))$?

Ясно, что в понятиях построенного поля для этого нужно, чтобы $\text{ord } x = p^n - 1$.

В понятиях $\mathbb{F}_p[x]$ это эквивалентно требованию, чтобы многочлен $a(x)$ был *примитивным* для x , т. е. когда $t = p^n - 1$ — наименьший показатель, при котором $a(x)$ делит бином $x^t - 1$.

Например, неприводимый над \mathbb{F}_2 многочлен $x^3 + x + 1$ примитивен:

$$x^{2^3-1} - 1 = x^7 - 1 = (x^3 + x + 1) \cdot (x^4 + x^2 + x + 1)$$

и легко показать, что $(x^t + 1) \nmid (x^3 + x + 1)$ ни при каком $4 \leq t < 7$.

Также и $\text{ord } x = 7$:

$$\begin{aligned} (\mathbb{F}_2[x]/(x^3 + x + 1))^* = \{ & x^0 = 1, x^1, x^2, x^3 = x + 1, \\ & x^4 = x^2 + x, x^5 = x^2 + x + 1, x^6 = x^2 + 1 \} \end{aligned}$$

— все *многочлены* из $\mathbb{F}_2[x]$ степени не выше 2.

Выше показано, что многочлен $(x^2 + 1)$ не примитивен: он делит, например, бином $x^4 - 1$, т. е. $t = 2 \neq 8$.

2.2 Вычисления в конечных кольцах и полях

Алгоритм Евклида — применяют для нахождения НОД(a, b) *натуральных* чисел a и b (рассматриваем простейший случай — вычисления в кольце \mathbb{Z}).

Поскольку общий делитель пары чисел (a, b) остаётся им и для пары $(a - kb, b)$, $a - kb \geq 0$, то вместо

$a - kb$ можно взять остаток от деления нацело a на b , и затем, переставив числа в паре, повторить процедуру; она закончится, т. к. числа в паре уменьшаются, но остаются неотрицательными. В результате образуется пара $(r, 0)$, и ясно, что $\text{НОД}(a, b) = r$.

Алгоритм Евклида²⁾ нахождения $\text{НОД}(a, b)$,
 $a \geq b$, $a, b \in \mathbb{N}$:

- 1) вычислить r — остаток от деления a на b :
 $a = bq + r$, $0 \leq r < b$;
- 2) если $r = 0$, то b — искомое значение;
- 3) иначе заменить пару чисел (a, b) парой (b, r) и перейти к шагу 1.

Пример 2.3. Найдём $\text{НОД}(252, 105)$ по алгоритму Евклида.

- (1) $252 = 105 \cdot 2 + 42 \quad \Rightarrow (105, 42)$;
- (2) $105 = 42 \cdot 2 + 21 \quad \Rightarrow (42, 21)$;
- (3) $42 = 21 \cdot 2 + 0 \quad \Rightarrow \text{НОД}(252, 105) = 21$.

Ясно, что $\text{НОД}(a, b, c) = \text{НОД}(a, (\text{НОД}(b, c)))$.

Утверждение 2.3 (соотношение Безу³⁾). Для любых натуральных a, b и $d = \text{НОД}(a, b)$ найдутся целые коэффициенты Безу x, y такие, что $d = ax + by$.

²⁾ дважды описан в «Началах» Евклида, но не был им открыт (упоминается в «Топике» Аристотеля)

³⁾ Открыто Клодом Гаспаром Баше за 106 лет до рождения Этьена Безу. Онлайн-калькулятор коэффициентов соотношения Безу доступен по адресу <http://wims.unice.fr/wims/wims.cgi>.

Доказательство. По алгоритму Евклида $d = \text{НОД}(a, b)$ есть остаток от деления некоторых чисел, которые в свою очередь суть тоже остатки от деления и т. д., так, что процесс заканчивается на числах a и b . Учитывая, что остаток от деления числа u на v представляется в виде $u + (-q)v$, получаем представление $d = ax + by$, где целые коэффициенты x и y — целые. \square

Замечание. Коэффициенты Безу могут быть выбраны неоднозначно, например

$$\text{НОД}(12, 30) = 6 = 3 \cdot 12 + (-1) \cdot 30 = (-2) \cdot 12 + 1 \cdot 30.$$

Расширенный алгоритм Евклида находит по двум натуральным числам a и b , $a \geq b$, их натуральный НОД d и два целых x , y коэффициента Безу таких, что $|x| < |b/d|$, $|y| < |a/d|$.

Расширенный алгоритм Евклида решения соотношения Безу $ax + by = d$, $a \geq b$ в кольце \mathbb{Z} .

0. Зададим матрицу $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $r = b$.
1. Перевычислим r как остаток от деления числа a на b : $a = bq + r$, $0 \leq r < b$.
2. Если $r = 0$, то второй столбец матрицы E дает вектор $(x \ y)^T$ решений заданного соотношения, а d есть последнее ненулевое значение r .
3. Иначе заменим матрицу E матрицей

$$E \times \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}.$$

4. Заменяем пару чисел (a, b) парой (b, r) и перейдем к шагу 1.

Пример 2.4. Расширенным алгоритмом Евклида найдём натуральное d и целые x и y такие, что

$$d = \text{НОД}(252, 105) = 252x + 105y.$$

- (0) Определим матрицу $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и положим $r = 105$.

- (1) Перевычисляем $r = 252 - 105 \cdot 2 = 42 \neq 0$.

- (2) Заменяем матрицу E матрицей

$$E \times \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}.$$

- (3) Заменяем пару чисел $(252, 105)$ парой $(105, 42)$ и перейдем к шагу 1.

- (4) Вычисляем $r = 252 - 105 \cdot 2 = 21 \neq 0$.

- (5) Заменяем матрицу E матрицей

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}.$$

- (6) Заменяем пару чисел $(252, 105)$ парой $(42, 21)$ и перейдём к шагу 1.

- (7) Вычисляем $r = 42 - 21 \cdot 2 = 0$. Значения $x = -2$ и $y = 5$ найдены, как и $d = 21$.

Алгоритм Евклида и его расширенная версия остаются справедливыми в любом евклидовом кольце.

Пример 2.5. В поле $\mathbb{Z}/(101)$ решить уравнение

$$4y = 1.$$

Поскольку $101y \equiv_{101} 0$, вместо данного соотношения можно расширенным алгоритмом Евклида решать в \mathbb{Z} соотношение

$$101x + 4y = 1,$$

а затем, при необходимости, выразить y элементом из поля $\mathbb{Z}/(101)$. Тогда в результате работы алгоритма получим

$$4^{-1} = y = -25 \equiv_{101} 76 \in \mathbb{Z}/(101) \text{ и } x = 1.$$

Алгоритм Евклида и его расширенная версия остаются справедливыми в любом евклидовом кольце, что позволяет решить относительно $y(x)$ соотношения вида

$$b(x) \cdot y(x) = d(x) \pmod{a(x)}. \quad (2.1)$$

где $a(x), b(x), y(x), d(x)$ — многочлены над \mathbb{F}_p , известны только $a(x)$ и $b(x)$, $\deg a(x) \geq \deg b(x)$.

Для этого решаем в кольце $\mathbb{F}_p[x]$ соотношение Безу

$$a(x) \cdot \chi(x) + b(x) \cdot y(x) = d(x), \quad (2.2)$$

а затем, при необходимости, выражаем $y(x)$ элементом кольца $\mathbb{F}_p[x]/(a(x))$.

Если $a(x)$ — неприводимый над $\mathbb{F}_p[x]$ многочлен, то решение расширенным алгоритмом Евклида соотношения (2.2) позволяет вычислить обратный к $y(x)$ элемент в поле $\mathbb{F}_p[x]/(a(x))$.

Для этого удобна следующая форма алгоритма.

Расширенный алгоритм Евклида нахождения в поле $\mathbb{F}_p[x]/(a(x))$ элемента $y(x)$, обратного к $b(x)$, $\deg a(x) \geq \deg b(x)$.

Шаг 0. Задаём начальные значения:

$$r_{-2}(x) = a(x), \quad r_{-1}(x) = b(x),$$

$$y_{-2}(x) = 0, \quad y_{-1}(x) = 1.$$

Шаг 1. Делим $r_{-2}(x)$ на $r_{-1}(x)$ и находим частное $q_0(x)$ и остаток $r_0(x)$:

$$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$$

полагаем $y_0(x) = -q_0(x)$.

При $\deg r_0(x) > 0$ переходим к следующему шагу; иначе — к Шагу $n + 1$.

Шаг $i > 1$. Делим $r_{i-3}(x)$ на $r_{i-2}(x)$, находим частное $q_{i-1}(x)$ и остаток $r_{i-1}(x)$:

$$r_{i-3}(x) = r_{i-2}(x)q_{i-1}(x) + r_{i-1}(x),$$

вычисляем

$$y_{i-1}(x) = y_{i-3}(x) - y_{i-2}(x)q_{i-1}(x).$$

При $\deg r_{i-1}(x) > 0$ продолжаем итерации.

Шаг n . Делим $r_{n-3}(x)$ на $r_{n-2}(x)$, находим частное $q_{n-1}(x)$, остаток $r_{n-1}(x)$:

$$r_{n-3}(x) = r_{n-2}(x)q_{n-1}(x) + r_{n-1}(x),$$

вычисляем

$$y_{n-1}(x) = y_{n-3}(x) - y_{n-2}(x)q_{n-1}(x).$$

При $\deg r_{n-1}(x) = 0$, то есть $r_0(x) = c$ — константа — конец итераций.

Шаг $n + 1$. Нормировка результата: при $c \neq 1$ полагаем $y(x) = c^{-1} \cdot y_{n-1}(x)$ и $y(x) = y_{n-1}(x)$, иначе.

Пример 2.6. Найдём $(x^2 + x + 3)^{-1}$ в поле

$$\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3).$$

Для этого расширенным алгоритмом Евклида решим соотношение Безу

$$(x^4 + x^3 + x^2 + 3) \cdot \chi(x) + (x^2 + x + 3) \cdot y(x) = 1.$$

$$\begin{aligned} \text{Шаг 0: } r_{-2}(x) &= x^4 + x^3 + x^2 + 3, \\ r_{-1}(x) &= x^2 + x + 3, \\ y_{-2}(x) &= 0, \quad y_{-1}(x) = 1. \end{aligned}$$

$$\begin{aligned} \text{Шаг 1: } r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= x^2 + 5, \\ r_0(x) &= 2x + 2, \quad \deg r_0(x) = 1, \\ y_0(x) &= -q_0(x) = -x^2 - 5. \end{aligned}$$

$$\begin{aligned} \text{Шаг 2: } r_{-1}(x) &= r_0(x)q_1(x) + r_1(x), \\ q_1(x) &= 4x, \\ r_1(x) &= 3, \quad \deg r_1(x) = 0, \\ y_1(x) &= y_{-1}(x) - y_0(x)q_1(x) = \\ &= 1 + 4x(x^2 + 5) = 4x^3 + 6x + 1. \end{aligned}$$

$$\begin{aligned} \text{Шаг 3: } \text{Остаток } r_1(x) &= 3 \neq 1, \text{ поэтому} \\ &\text{вычисляем элемент } 3^{-1} \equiv_7 5 \text{ и} \\ &\text{домножаем на него } y_1 : 5y_1(x) = y(x) = \\ &= 5(4x^3 + 6x + 1) \equiv_7 6x^3 + 2x + 5. \end{aligned}$$

2.3 Алгебра векторов над конечным полем

Векторное пространство

Определение 2.1. Абстрактным векторным пространством над полем $K = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\langle V, K; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — множество векторов, являющееся коммутативной группой по сложению (+) с нулевым элементом 0;
- \cdot — бинарная операция умножения элемента («числа») из K на вектор из V : $K \times V \rightarrow V$,

причём операции $+$ и \cdot удовлетворяют следующим аксиомам:

- 1) $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$, $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$;
- 2) $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$;
- 3) $1 \cdot v = v$.

Пример 2.7. Пусть $V = K^n$ — множество конечных последовательностей длины n элементов поля K . Сложение и умножение элементов из V на число из K определим покомпонентно.

Получившаяся структура есть векторное пространство, которое называют n -мерным координатным пространством над полем K . Ясно, что если K — конечное поле, то V содержит $|K|^n$ элементов.

Теорема 2.2. Поле $GF(q)$ характеристики p есть векторное пространство над $GF(p)$.

Доказательство. Поле $V = GF(q)$ — коммутативная группа по сложению с нулём 0, умножение элементов $K = GF(p)$ на элементы V можно заменять перемножением элементов $GF(q)$, поскольку K изоморфно его простому подполю, а аксиомы векторного пространства, очевидно, выполняются в поле $GF(q)$. \square

Следствия. 1. Поле Галуа $GF(q)$ характеристики p состоит из p^n элементов, т. е. $q = p^n$, $n \in \mathbb{N}$.

2. Для каждого простого p и натурального n существует ровно с точностью до изоморфизма поле Галуа.

Действительно, свяжем нули двух полей из p^n отображением изоморфизма, тогда их мультипликативные группы также изоморфны, как конечные циклические группы одинакового порядка.

Представление элементов конечных полей.

Поле $GF(p^n) = \mathbb{F}_p^n$, $n \in \mathbb{N}$ можно рассматривать

- как факторкольцо $\mathbb{F}_p[x]/(a(x))$ вычетов $\mathbb{F}_p[x]$ по идеалу некоторого неприводимого многочлена $a(x)$ степени n ,
- или как n -мерное координатное пространство над \mathbb{F}_p .

Следующая теорема указывает на базис поля $GF(p^n)$ как векторного пространства.

Теорема 2.3. Базис \mathbb{F}_p^n образуют n элементов $\bar{1}$, \bar{x} , \dots , \bar{x}^{n-1} .

Доказательство. Во-первых, любой элемент \mathbb{F}_p^n представим в виде линейной комбинации указанных векторов:

$$\overline{b_0 + b_1x + \dots + b_{n-1}x^{n-1}} = b_0\bar{1} + b_1\bar{x} + \dots + b_{n-1}\overline{x^{n-1}}.$$

Во-вторых, $\mathbb{F}_p^n \cong \mathbb{F}_p[x]/(a(x))$ для некоторого неприводимого многочлена $a(x)$ степени n . Поэтому если

$$c(x) = c_0\bar{1} + c_1\bar{x} + \dots + c_{n-1}\overline{x^{n-1}} = \bar{0},$$

то это означает, что многочлен $c(x)$ степени $n - 1$ делится без остатка на $a(x)$, что возможно лишь если при $c(x) \equiv 0$, т. е. $c_0 = \dots = c_{n-1} = 0$, а это означает, что система векторов $\bar{1}, \bar{x}, \dots, \overline{x^{n-1}}$ линейно независима. \square

Приведём в качестве примера таблицу ненулевых элементов поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^4 + x + 1)$, записанных многочленами от порождающего примитивного элемента $x = \alpha$. Многочлены будем записывать в порядке возрастания степеней формальной переменной.

степень α	$\alpha^4 = \alpha + 1$	1	x	x^2	x^3
α		(0	1	0	0)
α^2		(0	0	1	0)
α^3		(0	0	0	1)
$\alpha^4 = 1 + \alpha$		(1	1	0	0)
$\alpha^5 = \alpha + \alpha^2$		(0	1	1	0)
$\alpha^6 = \alpha^2 + \alpha^3$		(0	0	1	1)
$\alpha^7 = \alpha^3 + \alpha^4 = \alpha^3 + \alpha + 1$		(1	1	0	1)
$\alpha^8 = (1 + \alpha)^2 = 1 + \alpha^2$		(1	0	1	0)

$\alpha^9 = \alpha + \alpha^3$	$(0 \ 1 \ 0 \ 1)$
$\alpha^{10} = (\alpha + \alpha^2)^2 = \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2$	$(1 \ 1 \ 1 \ 0)$
$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$	$(0 \ 1 \ 1 \ 1)$
$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$	$(1 \ 1 \ 1 \ 1)$
$\alpha^{13} = 1 + \alpha^2 + \alpha^3$	$(1 \ 0 \ 1 \ 1)$
$\alpha^{14} = 1 + \alpha^3$	$(1 \ 0 \ 0 \ 1)$
$\alpha^{15} = 1$	$(1 \ 0 \ 0 \ 0)$

Пусть теперь требуется найти $(x^3 + x + 1) \cdot (x^2 + x + 1)$. Используя таблицу это сделать значительно легче, чем прямым перемножением многочленов:

$$(x^3 + x + 1)(x^2 + x + 1) = \alpha^7 \alpha^{10} = \alpha^{17} \stackrel{\alpha^{15}=1}{=} \alpha^2 = x^2.$$

Замечание. Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналогии доказанных теорем справедливы *не только в случае конечных полей.*

Например:

- 1) рассмотрим поле действительных чисел \mathbb{R} и кольцо многочленов $\mathbb{R}[x]$ над ним;
- 2) в кольце $\mathbb{R}[x]$ возьмём неприводимый многочлен $x^2 + 1$;

- 3) построим поле F как факторкольцо

$$F = \mathbb{R}[x]/(x^2 + 1);$$

- 4) базис F как векторного пространства есть $\{\bar{1}, \bar{x}\}$ и каждый элемент $z \in F$ представим в виде $z = a\bar{1} + b\bar{x}$, $a, b \in \mathbb{R}$.

Поле F изоморфно полю комплексных чисел \mathbb{C} .

Лемма 2.2. *Поле \mathbb{F}_p^m есть подполе \mathbb{F}_p^n , если и только если $m \mid n$.*

Доказательство. Пусть поле $K_1 = \mathbb{F}_p^m$ — подполе поля $K_2 = \mathbb{F}_p^n$. Рассуждая как при доказательстве теоремы 2.2, убеждаемся, что K_2 можно рассматривать, как векторное пространство некоторой размерности d над полем K_1 . А это значит, что K_2 имеет $|K_1|^d = p^n$ элементов, то есть $p^n = (p^m)^d$, что и означает $m \mid n$.

Обратное следует из существования и единственности с точностью до изоморфизма полей Галуа одинаковой мощности. \square

2.4 Корни многочленов над конечным полем

Минимальный многочлен. Рассмотрим элемент β некоторого конечного поля характеристики p и будем интересоваться многочленами над \mathbb{F}_p , для которых он является корнем.

Определение 2.2. *Минимальным многочленом (м. м.) элемента $\beta \in \mathbb{F}_p^n$ называется нормированный многочлен $m_\beta(x)$ над \mathbb{F}_p наименьшей степени, для которого β является корнем.*

Сразу заметим, что минимальный многочлен для x можно получить из порождающего поле неприводимого. Для этого рассмотрим поле

$F = \mathbb{F}_p[x]/(a(x)) \cong \mathbb{F}_p^n$, порождаемое неприводимым многочленом

$$a(x) = a_0 + a_1x + \dots + a_nx^n$$

и убедимся, что многочлен $a_n^{-1}a(x)$ — минимальный для элемента $\bar{x} = (0, 1, 0, \dots, 0) \in F$.

Во-первых, \bar{x} — корень $a(x)$, т. к.

$$a_0 + a_1\bar{x} + \dots + a_n(\bar{x})^n = \overline{a_0 + a_1x + \dots + a_nx^n} = \bar{0},$$

а значит и корень $a_n^{-1}a(x)$.

Во-вторых, если существует многочлен $b(x)$ степени $m < n$ такой, что

$$b(x) = \underbrace{b_0 + b_1\bar{x} + \dots + b_{n-1}(\bar{x})^m}_{= \bar{0}},$$

то подчеркнутое равенство означает линейную зависимость между элементами базиса $\bar{1}, \bar{x}, \dots, \overline{x^{n-1}}$ поля F , что невозможно.

Ясно, что примитивный многочлен является м. м. для примитивного элемента поля.

Свойства минимальных многочленов. Покажем, что м. м. для каждого элемента конечного поля: (а) существует, (б) неразложим и (в) единственен.

Утверждение 2.4. Для каждого элемента β поля \mathbb{F}_p^n существует м. м. и его степень не превосходит n .

Доказательство. Рассмотрим элементы $1, \beta, \beta^2, \dots, \beta^n$ поля \mathbb{F}_p^n . Их $n + 1$ штук, а размерность \mathbb{F}_p^n как векторного пространства равна n . Следовательно, эти элементы линейно зависимы, то есть существуют такие не все равные 0 коэффициенты c_0, \dots, c_n , что

$$c_0 + c_1\beta + \dots + c_n\beta^n = 0.$$

Поэтому β — корень многочлена $c(x) = c_0 + c_1x + \dots + c_nx^n$. М. м. для β будет некоторый нормированный неразложимый делитель $c(x)$. \square

Утверждение 2.5. *Минимальные многочлены неразложимы.*

Доказательство. Пусть $m_\beta(x)$ — м. м. для β и $m_\beta(x) = m_1(x) \cdot m_2(x)$, $1 < \deg m_1(x), \deg m_2(x)$.

Тогда из $m_\beta(\beta) = 0$ следует, что либо $m_1(\beta) = 0$, либо $m_2(\beta) = 0$, но степени этих многочленов строго меньше степени $m_\beta(x)$, и поэтому β не может быть их корнем. \square

Утверждение 2.6. *Пусть $m_\beta(x)$ — м. м. для элемента β в некоторого поля Галуа, а $f(x)$ — многочлен имеющий β своим корнем. Тогда $m_\beta(x) \mid f(x)$.*

Доказательство. Разделим $f(x)$ на $m_\beta(x)$ с остатком:

$$f(x) = u(x) \cdot m_\beta(x) + v(x), \quad 0 \leq \deg v < \deg m_\beta(x).$$

Подставляя в это равенство β вместо x , получаем

$$0 = f(\beta) = u(\beta) \cdot \underbrace{m_\beta(\beta)}_{=0} + v(\beta) = v(\beta),$$

то есть β — корень $v(x)$, что противоречит минимальности $m_\beta(x)$ и поэтому $v(x) \equiv 0$. \square

Следствие. Для каждого элемента поля существует не более одного м.м.

Действительно, если минимальных многочленов два, то они должны взаимно делить друг друга, а значит, различаться на обратимый множитель-константу. Поскольку м. м. нормирован, эта константа равна 1, т. е. эти многочлены совпадают.

Свойства многочленов над конечным полем.

Полем разложения (расширения) многочлена $f(x)$ над \mathbb{F}_p называют наименьшее по n расширение \mathbb{F}_p^n простого поля \mathbb{F}_p , в котором $f(x)$ разлагается в произведение линейных множителей.

Ясно, что в поле разложения лежат все корни данного многочлена.

Теорема 2.4. Любой элемент поля $GF(q)$ удовлетворяет равенству $x^q - x = 0$.

Доказательство. Мультипликативная группа поля $GF(q)$ имеет порядок $q - 1$, и поэтому каждый её элемент удовлетворяет равенству $x^{q-1} = 1$. Следовательно, каждый элемент поля, включая 0, удовлетворяет равенству $x(x^{q-1} - 1) = x^q - x = 0$. \square

Для $q = p^n$ имеем следующие

Следствия. 1) Каждый элемент поля \mathbb{F}_p^n , не включая 0, есть корень бинома $x^{p^n} - x$.

2) Каждый ненулевой элемент поля \mathbb{F}_p^n есть корень бинома $x^{p^n-1} - 1 = 0$, поэтому в этом поле справедливо представление

$$x^{p^n-1} - 1 = (x - \beta_1) \cdot \dots \cdot (x - \beta_{p^n-1}),$$

где $\{\beta_1, \dots, \beta_{p^n-1}\}$ — все элементы $(\mathbb{F}_p^n)^*$.

Это означает, что \mathbb{F}_p^n — поле разложения бинома $x^{p^n-1} - 1$.

- 3) Для случая $n = 1$ доказана теорема Ферма: любой элемент $a \in \mathbb{F}_p$, взаимно простой с p , удовлетворяет сравнению

$$a^{p-1} = 1 \pmod{p}.$$

Теорема 2.5 (о делимости биномов). В кольце многочленов

$$(x^m - 1) \div (x^n - 1) \Leftrightarrow m \div n.$$

Доказательство. Введём обозначение $x^n = y$, тогда $x^n - 1 = y - 1$ и далее $k \in \mathbb{N}$.

- Если $m \div n$, то $m = kn$ и имеем

$$x^m - 1 = y^k - 1 = (y-1) \cdot (y^{k-1} + y^{k-2} + \dots + y + 1).$$

- Если $m \not\div n$, то $m = kn + r$, $1 \leq r < n$ и имеем

$$x^m - 1 = x^r y^k - 1 = x^r \underbrace{(y^k - 1)}_{\text{делится на } y-1} + \underbrace{x^r - 1}_{\text{не делится на } y-1}.$$

□

Теорема даёт возможность раскладывать биномы $x^n - 1$ при составных n на (возможно разложимые далее) многочлены над \mathbb{F}_p .

Пример 2.8. Многочлен $x^{15} + 1$ над \mathbb{F}_2 (где $-1 = +1$) делится на $x^3 + 1$ и на $x^5 + 1$:

$$\begin{aligned} x^{15} + 1 &= (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1) = \\ &= (x^5 + 1)(x^{10} + x^5 + 1). \end{aligned}$$

Возможность раскладывать биномы *специального* вида на *неприводимые* даёт следующая

Теорема 2.6. *Все неприводимые многочлены n -й степени над \mathbb{F}_p делят бином $x^{p^n} - x$.*

Доказательство.

$n = 1$. Убеждаемся, что $(x - a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: поскольку $a^p = a$, оба бинома имеют корень a .

$n > 1$. Выбираем неприводимый нормированный многочлен $f(x)$ степени n из $\mathbb{F}_p[x]$ и строим поле $\mathbb{F}_p[x]/(f(x))$.

В нём x — корень и своего м. м. $f(x)$, и, по теореме 2.4, бинома $x^{p^n-1} - 1$. По свойствам м. м. (утверждение 2.6) $x^{p^n-1} - 1$ делится на $f(x)$. \square

Пример 2.9. Возвращаемся к разложению бинома $x^{15} + 1 \in \mathbb{F}_2[x]$.

Поскольку $15 = 2^4 - 1$, все неприводимые многочлены 4-й степени над \mathbb{F}_2 будут делителями $x^{16} - x$, следовательно, $x^{15} + 1$. Таких многочленов три:

$$x^4 + x + 1, \quad x^4 + x^3 + 1 \quad \text{и} \quad x^4 + x^3 + x^2 + x + 1.$$

Таким образом,

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

Далее замечаем, что $3 = 2^2 - 1$, и поэтому все неприводимые многочлены 2-й степени над \mathbb{F}_2 будут делителями $x^4 - x$ и, следовательно, $x^3 + 1$. Но такой многочлен только один: $x^2 + x + 1$.

Поэтому окончательно получаем разложение $x^{15} + 1$ на неразложимые над \mathbb{F}_2 многочлены:

$$\begin{aligned} x^{15} + 1 &= (x + 1)(x^2 + x + 1) \times \\ &\times (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1). \end{aligned}$$

Теорема 2.7. *Любой неприводимый многочлен, делящий бином $x^{p^n} - x$, имеет степень, не выше n .*

Доказательство. Пусть f — неприводимый многочлен степени k , который является делителем бинома $x^{p^n} - x$. Тогда $\mathbb{F}_p[x]/(f) = F$ — поле, которое рассмотрим как векторное пространство над \mathbb{F}_p с базисом $\bar{1}, \bar{x}, \dots, \overline{x^{k-1}}$.

Поскольку бином $x^{p^n} - x$, делится на f , то

$$x^{p^n} - x = 0. \quad (*)$$

С другой стороны, любой элемент $\beta \in F$ выражается через базис:

$$\beta = \sum_{i=0}^{k-1} a_i \bar{x}^i.$$

Возводим обе части этого равенства в степень p^n . Из тождества Фробениуса (см. лемму 2.1 на с. 28) и $\alpha^{p^n} = \alpha$ для любого $\alpha \in F$ получим

$$\beta^{p^n} = \left(\sum_{i=0}^{k-1} a_i \bar{x}^i \right)^{p^n} = \sum_{i=0}^{k-1} a_i \bar{x}^i = \beta,$$

то есть β — корень (*).

Но у (*) не более p^n различных корней, а в построенном поле F имеется p^k элементов. Поэтому $p^n \geq p^k$ и $n \geq k$. \square

Корни неприводимого многочлена

Теорема 2.8 (о корнях неприводимого многочлена). Пусть $\beta \in \mathbb{F}_p^n$ — корень неприводимого многочлена $f(x) \in \mathbb{F}_p[x]$. Тогда $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$ все различны и исчерпывают список всех n его корней.

Доказательство. При $n = 1$, утверждение теоремы тривиально и далее считаем, что $n > 1$.

Из тождества Фробениуса следует, что

$$f(\beta) = 0 \Leftrightarrow (f(\beta))^p = 0 \Leftrightarrow f(\beta^p) = 0,$$

и $\beta, \beta^p, \dots, \beta^{p^{n-1}}$ — корни многочлена $f(x)$.

Покажем, что все указанные корни различны, и тогда (многочлен степени n имеет не более различных n корней) можно утверждать, что найдены все корни многочлена $f(x)$.

Предположим, что $\beta^{p^l} = \beta^{p^k}$, $0 \leq l < k \leq n - 1$, но тогда $\beta^{p^{k-l}} = 1$, а это значит, что при $n > 1$ среди корней $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$ находится $1 \in \mathbb{F}_p$. В свою очередь, это означает, что $f(x)$ делится на $x - 1$ (см. с. 31), т. е. многочлен $f(x)$ разложим. \square

Поэтому если известен какой-либо один корень неприводимого многочлена, все остальные можно получить последовательно возводя его в степени p .

Корни $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$ нормированного неприводимого многочлена $f(x)$ степени n называют *сопряжёнными*.

Следствие. Если многочлен $f(x) \in \mathbb{F}_p[x]$ степени n неприводим, то $\mathbb{F}_p[x]/(f(x))$ — его поле разложения, в котором он имеет корни $x, x^p, x^{p^2}, \dots, x^{p^{n-1}}$.

Если в поле $\mathbb{F}_p^k \cong \mathbb{F}_p[x]/(\varphi(x))$, $\deg \varphi(x) = k < n$ многочлен $f(x)$ имеет корень β , то $\varphi(x) \mid f(x)$. Поэтому многочлен $f(x)$ имеет своим полем разложением поле $\mathbb{F}_p[x]/(f(x))$. Далее применяем теорему 2.8.

Пример 2.10. 1. Найдём корни неприводимого над \mathbb{F}_2 многочлена

$$f(x) = x^4 + x^3 + 1.$$

Эти корни будут элементами поля $\mathbb{F}_2[x]/(f(x))$, один из них получаем немедленно — это x , а остальные 3 суть $x^2, x^4 = x^3 + 1$ и

$$\begin{aligned} x^8 &= x^6 + 1 = (x^5 + x^2) + 1 = x^4 + x + x^2 + 1 = \\ &= x^3 + 1 + x^2 + x + 1 = x^3 + x^2 + x. \end{aligned}$$

2. *Задача:* найти все корни многочлена

$$f(x) = x^4 + 2x^3 + x^2 + x + 1 \in \mathbb{F}_3[x]$$

в минимальном расширении поля \mathbb{F}_3 .

Перебирая элементы $\mathbb{F}_3 = \{0, 1, 2\}$, находим, что 1 — корень $f(x)$, поэтому многочлен $f(x)$ приводим:

$$x^4 + 2x^3 + x^2 + x + 1 = (x - 1)(x^3 + x + 2).$$

Далее находим, что 2 — корень частного $x^3 + x + 2$ и справедливо разложение

$$x^3 + x + 2 = (x - 2)(x^2 + 2x + 2).$$

Многочлен $\varphi(x) = x^2 + 2x + 2$ над \mathbb{F}_3 неприводим. Поэтому определяем поле его разложения $\mathbb{F}_3[x]/(\varphi(x))$, в котором $\varphi(x)$ имеет корни x и x^3 .

В этом поле $x^2 = -2x - 2 = x + 1$ и $x^3 = x(x + 1) = x^2 + x = 2x + 1$.

Ответ: поле $\mathbb{F}_3[x]/(x^2 + 2x + 2) = \mathbb{F}_3^2$ является минимальным полем характеристики 3, в котором многочлен $f(x) = x^4 + 2x^3 + x^2 + x + 1$ имеет корни. Они суть 1, 2, x и $2x + 1$.

Нахождение минимальных многочленов. Для нахождения м. м. $m_\beta(x)$ элемента $\beta \in \mathbb{F}_p[x]/(a(x))$ вычисляем сопряжённые элементы $\beta^p, \beta^{p^2}, \dots$, пока на некотором шаге d окажется, что

1) $\beta^{p^d} = \beta$, тогда

$$m_\beta(x) = (x - \beta) \cdot (x - \beta^p) \cdot \dots \cdot (x - \beta^{p^{d-1}}).$$

2) $\beta^{p^d} = x$, тогда $m_\beta(x)$ есть многочлен $a(x)$ после нормировки, как и для случая $\beta = x$.

Пример 2.11. Найдём минимальные многочлены для элементов $x^2 + x$ и $x + 1$ поля $\mathbb{F}_2[x]/(x^4 + x + 1)$.

В этом поле $x^4 = x + 1$.

1. $\beta = x^2 + x$. Вычисляем элементы, сопряжённые с β :

$$\beta^2 = (x^2 + x)^2 = x^4 + x^2 = x^2 + x + 1,$$

$$\begin{aligned} \beta^4 &= (x^2 + x + 1)^2 = x^4 + x^2 + 1 = x + 1 + x^2 + 1 = \\ &= x^2 + x = \beta. \end{aligned}$$

Таким образом $m_\beta(x)$ — квадратный многочлен и

$$m_\beta(x) = (x - \beta)(x - \beta^2) = x^2 + (\beta^2 + \beta)x + \beta^3.$$

Вычисляем коэффициенты многочлена:

$$\beta^2 + \beta = (x^2 + x + 1) + (x^2 + x) = 1,$$

$$\beta^3 = (x^2 + x + 1)(x^2 + x) = \dots = (x + 1) + x = 1,$$

и окончательно $m_\beta(x) = x^2 + x + 1^4$.

2. $\beta = x + 1$. Элементы, сопряжённые с β :

$$\beta^2 = x^2 + 1, \quad \beta^4 = x^4 + 1 = x + 1 + 1 = x,$$

поэтому $m_\beta(x) = x^4 + x + 1$.

Существование для всех n неприводимых многочленов над F_p и полей $GF(p^n)$. Символом $((n))$ обозначим число нормированных неприводимых многочленов степени n из $\mathbb{F}_p[x]$.

Лемма 2.3. $\sum_{d|n} d \cdot ((d)) = p^n$.

⁴⁾ Заметим, что в данном случае вычислений коэффициентов можно было не проводить, поскольку $x^2 + x + 1$ — единственный неприводимый над \mathbb{F}_2 многочлен 2-й степени.

Следствия. 1. *Существование неприводимых многочленов любой степени.* Простая оценка ($p \geq 2, n \geq 2$)

$$\begin{aligned} n \cdot ((n)) &= p^n - \sum_{k|n, k < n} k \cdot ((k)) \geq \\ &\geq p^n - p^{n-1} - \dots - p - 1 = p^n - \frac{p^n - 1}{p - 1} > 0. \end{aligned}$$

влечёт $((n)) > 0$, то есть для любых простого p и натурального n над полем \mathbb{F}_p существует хотя бы один неприводимый нормированный многочлен степени n .

2. *Для любого n существует поле $GF(p^n)$ как факторкольца по идеалу, образованному неприводимым многочленом.*

Приведём ещё одну формулу для $((n))$.

Функция Мёбиуса $\mu(n)$ определяется для всех $n \in \mathbb{N}$: $\mu(1) = 1$ и для $n > 1$ —

$$\mu(n) = \begin{cases} 1, & \text{если примарное разложение } n \text{ состоит} \\ & \text{из чётного числа различных простых;} \\ -1, & \text{если примарное разложение } n \text{ состоит} \\ & \text{из нечётного числа различных простых;} \\ 0, & \text{если } n \text{ не свободно от квадратов.} \end{cases}$$

Например, $\mu(p) = -1$, если p — простое, $\mu(6) = \mu(2 \cdot 3) = 1$, $\mu(4) = 0$, $\mu(30) = \mu(2 \cdot 3 \cdot 5) = -1$.

Теорема 2.9 (формула Гаусса).

$$((n)) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Например:

$$p = 2, ((4)) = \frac{1}{4} [\underbrace{\mu(1)}_{=1} \cdot 2^4 + \underbrace{\mu(2)}_{=-1} \cdot 2^2 + \underbrace{\mu(4)}_{=0} \cdot 2] = 3;$$

$$p = 2, ((5)) = \frac{1}{5} [\mu(1) \cdot 2^5 + \mu(5) \cdot 2] = \frac{1}{5} [32 - 2] = 6;$$

$$p = 3, ((6)) = \frac{1}{6} [\mu(1) \cdot 3^6 + \mu(2) \cdot 3^3 + \mu(3) \cdot 3^2 + \mu(6) \cdot 3] = 116.$$

2.5 Циклические подпространства колец вычетов

Идеалы в кольцах классов вычетов. Далее будем рассматривать кольцо многочленов $R = \mathbb{F}_p[x]/(f)$ по модулю главного идеала (f) *возможно приводимого* многочлена f над \mathbb{F}_p .

Если f неприводим, то R — поле, что уже рассмотрено. Но в любом случае R — векторное пространство над \mathbb{F}_p , совокупность всех многочленов степени меньшей $\deg f$.

Теорема 2.10. Пусть $f, \varphi \in \mathbb{F}_p[x]$, $\varphi \mid f$, а φ — неприводимый нормированный многочлен. Тогда

- 1) совокупность всех многочленов, кратных φ , образует идеал (φ) в кольце $R = \mathbb{F}_p[x]/(f)$;
- 2) φ — единственный в (φ) нормированный многочлен минимальной степени;
- 3) идеал (φ) — векторное подпространство в R размерности $\deg f - \deg \varphi$.

Доказательство. $u, v, \varphi \in \mathbb{F}_p[x]$, $k = \deg \varphi \leq \deg f$,
 $\varphi = a_0 + a_1x + \dots + a_{k-1}x^{k-1} + x^k$, $f = \psi\varphi$.

1. Проверим, что (φ) — идеал в кольце $\mathbb{F}_p[x]/(f)$.
 Во-первых,

$$\begin{cases} \bar{g} \in (\varphi) \\ \bar{h} \in \mathbb{F}_p[x]/(f), \bar{h} \subseteq \bar{g} \end{cases} \Leftrightarrow \begin{cases} \bar{g} = u\varphi \\ \bar{h} = v\varphi = vu\varphi \end{cases} \Rightarrow \\ \Rightarrow \bar{h} \in (\varphi).$$

И, во-вторых,

$$\bar{g}, \bar{h} \in (\varphi) \Leftrightarrow \begin{cases} \bar{g} = u\varphi \\ \bar{h} = v\varphi \end{cases} \Rightarrow \bar{g} + \bar{h} = (u+v)\varphi \in (\varphi).$$

2. Покажем, что в (φ) нет других, кроме

$$\varphi = a_0 + a_1x + \dots + a_{k-1}x^{k-1} + x^k$$

нормированных многочленов степени, меньшей $k = \deg \varphi$.

Пусть $g = b_0 + b_1x + \dots + x^m$. Тогда

$$\bar{g} \in (\varphi) \Leftrightarrow g = u\varphi \Rightarrow \deg g = m \geq \deg \varphi = k.$$

3. Без доказательства. □

Пример 2.12. Рассмотрим два многочлена над \mathbb{F}_2 : приводимый $f = x^4 - 1$ и его неприводимый делитель $\varphi = x + 1$.

В кольце $R = \mathbb{F}_2[x]/(x^4 - 1)$ все кратные φ многочлены имеют вид

$$(ax^2 + bx + c)(x + 1) = ax^3 + (a + b)x^2 + (b + c)x + c,$$

$a, b, c \in \{0, 1\}$ и образуют идеал в нём.

Приведём элементы этого идеала:

$a b c$	элементы (φ)
0 0 0	0
0 0 1	$x + 1$
0 1 0	$x^2 + x$
0 1 1	$x^2 + 1$
1 0 0	$x^3 + x^2$
1 0 1	$x^3 + x^2 + x + 1$
1 1 0	$x^3 + x$
1 1 1	$x^3 + 1$

Легко проверяем, что для элементов g и h этого идеала многочлены $g + h$ и $g \cdot h \pmod{(x^4 - 1)}$ также ему принадлежат. Также видим, что $\varphi = x + 1$ — единственный в R многочлен минимальной степени и, очевидно, идеал $(x + 1)$ есть векторное пространство размерности $\deg f - \deg \varphi = 4 - 1 = 3$.

Циклическое пространство.

Определение 2.3. Подпространство координатного линейного пространства F^n над полем F называется *циклическим*, если вместе с набором (a_0, \dots, a_{n-1}) оно содержит его циклический сдвиг вправо (то есть $(a_{n-1}, a_0, \dots, a_{n-2})$), а следовательно и все циклические сдвиги на произвольное число позиций влево и вправо).

Конкретно, в кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как векторное пространство имеется естественный базис $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$.

Циклический сдвиг координат в этом базисе равносильно умножению на \bar{x} :

$$\begin{aligned} & \overline{a_0 + a_1x + \dots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}} \cdot \bar{x} = \\ & = \overline{a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} + a_{n-1} \underbrace{x^n}_{=1}} = \\ & = \overline{a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1}}. \end{aligned}$$

Теорема 2.11. В кольце классов вычетов по модулю многочлена $x^n - 1$ подпространство является циклическим если и только если оно идеал.

Доказательство. Если подпространство I — идеал, то оно замкнуто относительно умножения на \bar{x} , а это умножение и есть циклический сдвиг. Следовательно, подпространство I циклическое.

Обратно, пусть I — циклическое подпространство кольца $\mathbb{F}_p/(x^n - 1)$ и $g \in I$. Тогда циклические сдвиги $g \cdot \bar{x}$, $g \cdot \bar{x}^2$, \dots также принадлежат I . Значит, $g \cdot \bar{f} \in I$ для любого многочлена f , поэтому I — идеал. \square

Число и степени неприводимых делителей бинома $x^n - 1$. Рассмотрим разложение бинома $x^n - 1 \in \mathbb{F}_p[x]$ в произведение неприводимых многочленов.

Поскольку в поле характеристики p справедливо $x^{kp} - 1 = (x^k - 1)^p$, то в случае $n = kp$ корнями бинома $x^n - 1$ будут все корни $x^k - 1$, но p -й кратности. Это в свою очередь приведёт к тому, что если неприводимый полином $f(x)$ делит бином $x^n - 1$, то его делит и $(f(x))^p$.

Поэтому далее будем считать, что $n \neq kp$ и поэтому бином $x^n - 1$ разлагается в произведение k неприводимых многочленов $f_1(x), \dots, f_k(x)$:

$$x^n - 1 = f_1(x) \cdot \dots \cdot f_k(x),$$

которые все различны. Пусть эти многочлены имеют степени d_1, \dots, d_k соответственно.

Легко видеть, что n его корней образуют циклическую подгруппу корней из 1 степени n в мультипликативной группе своего поля разложения. Если β — корень неприводимого многочлена $f(x)$ степени d , то $\beta^p, \beta^{p^2}, \dots, \beta^{p^{d-1}}$ — также его корни. Отсюда следует, что величины k и d_1, \dots, d_k можно найти, разбив элементы $\mathbb{Z}/n\mathbb{Z}$ на орбиты отображения $t \mapsto pt \pmod{n}$.

Пример 2.13. 1. Вернёмся к разложению бинома $x^{15} + 1$ над \mathbb{F}_2 . Относительно умножения на 2 вычеты по модулю 15 разбиваются на следующие орбиты:

$$\{0\}, \{1, 2, 4, 8\}, \{3, 6, 12, 9\}, \{5, 10\}, \\ \{7, 14, 13, 11\}$$

Поэтому $x^{15} + 1$ разлагается в произведение одного неприводимого многочлена степени 1, одного неприводимого многочлена степени 2 и трех неприводимых многочленов степени 4. Конкретно разложение было найдено ранее (см. с. 53).

2. Рассмотрим разложение многочлена $x^{23} - 1$ над \mathbb{F}_2 . Относительно умножения на 2 вычеты по модулю 23 разбиваются на три орбиты:

$$\{0\}, \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\},$$

$$\{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

Поэтому $x^{23} - 1$ разлагается в произведение одного линейного многочлена и двух неприводимых многочленов 11-й степени.

Можно показать, что поле разложения бинома $x^n - 1 \in \mathbb{F}_p[x]$ при взаимно простых n и p есть \mathbb{F}_p^m , где m — максимальная степень неприводимого многочлена, его делящего: $m = \max\{d_1, \dots, d_k\}$ ⁵⁾. Это следует из того, что значение n как порядок группы корней из 1, должно делить порядок мультипликативной группы поля разложения.

2.6 Задачи

2.1. Найти

- а) $3^{-1} \pmod{5}$;
- б) $9^{-1} \pmod{14}$;
- в) $1^{-1} \pmod{118}$;
- г) $3 \cdot 4^{-1} \pmod{7}$;
- д) $(-3)^{-1} \pmod{7}$;
- е) $6^{-2} \pmod{11}$;
- ж) $3^{-3} \pmod{8}$.

2.2. Решите сравнение

- а) $7x = 11 \pmod{25}$;

⁵⁾ нетрудно видеть, что m есть число элементов в орбите, порождаемой вычетом 1.

- б) $9x = 3 \pmod{10}$;
- в) $6x + 2 = 3 \pmod{7}$;
- г) $6x + 2 = 3 \pmod{9}$;
- д) $6x + 2 = 4 \pmod{9}$;
- е) $6x + 1 = 4 \pmod{9}$.

2.3. В поле $F = \mathbb{F}_2^2$ вычислить произведение

$$P = \prod_{i=1}^3 (x - \beta_i),$$

где $\beta_1, \beta_2, \beta_3$ — все ненулевые элементы поля.

2.4. Найти сумму ненулевых элементов поля \mathbb{F}_p .

2.5 (Теорема Вильсона). Доказать, что

$$(p - 1)! \equiv_p -1, \quad p \text{ — простое.}$$

2.6. Построить поле из 4-х элементов.

2.7. В кольце $\mathbb{Z}_2[x]$ найти

$$\text{НОД} (x^5 + x^2 + x + 1, x^3 + x^2 + x + 1).$$

2.8. В расширении F простого поля \mathbb{F}_2 , построенного с помощью образующего полинома

$$a(x) = x^3 + x + 1$$

- 1) построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов;
- 2) построить таблицу умножения элементов;
- 3) для каждого элемента поля указать обратные;

- 4) найти порождающие элементы поля;
- 5) найти минимальные многочлены всех элементов поля.

2.9. Перечислить все подполя поля $GF(2^{30})$.

2.10. Многочлен $f(x) = x^5 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ разложить на неприводимые множители.

2.11. Многочлен $f(x) = x^3 + 2x^2 + 4x + 1 \in \mathbb{F}_5[x]$ разложить на неприводимые множители.

2.12. Многочлен $f(x) = x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$ разложить на неприводимые множители.

2.13. Многочлен

$$f(x) = x^4 + 3x^3 + 2x^2 + x + 4 \in \mathbb{F}_5[x]$$

разложить на неприводимые множители.

2.14. Разложить на неприводимые множители все нормированные многочлены 3-й степени из $\mathbb{F}_2[x]$.

2.15. Найти все нормированные неприводимые многочлены 2-й степени над $GF(3)$.

2.16. Найти все нормированные многочлены третьей степени, неприводимые над $GF(3)$.

2.17. Определить, является ли:

- 1) Многочлен $a(x) = x^2 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?

2) Элемент $4x^2 + 2$ — корнем $a(x)$ в факторкольце/поле $\mathbb{F}_5[x]/(x^3 + 2x + 4)$?

2.18. 1) Проверить, что факторкольцо $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ является полем.

2) В F найти обратный элемент к $1 - x$.

2.19. Найти порядок элемента $\beta = x + x^2$ в мультипликативной группе

1) поля $F_1 = \mathbb{F}_2[x]/(x^4 + x + 1)$;

2) поля $F_2 = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

2.20. Определить, является ли неприводимый многочлен $f(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$ примитивным?

2.21. Найти количество нормированных неприводимых многочленов

1) степени 7 над полем \mathbb{F}_2 ;

2) степени 6 над полем \mathbb{F}_5 .

2.22. Для поля $F = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов.

С её помощью вычислить выражение

$$S = \frac{1}{2x + 1} - \frac{2(2x)^7}{(x)^9(x + 2)}.$$

2.23. Для поля $F = \mathbb{F}_3[x]/(x^2 + 1) \cong \mathbb{F}_3^2$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

2.24. В факторкольце $R = \mathbb{F}_3[x]/(x^4 + 1)$ найти все элементы главного идеала $(x^2 + x + 2)$.

2.25. В поле $F = \mathbb{F}_5[x]/(x^2 + 3x + 3)$ найти обратную к матрице

$$M = \begin{pmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{pmatrix}.$$

2.26. Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

2.27. Найти поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители и найти в нём все корни данного многочлена.

2.28. Найти м. м. для всех элементов β поля $F = \mathbb{F}_2[x]/(x^4 + x + 1)$.

2.29. Найти минимальный многочлен элемента α^3 , где α — примитивный элемент поля

$$F = \mathbb{F}_5[x]/(x^2 + x + 2).$$

2.30. Примитивен ли элемент x в полях

$$1) \mathbb{F}_2[x]/(x^3 + x + 1) = F_1?$$

$$2) \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1) = F_2?$$

2.31. Найти корни многочлена

$$f(x) = x^3 + 3x^2 + 4x + 4 \in \mathbb{F}_5[x].$$

2.32. Является ли многочлен

$$f(x) = x^2 + x + 2 \in \mathbb{F}_5[x]$$

примитивным?

2.33. Для бинорма $x^{40} - 1 \in \mathbb{F}_5[x]$ определить количество и степени неприводимых сомножителей. В каком минимальном поле расширения $\mathbb{F}_5[x]$ данный бинорм раскладывается на линейные множители?

2.34. Найти корни $f(x) = x^2 + x + 1 = 0$, если

(1) $f(x) \in \mathbb{F}_2[x]$; (2) $f(x) \in \mathbb{F}_3[x]$; (3) $f(x) \in \mathbb{F}_5[x]$.

2.35. Решить уравнение

$$f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0, \text{ где } f(x) \in \mathbb{F}_5[x].$$

2.36. Решить уравнение

$$f(x) = x^8 + x^4 + x^2 + x + 1 = 0, \text{ где } f(x) \in \mathbb{F}_2[x].$$

2.37. Найти корень многочлена

$$f(x) = x^4 + 2x + 2 \in \mathbb{F}_3[x].$$

2.38. Решить уравнение $f(x) = x^5 + x^2 + 1 = 0$ для $f(x) \in \mathbb{F}_2[x]$.

Глава 3

Коды, исправляющие ошибки

3.1 Блочное кодирование: основные понятия

Задача помехоустойчивого кодирования. По каналу с шумом проходит поток *битовой* информации, вследствие чего возникают ошибки (вариант: хранимая информация искажается).

- *Модель ошибок:* биты случайно, независимо и с равными вероятностями могут оказаться инвертированными, вставки/выпадения битов нет (имеем т. н. *двоичный симметричный канал*).
- *Задача:* обеспечить автоматическое исправление ошибок.

Подход к решению (один из возможных!):

- 1) входной поток информации разбить на *сообщения* — непересекающиеся блоки фиксированной длины k ;
- 2) каждый блок *кодировать* (модифицировать) —
 - а) независимо от других — *блочное кодирование*;

б) в зависимости от предыдущих — *свёрточное* или *потокное кодирование* (турбо-коды).

Далее рассматриваем только *блочное кодирование*:

- задан полный набор *сообщений* S_1, \dots, S_{2^k} , длины k каждое, которые нужно передать по каналу связи с шумом;
- для обеспечения помехозащищённости вместо этих сообщений передают *словесные коды*, каждое длины $n = k + t$, $t > 0$.
- *код* — инъективное отображение $\varphi : B^k \rightarrow B^n$.
- множество C *словесных слов* — область значений $Im \varphi$ кода. Часто C обозначает и сам код.
- $R = k/n$ — *скорость*, t/n — *избыточность* кода.

Чем меньше избыточность и чем больше число ошибок, которые может исправить код, тем он лучше. Однако эти требования противоречивы и одно достигается за счёт другого.

Кодовое расстояние.

Определение 3.1. Минимальное хемингово расстояние между парами слова кода C называется его *словесным расстоянием*, символически $d(C)$ или просто d .

Ясно, что код C может исправить не менее r ошибок, если шары радиусов r с центрами в словесных кодах непересекаются. Действительно, если в векторе $\tilde{\alpha}$

искажено не более r бит, то набор останется в шаре $S_r(\tilde{\alpha})$ и искомое кодовое слово — центр шара, ближайший к полученному набору.

Следовательно, у кода, исправляющего r ошибок, кодовое расстояние d должно быть не менее $2r + 1$.

Определение кодового расстояния произвольного кода C крайне трудоёмкая задача: показано, что она NP -трудна. В общем случае для нахождения $d(C)$ требуется перебрать все $(2^k(2^k - 1))/2$ пар кодовых слов, что практически невозможно уже начиная с $k = 50$. Поэтому важной задачей является построение кодов с заданным кодовым расстоянием.

Блочное кодирование и декодирование

Блочное кодирование — взаимно-однозначное преобразование сообщений в кодовые слова большей длины.

Декодирование — восстановление сообщения по принятому, возможно искажённому, слову.

Пример 3.1. Информация разбивается на блоки по $k = 1$ бит, то есть передаются два сообщения: $S_0 = 0$ и $S_1 = 1$.

Код-повторение $a \mapsto \underbrace{a \dots a}_{2r+1 \text{ раз}}$, очевидно, исправит r ошибок. Простейший вариант — утраивание: $0 \mapsto 000$, $1 \mapsto 111$. Ясно, однако, что такое кодирование крайне неэффективно.

Этот и другие *тривиальные n -коды* с $k = 0$, или $n = k$ не рассматриваем.

Кодирование. Все векторы далее мы будем считать вектор-столбцами; часто используют векторы-строки — будьте внимательны!

Обозначения:

- сообщение — вектор

$$\mathbf{u} = \begin{bmatrix} u_1 \\ \dots \\ u_k \end{bmatrix} \in \{0, 1\}^k;$$

- кодовое слово — вектор $\mathbf{v} \in \{0, 1\}^n$;
- множество всех кодовых слов — (n, k) -код, или, с кодовым расстоянием — (n, k, d) -код¹⁾.

Блочное кодирование всегда можно осуществить с использованием таблицы размера $2^k \times n$. Однако такое «табличное» кодирование весьма неэффективно: значения n и k могут достигать сотен тысяч.

При передаче по каналу с шумом кодовое слово \mathbf{v} превращается в принятое слово \mathbf{w} той же длины n ,

$$\mathbf{v} \rightarrow \mathbf{w} = \mathbf{v} + \mathbf{e},$$

где $\mathbf{e} \in \{0, 1\}^n$ — вектор ошибок, содержащий 1 в тех и только тех битах, в которых произошли ошибки.

Декодирование (n, k, d) -кода обычно значительно сложнее кодирования. Оно основано на разбиении единичного куба B^n на k областей, содержащих шары радиуса $r = \lfloor (d-1)/2 \rfloor$ с центрами в кодовых словах и предположении, что произошло $\leq r$ ошибок.

¹⁾ если надо указать, что код двоичный, пишут $(n, k, d)_2$ -код

Декодирование блокового (n, k, d) -кода проводится в два этапа:

1-й этап: Определение кодового слова $\hat{\mathbf{v}}$ как ближайшего в метрике Хэмминга слову \mathbf{w} , т. е. нахождение центра соответствующего шара (*декодирование в ближайшее кодовое слово* или *по максимуму правдоподобия*). Если произошло не более r ошибок, то $\hat{\mathbf{v}} = \mathbf{v}$.

2-й этап: Удаление избыточности и восстановление исходного сообщения по найденному кодовому слову.

Ясно, что при выполнении 1-го этапа в общем случае надо перебрать все 2^n строк в $(2^n \times k)$ -таблице кодовых слов. Поэтому декодирование блокового (n, k) -кода *общего вида* является крайне ресурсоёмким процессом, и использование таких кодов возможно лишь при небольших значениях n и k .

Однако, приняв дополнительные ограничения на множество кодовых слов, можно перейти от *экспоненциальных* требований по памяти и по сложности алгоритмов кодирования/декодирования к *линейным*. Эти ограничения приводят к использованию блоковых кодов специального вида: *групповых*, а из групповых — *циклических*.

Плотная упаковка шаров в единичный куб. Чтобы построить код минимальной избыточности, исправляющий данное количество r ошибок, нужно вложить в единичный куб B^n максимально возможное

число непересекающихся шаров радиуса r — это задача плотной упаковки.

Вопрос: При каких n и r в куб B^n можно уложить непересекающиеся шары радиуса r «плотно», «без зазоров»?

Ответ: Такое удаётся только в двух нетривиальных²⁾ случаях, когда получаются совершенные или экстремальные коды:

- 1) $n = 2^m - 1$, $r = 1$ — коды Хэмминга; у них $k = 2^m - 1 - m$;
- 2) $n = 23$, $r = 3$ — код Голея; к нему $m = 11$ и $k = 12$.

Теорема 3.1 (Хэмминга). При $2r < n$ максимальное число t кодовых слов находится в пределах

$$\frac{2^n}{C_n^0 + C_n^1 + \dots + C_n^{2r}} \leq t \leq \frac{2^n}{\underbrace{C_n^0 + C_n^1 + \dots + C_n^r}_{\text{граница Хэмминга}}}.$$

Доказательство. Для получения верхней оценки числа непересекающихся шаров радиуса r разделим объём булева куба на объём шара. Шар радиуса r содержит: центр и все точки с одной, двумя, ..., r изменёнными координатами.

Для оценки снизу построим негрупповой код:

- 1) берём произвольную точку B^n и строим вокруг неё шар радиуса $2r$;

²⁾ для групповых кодов, см. ниже

- 2) берем произвольную точку вне построенного шара и строим вокруг неё шар радиуса $2r$;
- 3) и т. д., каждая новая точка выбирается вне построенных шаров.

В результате шары радиуса $2r$, возможно, пересекаются, но каждый шар занимает $v = C_n^0 + C_n^1 + \dots + C_n^{2r}$ точек, поэтому всех шаров не менее $2^n/v$. Однако шары радиуса r с центрами в выбранных точках не пересекаются. \square

Построим конкретный исправляющий одну ошибку код Хэмминга длины $n = 2^m - 1$ и покажем, что для него граница Хэмминга достигается.

Рассмотрим таблицу, приписав справа к единичной матрице порядка $k = 2^m - 1 - m$ все бинарные наборы длины m , содержащие не менее двух единиц:

$$k = 2^m - (m+1) \left\{ \begin{array}{ll} 100 \dots 000 & 1100 \dots 000 \\ 010 \dots 000 & 1010 \dots 000 \\ 001 \dots 000 & 1001 \dots 000 \\ & \dots \\ & \dots \\ 000 \dots 001 & 1111 \dots 111 \end{array} \right.$$

$\underbrace{\hspace{10em}}$
 $k = 2^m - (m+1)$

$\underbrace{\hspace{10em}}$
 m

Просуммировав все (включая пустую) совокупности строк таблицы, получим $|C| = 2^k$ различных кодовых слов, и

$$2^k = 2^{2^m - m - 1} = \frac{2^{2^m - 1}}{2^m} = \frac{2^n}{\underbrace{1 + n}_{\substack{\text{объём шара} \\ \text{радиуса 1}}}}$$

Найдём кодовое расстояние построенного кода:

- в каждой строке таблицы — не менее трёх единиц;
- если сложить

две строки — в левой части будет две единицы, а в правой — хотя бы одна, не менее трёх строк — в левой части будет не менее трёх единиц.

Отсюда следует, что всегда $\rho(\tilde{\alpha}, \tilde{\beta}) \geq 3$ и шары единичного радиуса с центрами в полученных наборах не пересекаются.

Пример 3.2. Для $m = 3$ ($n = 2^3 - 1 = 7$) составим таблицу

1	0	0	0	1	1	0
0	1	0	0	1	0	1
0	0	1	0	0	1	1
0	0	0	1	1	1	1

Складывая по mod 2 все, включая пустую, совокупности строк полученной таблицы, получаем $2^4 = 16$ слов (7, 4, 3)-кода Хэмминга.

Код Голея — (23, 12, 7)-код. М. Голей обнаружил, что

$$\underbrace{C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3}_{\text{объём шара радиуса 3}} = 2^{11}.$$

Это позволило предположить, что существует содержащий $2^{23}/2^{11} = 2^{12} = 4096$ кодовых слов совершенный (23, 12, 7)-код, исправляющий до 3-х ошибок, и М. Голей в своей статье указал такой код.

Доказано, что других пар (n, r) , удовлетворяющих условию $2^n / (C_n^0 + \dots + C_n^r)$ — целое, кроме кодов Хэмминга и тривиальных, не существует.

3.2 Линейные коды

Линейные коды: определение, свойства. Большая часть теории блокового кодирования построена на *линейных* кодах, позволяющих в ряде случаев реализовывать алгоритмы кодирования/декодирования, приемлемые по эффективности. В двоичном случае их называют *групповыми*, т. к. они образуют группу относительно операции «сумма по mod 2» (+).

Легко видеть, что устойчивая относительно операции суммы по mod 2 совокупность кодовых слов C образует (коммутативную) группу. Действительно, свойствами операции + обеспечивается ассоциативность, существование нуля ($\tilde{\alpha} + \tilde{\alpha} = \tilde{0} = (0, \dots, 0)$) и противоположных элементов ($-\tilde{\alpha} = \tilde{\alpha}$) кода C .

Легко видеть, что кодовое расстояние d группового кода равно

$$d = \min_{\tilde{\alpha} \neq \tilde{\beta}} \rho(\tilde{\alpha}, \tilde{\beta}) = \min_{\tilde{\gamma} \neq \tilde{0}} \|\tilde{\gamma}\|,$$

где $\tilde{\alpha}$, $\tilde{\beta}$ и $\tilde{\gamma}$ — кодовые слова из C .

Действительно, для произвольных кодовых слов $\tilde{\alpha}$ и $\tilde{\beta}$ всегда существует их сумма — кодовое слово $\tilde{\gamma}$:

$$\rho(\tilde{\alpha}, \tilde{\beta}) = \|\tilde{\alpha} + \tilde{\beta}\| = \|\tilde{\gamma}\|,$$

причем $\tilde{\gamma} \neq \tilde{0}$ при $\tilde{\alpha} \neq \tilde{\beta}$.

Отсюда получаем оценку $\min_{\tilde{\alpha} \neq \tilde{\beta}} \rho(\tilde{\alpha}, \tilde{\beta}) \geq \min_{\tilde{\gamma} \neq \tilde{0}} \|\tilde{\gamma}\|$, которая достигается, например, при $\tilde{\beta} = \tilde{0}$.

Поэтому для вычисления кодового расстояния группового кода нужно перебрать $2^k - 1$ кодовых слов (экспоненциальная сложность).

Определение 3.2. Блочный (n, k) -код называется *линейным*, если он образует векторное подпространство размерности k координатного пространства B^n .

Это означает, что в *линейном* коде C :

- 1) сумма любых кодовых слов — кодовое слово, то есть это *групповой* код;
- 2) кодовое расстояние $d(C) = \min_{\tilde{\gamma} \in C \setminus \{\tilde{0}\}} \|\tilde{\gamma}\|$;
- 3) существует базис $\{\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_{k-1}\}$ из k векторов $\mathbf{g}_i \in B^n$, $i = 0, \dots, k-1$, поэтому любой вектор $\mathbf{v} \in C$ может быть представлен как

$$\mathbf{v} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i, \quad u_i \in \{0, 1\}.$$

- 4) значение $k < n$, вообще говоря, произвольно.

Порождающая матрица. Систематическое кодирование Составим из векторов базиса кода матрицу $G = [\mathbf{g}_0 \mathbf{g}_1 \dots \mathbf{g}_{k-1}]$ размера $n \times k$. Её называют *порождающей матрицей* линейного кода C и для неё

$$\mathbf{v} = G\mathbf{u}.$$

Ясно, что все кодовые слова суть линейные комбинации столбцов порождающей матрицы G , а сама она определена с точностью до *элементарных преобразований столбцов* (их перестановкам и сложению по $\text{mod } 2$ данного столбца с любым другим). Данные преобразования эквивалентны переходу к другому базису *этого же* кода.

Пусть линейный код задан порождающей матрицей $G_{n,k}$. Из неё с помощью элементарных преобразований столбцов может быть получена матрица \tilde{G} , у которой *первые* k строк образуют единичную подматрицу I_k . Тогда при кодировании $\mathbf{v} = \tilde{G}\mathbf{u}$ первые k бит сообщения перейдут в первые биты кодового слова.

Кодирование, при котором информационные биты переходят в фиксированные позиции кодового слова, называют *систематическим* или *разделимым*. Остальные (избыточные) биты сообщения называют *проверочными*. Любой линейный код можно преобразовать в эквивалентный ему систематический.

Систематическое кодирование делает тривиальным 2-й этап декодирования: исходное сообщение есть результат удаления из кодового слова проверочных бит.

Пример 3.2 (продолжение — (7, 4)-код Хэмминга).

Ранее была получена таблица, сложением различных групп строк которой получают все кодовые слова данного кода Хэмминга. Порождающая матрица кода получается транспонированием этой таблицы:

$$G_{7 \times 4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \begin{array}{l} \text{— порождающая матрица} \\ \text{в систематической форме:} \\ \text{при кодировании исходные} \\ \text{сообщения помещаются в} \\ \text{первые 4 бита кодового слова} \end{array}$$

Историческая справка. Первой ЭВМ, в которой использовался код Хэмминга, была IBM 7030, построенная в 1960 г., через 10 лет после появления кода Хэмминга. До этого применялся лишь простейший способ повышения надежности — *проверка на чётность*.

Ортогональное дополнение к коду и проверочная матрица. Итак, линейный код C есть k -мерное подпространство n -мерного линейного пространства $\{0, 1\}^n = B^n$. Элементы B^n , ортогональные ко всем кодовым словам C , образуют *ортогональное подпространство* C^\perp :

$$\forall \mathbf{v} \in C \quad \forall \mathbf{w} \in C^\perp : \mathbf{v}^T \times \mathbf{w} = 0.$$

Замечания:

- $\dim B^n = n = \underbrace{\dim C}_k + \underbrace{\dim C^\perp}_{n-k=m}$;
- B^n — не есть прямая сумма подпространств C и C^\perp : произвольный вектор из B^n может либо не разлагаться, либо разлагаться неоднозначно в сумму векторов из C и C^\perp .

Причиной этих «старанностей» является то, что из ортогональности системы векторов над B^n не следует их линейной независимости, как это имеет место в евклидовом пространстве.

Пусть $\{\mathbf{h}_0, \dots, \mathbf{h}_{m-1}\}$ — базис C^\perp , \mathbf{h}_i — векторы-столбцы из B^n , $i = 0, \dots, m-1$. Тогда матрица

$$H_{m \times n} = \begin{bmatrix} \mathbf{h}_0^T \\ \mathbf{h}_1^T \\ \vdots \\ \mathbf{h}_{m-1}^T \end{bmatrix}$$

называется *проверочной матрицей* кода C .

Ясно, что

- $\forall \mathbf{v} \in C: H\mathbf{v} = \mathbf{0}$ — нулевой m -мерный вектор;
- $HG = O_{m \times k}$ — нулевая матрица;
- проверочная матрица определена с точностью до элементарных преобразований *строк*.

Пусть I_k и I_m — единичные матрицы порядков k и m соответственно. Тогда если порождающая матрица имеет вид

$$G = \begin{bmatrix} I_k \\ P_{m \times k} \end{bmatrix},$$

то матрица $H = [P_{m \times k} \ I_m]$ будет проверочной. Действительно, в этом случае

$$H\mathbf{v} = HG\mathbf{u} = [P \ I] \times \begin{bmatrix} I \\ P \end{bmatrix} \mathbf{u} = (P + P)\mathbf{u} = \mathbf{0}.$$

Проверочную матрицу называют также *матрицей проверки на чётность*, а строки — *правилами проверки на чётность*.

Пример 3.2 (продолжение — $(7, 4)$ -код Хэмминга). Для построенной порождающей матрицы $G_{7 \times 4}$ проверочной будет

$$H_{3 \times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Легко видеть, что столбцами проверочной матрицы кода Хэмминга являются все ненулевые векторы длины m (в нашем примере $m = 3$).

Задание линейного кода. Пример кодирования. Резюмируем: линейный код C для сообщений длины k имеет длину $n = k + m$, m — число избыточных (при систематическом кодировании — проверочных) символов, и задаётся либо порождающей матрицей $H_{n \times k}$, либо проверочной матрицей $G_{m \times n}$.

Эти матрицы определены с точностью до элементарных преобразований столбцов и строк соответственно, что отвечает выбору различных базисов в пространствах C и C^\perp . Однако фиксирование позиций информационных бит при систематическом кодировании задаёт H и G однозначно.

Увеличение m ведёт к увеличению кодового расстояния d (как конкретно — очень трудный вопрос) и, следовательно, к увеличению количества ошибок, которые может исправить код.

Пример 3.3 (кодирования блоковым линейным кодом). Пусть линейный $(6, 3)$ -код задан порождающей матрицей

$$G_{6 \times 3} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Требуется:

- 1) с использованием данного кода осуществить несистематическое и систематическое кодирование векторов $\mathbf{u}_1 = [0 \ 1 \ 1]^T$ и $\mathbf{u}_2 = [1 \ 0 \ 1]^T$;
- 2) построить проверочную матрицу H ;
- 3) определить кодовое расстояние d данного кода.

1. *Несистематическое кодирование* находим непосредственно:

$$[\mathbf{v}_1^n \ \mathbf{v}_2^n] = G \times [\mathbf{u}_1 \ \mathbf{u}_2] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Для *систематического кодирования* с помощью элементарных преобразований столбцов выделим в матрице G единичную подматрицу порядка 3 (над стрелкой указано проводимое преобразование):

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{(1)+(2) \mapsto (1)} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \tilde{G}.$$

В полученной матрице в строках 3, 5 и 1 стоит единичная подматрица. Это приведёт к тому, что биты сообщения последовательно перейдут в 3, 5 и 1-й биты кодового слова.

Найдём систематическое кодирование $\mathbf{u}_1, \mathbf{u}_2$:

$$[\mathbf{v}_1 \ \mathbf{v}_2] = \tilde{G} \times [\mathbf{u}_1 \ \mathbf{u}_2] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

2. Для построения проверочной матрицы H сначала формируем матрицу $P_{3 \times 3}$ из строк \tilde{G} , отличных от строк единичной подматрицы:

$$P_{3 \times 3} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Далее нужно

- последовательно разместить столбцы P соответственно в 3, 5 и 1-м столбцах H ,

- остальные 2, 4 и 6-й столбцы H должны образовывать единичную подматрицу.

В итоге получим проверочную матрицу

$$H_{3 \times 6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Предлагается самостоятельно проверить, что $HG = H\tilde{G} = \mathbf{0}$ — нулевая (3×3) -матрица. и удостовериться, что в результате как систематического, так и несистематического кодирования были действительно найдены кодовые слова, перемножая H последовательно на \mathbf{v}_1^n , \mathbf{v}_2^n , \mathbf{v}_1 , \mathbf{v}_2 и получая нулевые векторы.

3. Найдем кодовое расстояние d . Для этого закодируем все $2^3 = 8$ сообщений и найдем минимальный ненулевой хэммингов вес кодового слова:

$$\begin{aligned} C &= [\mathbf{v}_1 \dots \mathbf{v}_8] = \tilde{G} \times [\mathbf{u}_1 \dots \mathbf{u}_8] = \\ &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \end{aligned}$$

$$\begin{array}{l}
 \mathbf{u}_1, \dots, \mathbf{u}_8 \text{ — все } 8 \\
 \text{возможных сообщений,} \\
 \mathbf{v}_1, \dots, \mathbf{v}_8 \text{ — все } 8 \\
 \text{возможных кодовых слов.} \\
 \text{Оказалось } d = 3.
 \end{array}
 =
 \begin{bmatrix}
 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1
 \end{bmatrix}.$$

3.3 Синдромное декодирование линейных кодов

Синдром

Определение 3.3. Синдромом слова $\mathbf{w} \in \{0, 1\}^n$, принятого при передаче сообщения, закодированного линейным (n, k) -кодом и, возможно, содержащего ошибки, назовём m -вектор $\mathbf{s} = H\mathbf{w}$, где H — проверочная матрица кода, $m = n - k$.

Свойства синдрома:

- $\mathbf{s} = \mathbf{0} \Leftrightarrow \mathbf{w}$ — кодовое слово, то ошибок нет.
Точнее, $\mathbf{s} = \mathbf{0}$ означает отсутствие *ошибок определённого типа*, а не их отсутствие вообще; это замечание относится и к декодированию всех рассматриваемых здесь и далее кодов.
- $\mathbf{s} = H\mathbf{w} = H(\mathbf{v} + \mathbf{e}) = \underbrace{H\mathbf{v}}_{=0} + H\mathbf{e} = H\mathbf{e}$.

Отсюда следует, что вектор ошибок \mathbf{e} удовлетворяет неоднородной недоопределённой СЛАУ

$$H\mathbf{e} = \mathbf{s}, \quad (*)$$

а кодовые слова являются решениями соответствующей однородной системы

$$H\mathbf{v} = \mathbf{0}.$$

Таким образом, вектор \mathbf{e} может быть представлен как частное решение $\hat{\mathbf{e}}$ неоднородной системы (*) и общее решение $\mathbf{v} = G\mathbf{u}$ соответствующей однородной —

$$\mathbf{e} = \hat{\mathbf{e}} + G\mathbf{u}.$$

Определение ошибок по синдрому. Поскольку и принятый вектор \mathbf{w} , и соответствующий ему вектор ошибок \mathbf{e} имеют одинаковые синдромы, можно попытаться восстановить неизвестный вектор \mathbf{e} , используя тот факт, что он является решением системы (*).

Для этого нужно составить *словарь синдромов* — таблицу, строки которой соответствуют всем возможным синдромам $\mathbf{s}_1, \dots, \mathbf{s}_{2^m}$, а каждая строка содержит *наиболее вероятный вектор ошибок*, данному синдрому соответствующий. Этот вектор должен иметь наименьший вес среди возможных решений системы (*) для данного \mathbf{s} , и его называют *лидером* класса векторов ошибок, имеющих общий синдром \mathbf{s} . Если таких векторов минимального веса несколько, то в качестве лидера может быть выбран любой из них.

Таким образом, данный метод потребует хранения проверочной матрицы размера $m \times n$, словаря синдромов размера $2^m \times n$, но не требует нахождения векторов ошибок минимального веса (они уже найдены на этапе проектирования декодирующего устройства).

Однако в любом случае алгоритм декодирования остаётся экспоненциально трудоёмким и по памяти, и по числу операций.

Декодирование кода Хэмминга. В случае кода Хэмминга декодирование можно существенно упростить. Особенностью проверочной матрицы $H_{m \times n}$ кода Хэмминга является то, что её столбцы представляют собой двоичные коды чисел от 1 до $n = 2^m - 1$.

Например, в *Примере 3.2* получена матрица

$$H_{3 \times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Хэмминг предложил использовать коды, у которых расположение столбцов проверочной матрицы H было такое, чтобы синдром являлся двоичным представлением позиции ошибки в принятом сообщении.

Для этого столбцы H должны быть двоичными представлениями чисел от 1 до $2^m - 1$ последовательно. Тогда любой синдром есть соответствующий столбец H , то есть двоичное представление своего номера = позиция ошибки.

Заметим, что единичную подматрицу такой матрицы будут образовывать столбцы 1, 2, ..., 2^{m-1} с номерами, являющимися степенью 2.

Пример 3.4. Для рассматриваемого (7, 4)-кода Хэмминга получаем матрицу

$$\tilde{H}_{3 \times 7} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Тогда порождающая матрица есть

$$G_{7 \times 4} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Она помещает сообщение последовательно в 3, 5, 6 и 7-ю позиции кодового слова, а остальные биты являются проверочными.

Закодируем этим кодом сообщение $\mathbf{u} = [0\ 1\ 0\ 1]^T$:

$$\mathbf{v} = G\mathbf{u} = [0\ 1\ 0\ 0\ 1\ 0\ 1]^T.$$

Пусть при передаче ошибка произошла в 5-м бите, то есть получено слово $\mathbf{w} = [0\ 1\ 0\ 0\ \underline{0}\ 0\ 1]^T$. Тогда синдром $\mathbf{s} = \tilde{H}\mathbf{w} = [1\ 0\ 1]^T$ указывает позицию ошибки.

3.4 Циклические коды

Полиномиальное представление слов. Установим изоморфное соответствие бинарных векторов и их представлениями полиномами из $\mathbb{F}_2[x]$:

$$\begin{aligned}
 \mathbf{u} &= [u_0 \ u_1 \ \dots \ u_{k-1}]^T \leftrightarrow \\
 &\leftrightarrow u(x) = u_0 + u_1x + \dots + u_{k-1}x^{k-1}, \\
 \mathbf{v} &= [v_0 \ v_1 \ \dots \ v_{n-1}]^T \leftrightarrow \\
 &\leftrightarrow v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}.
 \end{aligned}$$

Определение и построение циклических кодов

Определение 3.4. Код называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов своих кодовых слов.

Было показано, что в кольце $R = \mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как n -мерное циклическое векторное пространство над полем \mathbb{F}_p , имеется базис $\{1, x, \dots, x^{n-1}\}$ и циклический сдвиг координат в этом базисе осуществляется умножением на x . Подпространство I кольца этого кольца останется циклическим если и только если I — идеал R . Поскольку R — КГИ, то любой идеал в нём порождается некоторым полиномом.

Поэтому построить циклический (n, k) -код длины можно следующим образом³⁾.

1. Задаёмся нечётным (чтобы обеспечить взаимную простоту с $p = 2$) значением n и выбираем любой делитель $g(x)$ бинорма $x^n - 1$.

Многочлен $g(x)$ называют *порождающим* или *образующим*; $\deg g(x) = m$, $k = n - m$.

³⁾ Избыточный циклический код — англ. CRC, *Cyclic Redundancy Code*.

2. Идеал $(g(x))$ кольца $R = \mathbb{F}_p[x]/(x^n - 1)$, образующий циклическое векторное подпространство в R , состоит из всех многочленов вида $f(x) \cdot g(x)$, $\deg f(x) \leq k$.

Коэффициенты многочленов из этого идеала будут кодовыми словами. При удачном выборе порождающего полинома получается код с приемлемым значением d .

Итак, *циклический код полностью определяется своим порождающим многочленом*. Заметим, что поскольку $m = \deg g(x)$, то значение $k = n - m$ уже не произвольно, как у линейных кодов общего вида. Определение кодового расстояния циклического кода в общем случае является чрезвычайно трудоёмкой задачей.

Из всех линейных (n, k) -кодов будем далее рассматривать исключительно циклические.

Пример 3.5. Построим циклический код длины $n = 23$. В п. 2 примера 2.13 найдены число и степени неприводимых многочленов, факторизующих бином $x^{23} - 1$. Конкретно это разложение таково:

$$f(x) = (x + 1) \underbrace{(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)}_{g_1(x)} \times \\ \times \underbrace{(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)}_{g_2(x)}.$$

Поскольку степени полиномов $g_1(x)$ и $g_2(x)$ оказались равными $m = 11$, для построения $(23, 12)$ -кода может быть выбран любой из них.

Можно показать, что в обоих случаях кодовое расстояние оказывается равным 7. Ясно, что построен код Голея.

Построенная в примере 3.2 таблица 4×7 для кода Хэмминга *не порождает циклического кода*. Однако если переставить 3-элементные окончания некоторых строк, то полученная таблица (см. ниже)

1	0	0	0	1	1	0
0	1	0	0	0	1	1
0	0	1	0	1	1	1
0	0	0	1	1	0	1

уже порождает циклический код.

Кодирование циклическими кодами. Пусть определён порождающий полином $g(x)$, делящий бином $x^n - 1$, $\deg g(x) = m < n$ и задающий код C .

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий:

$$u(x) \mapsto v(x) = g(x)u(x).$$

Систематическое кодирование осуществляется приписыванием к кодовому слову *слева* (в младшие разряды) остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$.

Действительно, умножение $u(x)$ на x^m помещает сообщение в старшие разряды n -битного слова. Поделим теперь $x^m u(x)$ на $g(x)$ с остатком:

$$x^m u(x) = g(x)q(x) + r(x), \quad \deg r(x) < m,$$

откуда

$$v(x) = x^m u(x) + r(x) = g(x)q(x) \in C \in \{0, 1\}^n.$$

Пример 3.6. 1. Построим циклический код длины $n = 7$.

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени неприводимых делителей данного бинома, для чего применим способ разбиения вычетов по модулю 7 на орбиты относительно умножения на 2 (см. с. 62):

$$\{0\}, \{1, 2, 4\}, \{3, 6, 5\}.$$

Пусть теперь α — корень бинома $x^7 - 1$ из поля его разложения. С учётом теоремы 2.8 о корнях неприводимого многочлена, приходим к выводу, что все 7 корней бинома $x^7 - 1$ разбиваются на классы

$$C_0 = \{\alpha^0 = 1\}, C_1 = \{\alpha, \alpha^2, \alpha^4\}, C_2 = \{\alpha^3, \alpha^6, \alpha^5\}.$$

Таким образом, бином $x^7 - 1$ имеет один неприводимый делитель 1-й степени и два неприводимых делителя 3-й степени. Поскольку линейный делитель, очевидно, есть $x - 1$, а остальные делители единственны, получаем разложение

$$x^7 - 1 = x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

В качестве порождающего полинома $g(x)$ можно выбрать любой из вышеуказанных полиномов 3-й степени. Тогда $m = 3$, $k = 4$ и будет построен *циклический (7, 4)-код*⁴⁾.

⁴⁾ Ясно, это код Хэмминга. При выборе $g(x) = x + 1$ получаем код с проверкой на чётность, а при выборе, например $g(x) = (x + 1)(x^3 + x + 1) -$ т. н. *расширенный код Хэмминга*.

Определяя код, выберем конкретно

$$g(x) = x^3 + x + 1.$$

2. Закодируем несистематическим и систематическим кодированием сообщение

$$\mathbf{u} = [0\ 0\ 1\ 1]^T \leftrightarrow u(x) = x^3 + x^2.$$

Несистематическое кодирование.

$$\begin{aligned} v(x) &= u(x)g(x) = (x^3 + x^2)(x^3 + x + 1) = \\ &= x^6 + x^5 + x^4 + x^2 \leftrightarrow [0\ 0\ 1\ 0\ 1\ 1\ 1]^T = \mathbf{v}. \end{aligned}$$

Систематическое кодирование.

Находим $r(x) = \left\{ \frac{x^3 u(x)}{g(x)} \right\}$:

$$x^3(x^3 + x^2) = x^6 + x^5 = (x^3 + x^2 + x)(x^3 + x + 1) + x,$$

ПОЭТОМУ

$$v(x) = x^3 u(x) + r(x) = x^6 + x^5 + x \leftrightarrow [0\ 1\ 0\ \underbrace{0\ 0\ 1\ 1}]^T = \mathbf{v}.$$

Декодирование циклических кодов

Определение 3.5. Синдромом $s(x)$ слова $w(x)$, принятого при передаче сообщения, закодированного циклическим кодом и, возможно, содержащего ошибки, называют остаток от деления $w(x)$ на порождающий код многочлен $g(x)$.

Свойства синдрома $s(x)$:

- $0 \leq \deg s(x) < m$;
- $s(x) = 0 \Leftrightarrow w(x)$ — кодовое слово;

$$\bullet s(x) \equiv_{g(x)} w(x) \equiv_{g(x)} v(x) + e(x) \equiv_{g(x)} e(x).$$

Схема синдромного декодирования слова $w(x)$:

- 1) вычисляется синдром $s(x)$;
- 2) для всех 2^k возможных сообщений $u(x)$ находят-ся полиномы $e(x) = s(x) + g(x)u(x)$;
- 3) из всех возможных полиномов ошибок выбира-ется полином $e_0(x)$ с минимальным числом мо-номов; если таковых несколько, то выбирают любой из них;
- 4) восстанавливается переданное сообщение $u(x) = w(x) + e_0(x)$.

Примеры декодирования циклических кодов бу-дут даны при рассмотрении БЧХ-кодов⁵⁾.

3.5 Коды БЧХ

Определение и основные свойства БЧХ-кодов.
Коды Боуза-Чоудхури-Хоквингема (ВСН, БЧХ) — подкласс циклических кодов, исправляющих не менее заранее заданного числа ошибок⁶⁾.

⁵⁾ Существуют и альтернативные методы декодирования циклических кодов общего вида (декодеры Меггита, Касами-Рудольфа, пороговый, мажоритарный, ...), все — также экспоненциальной по k трудоёмкости.

⁶⁾ предложены Раджем Чандра Боузом и Двайджендра Камар Рей-Чоудхури в 1960 г. независимо от опубликованной на год ранее работы Алек-сиса Хоквингема

Циклотомический класс элемента поля. В теории кодирования рассматривают коды общего вида и вводят понятие циклотомического класса (или класса сопряжённости), элемента α поля \mathbb{F}_2^{kl} над своим подполем \mathbb{F}_2^k .

Для бинарных кодов $k = 1$, и это понятие тесно связано с понятием орбиты отображения $t \mapsto 2t \pmod{2^l - 1}$ элементов мультипликативной группы (см. с. 63) поля \mathbb{F}_2^l , когда оно является полем разложения неприводимых над \mathbb{F}_2 полиномов.

Определение 3.6 (для поля \mathbb{F}_2). *Циклотомическим классом* элемента $\alpha \neq 0$ поля \mathbb{F}_2^l над своим простым подполем \mathbb{F}_2 называется множество всех различных элементов $\alpha, \alpha^2, \alpha^4, \dots$ из \mathbb{F}_2^l .

Свойства циклотомических классов.

1. Циклотомические классы C_0, C_1, \dots различных элементов либо совпадают, либо не пересекаются, и в совокупности образуют разбиение мультипликативной группы поля \mathbb{F}_2^l , или, как говорят, её *разложение на классы*.
2. Если α — примитивный элемент поля \mathbb{F}_2^l , то его циклотомический класс *содержит ровно l элементов*: поскольку $\alpha^{2^l} = 1$, данный класс есть

$$C_1 = \left\{ \alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{l-1}} \right\}.$$

3. Минимальный многочлен некоторого элемента циклотомического класса является общим для всех элементов этого класса.

Пример 3.7. Пусть $l = 4$ и α — примитивный элемент поля $\mathbb{F}_2^4 = F$. Тогда $\alpha^{15} = 1$ и разложение F^* над \mathbb{F}_2 на циклотомические классы есть

$$C_0 = \{1\}, C_1 = \{\alpha, \alpha^2, \alpha^4, \alpha^8\}, C_2 = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}, \\ C_3 = \{\alpha^5, \alpha^{10}\}, C_4 = \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}.$$

БЧХ-коды: определение (простейший случай), синдромы. Пусть выбраны параметр l , определяющий длину кода $n = 2^l - 1$ и *конструктивное расстояние* $d_c < n$. Далее рассматривается поле \mathbb{F}_2^l разложения биннома $x^n - 1$ и некоторый примитивный элемент α этого поля.

Код БЧХ есть циклический (n, k, d) -код, в котором делящий бином $x^n - 1$ порождающий многочлен $g(x)$ является полиномом минимальной степени, имеющим корнями *нули кода* $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{d_c-1}$.

Для построенного кода $\deg g(x) = m, k = n - m$. При этом кодовое расстояние d оказывается не менее выбранного конструктивного расстояния d_c ; это *важнейшее свойство БЧХ-кодов*.

Поскольку все кодовые слова циклического кода делятся на полином $g(x)$ с корнями в нулях кода, то они одновременно и корни любого кодового слова.

Определение 3.7. *Синдромами полинома $w(x)$, принятого при передаче сообщения, закодированного БЧХ-кодом с нулями α^i , и, возможно, содержащего ошибки, назовём набор значений $w(x)$ в нулях кода: $s_i = w(\alpha^i), i = \overline{1, d-1}$.*

Далее, поскольку

$$w(x) = v(x) + e(x), \quad \text{то} \quad s_i = w(\alpha^i) = e(\alpha^i),$$

и все синдромы равны нулю если и только если $w(x)$ — кодовое слово.

Алгоритм построения БЧХ-кода. БЧХ (n, k) -код, как и любой циклический, задаётся порождающим полиномом $g(x)$ — делителем бинома $x^n - 1$, $\deg g(x) = m$, $k = n - m$.

Для построения кода БЧХ нужно:

- 1) выбрать величину l , определяющую длину кода $n = 2^l - 1$ и степень расширения простого поля \mathbb{F}_2 ;
- 2) задать величину конструктивного расстояния $d_c = 2r + 1 < n$, если необходимо исправлять до r ошибок;
- 3) выбрав неприводимый полином $a(x) \in \mathbb{F}_2[x]$ степени l , определить поле $\mathbb{F}_2^l = \mathbb{F}_2[x]/(a(x))$ с примитивным элементом α ;
- 4) найти циклотомические классы поля \mathbb{F}_2^l над \mathbb{F}_2 , в которые попадают $d_c - 1$ нулей кода $\alpha, \alpha^2, \dots, \alpha^{2r}$; пусть таких классов h ;
- 5) найти минимальные многочлены $g_1(x), \dots, g_h(x)$ каждого циклотомического класса;
- 6) вычислить порождающий полином кода

$$g(x) = g_1(x) \cdot g_2(x) \cdot \dots \cdot g_h(x).$$

Пример 3.8. Выберем $l = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

Возьмём многочлен $a(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ и образуем поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^3$.

Поскольку многочлен $a(x)$ — примитивный, то элемент $\alpha = x$ примитивен, и, как показано в п. 1 примера 3.6 на с. 94, F^* разбивается на следующие циклотомические классы над \mathbb{F}_2 :

$$C_0 = \{1\}, C_1 = \{\alpha, \alpha^2, \alpha^4\}, C_2 = \{\alpha^3, \alpha^6, \alpha^5\}.$$

Для построения кодов, исправляющих заданное количество ошибок, необходимо определить соответствующий порождающий полином.

1. Код БЧХ длины $n = 7$, исправляющий $r = 1$ ошибку.

В этом случае $d_c - 1 = 2r = 2$ и нули кода α, α^2 попадают в один циклотомический класс C_1 .

Минимальный многочлен элементов этого класса — $a(x)$, поэтому порождающий полином $g(x) = a(x)$, $m = 3$, $k = 4$ и в результате получаем уже известный $(7, 4, 3)$ -код Хэмминга.

2. Код БЧХ длины $n = 7$, исправляющий не менее $r = 2$ ошибок.

Теперь $2r = 4$. Нули строящегося кода $\alpha, \alpha^2, \alpha^3, \alpha^4$ входят в циклотомические классы C_1 и C_2 , поэтому

$$g(x) = g_1(x) \cdot g_2(x),$$

где $g_1(x)$ и $g_2(x)$ — м. м. классов C_1 и C_2 .

М. м. для C_1 известен: $g_1(x) = a(x) = x^3 + x + 1$.

Найдем м. м. для C_2 :

$$\begin{aligned} g_2(x) &= (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) = \\ &= x^3 + (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^8 + \alpha^9 + \alpha^{11})x + \alpha^{14}. \end{aligned}$$

Вычислим коэффициенты $g_2(x)$:

$$\begin{aligned} \alpha^3 + \alpha^5 + \alpha^6 &= (\alpha + 1) + \alpha^2(\alpha + 1) + (\alpha + 1)^2 = \\ &= \alpha + 1 + \alpha^3 + \alpha^2 + \alpha^2 + 1 = \\ &= \alpha + \alpha^3 = 1, \\ \alpha^8 + \alpha^9 + \alpha^{11} &= \alpha^2 + \alpha + \alpha^4 = \alpha^2 + \alpha + \alpha(\alpha + 1) = 0, \\ \alpha^{14} &= (\alpha^7)^2 = 1. \end{aligned}$$

Таким образом $g_2(x) = x^3 + x^2 + 1$ ⁷⁾ и

$$\begin{aligned} g(x) &= g_1(x) \cdot g_2(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Получаем $m = \deg g(x) = 6$ и $k = 1$, то есть построен тривиальный код с 7-кратным повторением, исправляющий 3 ошибки, но его скорость $R = 1/7$.

Пример 3.9. Попытаемся построить лучший код для исправления двух ошибок, взяв бóльшую его длину: выберем $l = 4$ и тогда длина кода $n = 2^4 - 1 = 15$.

Рассмотрим поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^4$, образованное некоторым неприводимым многочленом $a(x)$ степени $l = 4$. Тогда F^* относительно своего примитивного элемента α , как показано в п. 2 примера 3.7, разобьётся на 5 циклотомических классов над \mathbb{F}_2 :

⁷⁾ что можно было понять сразу: это второй из двух неприводимых многочленов степени 3 из $\mathbb{F}_2[x]$

$$C_0 = \{1\}, C_1 = \{\alpha, \alpha^2, \alpha^4, \alpha^8\}, C_2 = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}, \\ C_3 = \{\alpha^5, \alpha^{10}\}, C_4 = \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}.$$

Конкретно в качестве многочлена 4-й степени, образующего поле возьмём примитивный многочлен

$$a(x) = x^4 + x + 1,$$

который одновременно является м. м. для примитивного элемента $\alpha = x$ и всего класса C_1 .

1. Код БЧХ длины $n = 15$, исправляющий $r = 2$ ошибки.

В этом случае $2r = 4$ и нули $\alpha, \alpha^2, \alpha^3, \alpha^4$ конструируемого кода располагаются в циклотомических классах C_1 и C_2 .

М. м. для элементов этих классов суть: первого — $g_1(x) = a(x)$, второго —

$$g_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = \dots \\ \dots = x^4 + x^3 + x^2 + x + 1.$$

Тогда порождающий полином кода есть

$$g(x) = g_1(x) \cdot g_2(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

Получено $m = 8$, $k = 7$ и, как можно показать, $d = d_c = 5$, то есть построен БЧХ (15, 7, 5)-код со скоростью уже $R = 7/15 > 1/7$.

2. Код БЧХ длины $n = 15$, исправляющий $r = 3$ ошибки.

Теперь $2r = 6$ и нужно найти полином, являющийся м. м. для нулей $\alpha, \alpha^2, \dots, \alpha^6$, которые попадают в циклотомические классы C_1, C_2 и C_3 .

Минимальные многочлены для α и α^3 уже найдены. Далее, очевидно $g_3(x) = x^2 + x + 1$, поскольку это единственный неприводимый квадратный многочлен над \mathbb{F}_2 . Тогда порождающий полином есть

$$\begin{aligned} g(x) &= g_1(x) \cdot g_2(x) \cdot g_3(x) = \\ &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \end{aligned} \quad (3.1)$$

Получено $m = 10$, $k = 5$ и можно показать, что $d = d_c = 7$. Этот $(15, 5, 7)$ -код БЧХ при той же длине, что и предыдущий, исправляет больше ошибок, но имеет меньшую скорость $R = 1/3$.

3.6 Декодирование кодов БЧХ

Декодирование кода Хэмминга как линейного кода с помощью проверочной матрицы было уже рассмотрено в разделе 3.3. Опишем ещё один метод декодирования кодов Хэмминга как кодов БЧХ.

В этом случае $d = 3$, и нулями кода являются α и α^2 , где α — примитивный элемент поля \mathbb{F}_2^n , $n = 2^l - 1$.

Для декодирования принятого слова $w(x)$ вычисляем синдром $s_1 = w(\alpha) = s$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется). При $s = 0$ считаем, что ошибок не произошло. Если $s \neq 0$, то определяем значение j , для которого $\alpha^j = s$ и считаем, что произошла единичная ошибка в j -м разряде для $j = 0, 1, \dots, n-1$.

Пример 3.10. Рассматриваем $(7, 4)$ -код Хэмминга, построенный в примере 3.6 для циклических кодов, где

был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [0\ 0\ 1\ 1]^T$:

$$v(x) = x^3 u(x) + x \leftrightarrow [0\ 1\ 0\ \underline{0\ 0\ 1\ 1}]^T.$$

u

Пусть при передаче кодового слова $v(x)$ произошла ошибка в 5-й позиции, то есть принято слово

$$[0\ 1\ 0\ 0\ 0\ \overline{0}\ 1]^T \leftrightarrow w(x) = x^6 + x.$$

Для декодирования $w(x)$ найдем синдром:

$$\begin{aligned} s = w(\alpha) &= \alpha^6 + \alpha = (\alpha^3)^2 + \alpha = (\alpha + 1)^2 + \alpha = \\ &= \alpha^2 + 1 + \alpha \neq 0. \end{aligned}$$

Определим значение j , для которого $\alpha^j = s$:

$$\begin{aligned} \alpha^0 &= 1, & \alpha^3 &= \alpha + 1, \\ \alpha^1 &= \alpha, & \alpha^4 &= \alpha(\alpha + 1) = \alpha^2 + \alpha, \\ \alpha^2 &= \alpha^2, & \alpha^5 &= \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 = s \end{aligned}$$

и 5-я позиция ошибки определена верно.

Декодирование кодов БЧХ: общий случай.

Рассмотрим (n, k, d) -код БЧХ длины $n = 2^l - 1$ при построении которого для определения порождающего полинома использовалось поле $F = \mathbb{F}_2^l = \mathbb{F}_2[x]/(a(x))$, $\deg a(x) = l$ и пусть α — нуль кода.

Пусть при передаче кодового слова произошло $\nu \leq r = \lfloor (d-1)/2 \rfloor$ ошибок в позициях j_1, \dots, j_ν . Тогда полином ошибок есть

$$e(x) = x^{j_1} + x^{j_2} + \dots + x^{j_\nu}.$$

Результатом работы декодера является полином локаторов ошибок $\sigma(x)$, степень которого есть число реально произошедших ошибок $\nu = \deg \sigma(x)$.

После нахождения $\sigma(x)$ можно отыскать все ν его корней α^{-j_i} , а по ним — позиции ошибок j_i , $i = \overline{1, \nu}$.

Алгоритм декодирования (n, k, d) -кода БЧХ

Пусть $n = 2^l - 1$, α — нуль кода, примитивный элемент поля $F = \mathbb{F}_2[x]/(a(x)) = \mathbb{F}_2^l$, $\deg a(x) = l$ и принято слово $w(x)$.

1. Найти все синдромы $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$; если все они равны 0, то считаем, что ошибок нет, $v(x) = w(x)$ и переход к пункту 6.
2. Используя тот или иной декодер, найти полином локаторов ошибок $\sigma(x)$; число произошедших ошибок $\nu = \deg \sigma(x)$.
3. Найти все корни $\sigma(x)$, например, перебором элементов F^* ; пусть эти корни суть $\alpha^{k_1}, \dots, \alpha^{k_\nu}$.
4. Найти позиции ошибок $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
5. Найти полином ошибок $e(x) = x^{j_1} + \dots + x^{j_\nu}$ и восстановить кодовое слово $v(x) = w(x) + e(x)$.
6. По $v(x)$ восстановить сообщение $u(x)$.

Декодер на основе расширенного алгоритма Евклида. Определим *синдромный полином*

$$s(x) = 1 + s_1x + s_2x^2 + \dots + s_{2r}x^{2r},$$

где s_i — синдромы, $i = \overline{1, 2r}$ и, формально, $s_0 = 1$ и $s_i = 0$ при $i > 2r$.

Перемножив введённые полиномы, получим *полином значений ошибок*:

$$s(x)\sigma(x) = 1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_{2r+\nu}x^{2r+\nu}.$$

Его коэффициенты определяются соотношением для произведения многочленов —

$$\lambda_i = \sum_{j=0}^i \sigma_j s_{i-j}, \quad i = \overline{1, 2r + \nu}.$$

Замечаем, что значения λ_i по данной формуле для $i = \nu + 1, \dots, 2r$ суть левые части соотношений (*), то есть все они равны 0. Значит, полином значений ошибок имеет нулевую «среднюю часть». Обозначим его начальную часть $\lambda(x)$, а из заключительной вынесем за скобку x^{2r+1} :

$$s(x)\sigma(x) = \underbrace{1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_\nu x^\nu}_{\lambda(x)} + x^{2r+1} (\lambda_{2r+1} + \dots + \lambda_{2r+\nu}x^{\nu-1}), \quad 1 \leq \nu \leq r.$$

Это означает, что

$$s(x)\sigma(x) = \lambda(x) \pmod{x^{2r+1}}.$$

Данное соотношение называют *ключевым уравнением*. Его решение $\sigma(x)$ при $\nu \leq r$ единственно.

Ключевое уравнение имеет вид (2.1). Это позволяет записать его в виде соотношения Безу

$$s(x)\sigma(x) + x^{2r+1}b(x) = \lambda(x),$$

которое может быть решено расширенным алгоритмом Евклида в поле F (см. с. 41) с условием останова

$\deg \lambda(x) \leq r$, конкретно — «степень полученного остатка не более r », и опусканием заключительного шага нормировки.

Пример 3.11. Будем использовать БЧХ $(15, 5, 7)$ -код с полем разложения $\mathbb{F}_2[x]/(x^4 + x + 1) = F$, построенный в п. 2 примера 3.9. При вычислениях будем пользоваться таблицей со с. 45.

Пусть передаётся сообщение

$$\mathbf{u} = [0 \ 1 \ 1 \ 0 \ 1]^T \leftrightarrow u(x) = x^4 + x^2 + x.$$

При систематическом кодировании порождающим полиномом (3.1) кодовом словом, как можно показать, будет

$$\mathbf{v} = [0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]^T.$$

Предположим, что при передаче ошибки произошли в 0, 6 и 12-й позициях, то есть принято слово (ошибки подчёркнуты)

$$\begin{aligned} w(x) &= x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \leftrightarrow \\ &\leftrightarrow [\overline{1} \ 1 \ 1 \ 1 \ 1 \ 0 \ \overline{1} \ 0 \ 1 \ 0 \ 0 \ 1 \ \overline{0} \ 0 \ 1]^T = \mathbf{w}. \end{aligned}$$

1. Найдём все $2r = 6$ синдромов:

$$\begin{aligned} s_1 = w(\alpha) &= \underbrace{(\alpha^3 + 1)}_{\alpha^{14}} + \underbrace{(\alpha^3 + \alpha^2 + \alpha)}_{\alpha^{11}} + \underbrace{(\alpha^2 + 1)}_{\alpha^8} + \\ &+ \underbrace{(\alpha^3 + \alpha^2)}_{\alpha^6} + \underbrace{(\alpha + 1)}_{\alpha^4} + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha, \end{aligned}$$

$$s_2 = w(\alpha^2) = (w(\alpha))^2 = s_1^2 = \alpha^2,$$

$$s_3 = w(\alpha^3) = \alpha^{42} + \alpha^{33} + \alpha^{24} + \alpha^{18} + \alpha^{12} + \alpha^9 +$$

$$\begin{aligned}
& + \alpha^6 + \alpha^3 + 1 = \dots = \alpha^8, \\
s_4 = w(\alpha^4) &= s_1^4 = \alpha^4, \\
s_5 = w(\alpha^5) &= \alpha^{70} + \alpha^{55} + \alpha^{40} + \alpha^{30} + \alpha^{20} + \alpha^{15} + \\
& + \alpha^{10} + \alpha^5 + 1 = \dots = 1, \\
s_6 = w(\alpha^6) &= s_3^2 = \alpha^{16} = \alpha.
\end{aligned}$$

Таким образом, синдромный полином есть

$$s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha x + 1.$$

2. По декодеру на базе расширенного алгоритма Евклида решаем относительно $\sigma(x)$ соотношение Безу

$$x^7 b(x) + s(x) \sigma(x) = \lambda(x).$$

$$\begin{aligned}
\text{Шаг 0. } r_{-2}(x) &= x^7, \\
r_{-1}(x) &= s(x), \\
\sigma_{-2}(x) &= 0, \quad \sigma_{-1}(x) = 1.
\end{aligned}$$

$$\begin{aligned}
\text{Шаг 1. } r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\
q_0(x) &= \alpha^{14}x + \alpha^{13}, \\
r_0(x) &= \alpha^8 x^5 + \alpha^{12} x^4 + \alpha^{11} x^3 + \alpha^{13}, \\
\deg r_0(x) &= 5 > 3 = r, \\
\sigma_0(x) &= q_0(x).
\end{aligned}$$

$$\begin{aligned}
\text{Шаг 2. } r_{-1}(x) &= r_0(x)q_1(x) + r_1(x), \\
q_1(x) &= \alpha^8 x + \alpha^2, \\
r_1(x) &= \alpha^{14} x^4 + \alpha^3 x^3 + \alpha^2 x^2 + \alpha^{11} x, \\
\deg r_1(x) &= 4 > 3 = r, \\
\sigma_1(x) &= \sigma_{-1}(x) + \sigma_0(x)q_1(x) = \\
&= \alpha^7 x^2 + \alpha^{11} x.
\end{aligned}$$

$$\begin{aligned}
\text{Шаг 3. } r_0(x) &= r_1(x)q_2(x) + r_2(x), \\
q_2(x) &= \alpha^9x, \\
r_2(x) &= \alpha^5x + \alpha^{13}, \\
\deg r_2(x) &= 1 \leq 3 = r, \\
\sigma_2(x) &= \sigma_0(x) + \sigma_1(x)q_2(x) = \\
&= \alpha x^3 + \alpha^5x^2 + \alpha^{14}x + \alpha^{13}.
\end{aligned}$$

Это последний шаг алгоритма, т. к. степень остатка $r_2(x)$ не превосходит r . Таким образом, полином локаторов ошибок найден:

$$\sigma(x) = \sigma_2(x) = \alpha x^3 + \alpha^5x^2 + \alpha^{14}x + \alpha^{13},$$

и установлено число ошибок $\nu = \deg \sigma(x) = 3$.

3. Найдём корни $\sigma(x)$ перебором элементов F^* .

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2, \\
\sigma(\alpha^2) &= \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha, \\
\sigma(\alpha^3) &= \alpha^{10} + \alpha^{11} + \alpha^2 + \alpha^{13} = \mathbf{0}, \\
\sigma(\alpha^4) &= \alpha^{13} + \alpha^{13} + \alpha^3 + \alpha^{13} = \alpha^2 + 1, \\
\sigma(\alpha^5) &= \alpha + 1 + \alpha^4 + \alpha^{13} = \alpha^{13}, \\
\sigma(\alpha^6) &= \alpha^4 + \alpha^2 + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^2, \\
\sigma(\alpha^7) &= \alpha^7 + \alpha^4 + \alpha^6 + \alpha^{13} = \alpha^3 + 1, \\
\sigma(\alpha^8) &= \alpha^{10} + \alpha^6 + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + 1, \\
\sigma(\alpha^9) &= \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = \mathbf{0}, \\
\sigma(\alpha^{10}) &= \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha, \\
\sigma(\alpha^{11}) &= \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha, \\
\sigma(\alpha^{12}) &= \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1, \\
\sigma(\alpha^{13}) &= \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,
\end{aligned}$$

$$\begin{aligned}\sigma(\alpha^{14}) &= \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1, \\ \sigma(\alpha^{15}) &= \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = \mathbf{0}.\end{aligned}$$

4. По найденным корням $\alpha^3, \alpha^9, \alpha^{15}$ вычисляем позиции ошибок:

$$j_1 = -3 \equiv_{15} 12, \quad j_2 = -9 \equiv_{15} 6, \quad j_3 = -15 \equiv_{15} 0.$$

5. Таким образом полином ошибок

$$e(x) = x^{12} + x^6 + 1$$

определён и переданное кодовое слово есть

$$v(x) = w(x) + e(x) \leftrightarrow [0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ \underbrace{0 \ 1 \ 1 \ 0 \ 1}_u]^T.$$

Проверка $v(\alpha) = v(\alpha^2) = \dots = v(\alpha^6) = 0$ говорит о том, что восстановление верное (или же произошло $r \gg 3$ ошибок, что маловероятно).

6. Поскольку применялось систематическое кодирование, исходное сообщение $u(x)$ восстанавливается элементарно.

Помехоустойчивое кодирование применяется:

- Для получения надёжной связи либо при малом отношении сигнал/шум канала, либо в системах, критичных к ошибкам (ВТ).
- Для защиты данных во внутренних и внешних ЗУ: ленты, SSD диски, flash-память.
- При синтезе отказоустойчивых дискретных управляющих устройств (например, БИС).

Справка. В системах передачи данных широко используется двоичный $(255, 231, 7)$ -код БЧХ, для которого $l = 8$ и степень порождающего код многочлена $g(x)$ есть $m = 24$. При этом в общем количестве слов длины 255 доля кодовых есть $2^{-24} \approx 17 \cdot 10^{-6}$, а все шары радиуса 3 с центрами в кодовых словах занимают $\approx 16,5\%$ объёма куба B^{255} .

В течении многих лет не было случая, чтобы ошибка передачи прошла незамеченной.

Замечание. Исправление ошибок может требоваться не всегда: часто достаточно лишь проверить наличие ошибок и при необходимости повторить передачу нужное число раз. В этих случаях применяются коды, предназначенные только для обнаружения ошибок.

3.7 Задачи

3.1. Для линейного кода, заданного своей проверочной матрицей

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

требуется

- 1) построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;

2) найти такое кодирование для сообщений

$$\mathbf{u}_1 = [1\ 1\ 0\ 1]^T, \quad \mathbf{u}_2 = [1\ 0\ 0\ 1]^T.$$

3.2. Циклический $(9, 3)$ -код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние d , а также осуществить систематическое кодирование полинома

$$u(x) = x^2 + x \leftrightarrow [0\ 1\ 1]^T.$$

3.3. Рассмотрим код Хэмминга систематического кодирования с порождающим примитивным полиномом $a(x) = x^3 + x + 1$.

Требуется декодировать полиномы

$$1) \quad w_1(x) = x^6 + x^2 + x,$$

$$2) \quad w_2(x) = x^6 + x^5 + x^3 + x^2 + x,$$

$$3) \quad w_3(x) = x^6 + x^3 + x^2 + x.$$

3.4. Пусть $n = 5$ и α — примитивный элемент поля $\mathbb{F}_2^5 = F$. Найти разложение F^* над \mathbb{F}_2 .

3.5. Пусть α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^4 + x + 1)$. Для кода БЧХ с нулями α , α^2 , α^3 и α^4 и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

3.6. Рассмотрим код БЧХ, нули которого определяются степенями α , где α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^4 + x + 1)$.

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок есть

$$\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить *позиции ошибок* в $w(x)$.

3.7. Построить 31-разрядный БЧХ-код для исправления не менее $r = 3$ ошибок.

3.8. Рассмотрим БЧХ-код, нули которого есть степени примитивного элемента α поля $F = \mathbb{F}_2[x]/(x^4 + x + 1)$.

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить *позиции ошибок* в данном слове.

Решения задач

1. Группы, кольца, поля

1.1. (1) Да, (2) нет (противоположного элемента), (3) нет (устойчивости), (4) нет (ассоциативности), (5) нет (обратного у 0), (6) да, (7) да, (8) нет (ассоциативности), (9) да, (10) нет (обратных у всех), (11)–(16) да.

1.2. Любая циклическая 6-элементная группа изоморфна $\mathbb{Z}_6 = \langle \{0, 1, \dots, 5\}, +, 0 \rangle$.

$$\text{ord } 0 = 1;$$

$$1, 1 + 1 = 2, \dots = 6 \cdot 1 = 0 \Rightarrow \text{ord } 1 = 6;$$

$$2, 2 + 2 = 4, 4 + 2 = 0 \Rightarrow \text{ord } 2 = 3;$$

$$3, 3 + 3 = 0 \Rightarrow \text{ord } 3 = 2;$$

$$4, 4 + 4 = 2, 2 + 4 = 0 \Rightarrow \text{ord } 4 = 3;$$

$$5, 5 + 5 = 4, 4 + 5 = 3, \dots, 6 \cdot 5 = 0 \Rightarrow \text{ord } 5 = 6.$$

Порождающие элементы — 1 и 5, их порядок — 6.

1.3. Любая циклическая 24-элементная группа изоморфна $\mathbb{Z}_{24} = \langle \{0, 1, \dots, 23\}, +, 0 \rangle$.

1. Все подгруппы циклической группы — циклические. Порождающими элементами подгрупп \mathbb{Z}_{24} будут делители m порядка группы 24: то есть $m = 1, 2, 3, 4, 6, 8, 12, 24 \equiv 0$.

Порядок соответствующей подгруппы — $24/m$.

$$m = 1 : \{1, 2, \dots, 23, 0\} = \langle 1 \rangle = C \cong \mathbb{Z}_{24};$$

$$m = 2 : \{2, 4, 6, \dots, 22, 0\} = \langle 2 \rangle \cong \mathbb{Z}_{12};$$

$$m = 3 : \{3, 6, 9, \dots, 21, 0\} = \langle 3 \rangle \cong \mathbb{Z}_8;$$

$$m = 4 : \{4, 8, 12, \dots, 20, 0\} = \langle 4 \rangle \cong \mathbb{Z}_6;$$

$$m = 6 : \{6, 12, 18, 0\} = \langle 6 \rangle \cong \mathbb{Z}_4;$$

$$m = 8 : \{8, 16, 0\} = \langle 8 \rangle \cong \mathbb{Z}_3;$$

$$m = 12 : \{12, 0\} = \langle 12 \rangle \cong \mathbb{Z}_2;$$

$$m = 24 : \{0\} = \langle 0 \rangle \cong E \text{ — единичная.}$$

2. Циклическая группа \mathbb{Z}_{24} имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \cdot \varphi(2) \cdot \varphi(3) = 4 \cdot 1 \cdot 2 = 8$ генераторов m , взаимно простых с 24, то есть $m = 1, 5, 7, 11, 13, 17, 19, 23$.

$$\begin{aligned} 1.4. \quad \varphi(n) &= \varphi(p_1^{\alpha_1}) \cdot \dots \cdot (p_k^{\alpha_k}) = \\ &= p_1^{\alpha_1-1} \varphi(p_1) \cdot \dots \cdot p_k^{\alpha_k-1} \varphi(p_k) = \\ &= p_1^{\alpha_1-1} \cdot \dots \cdot p_k^{\alpha_k-1} \varphi(p_1) \cdot \dots \cdot \varphi(p_k) = \\ &= \frac{n}{p_1 \cdot \dots \cdot p_k} (p_1 - 1) \cdot \dots \cdot (p_k - 1) = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

1.5. (1) Кольцо (обратной матрицы может не быть), (2) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы), (3) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ в случае $a_0 = 0$ необратимы).

1.6. По дистрибутивности

$$\begin{aligned} x \cdot (y+z) &= x \cdot y + x \cdot z \Rightarrow x \cdot (0+0) = x \cdot 0 = x \cdot 0 + x \cdot 0 \Rightarrow \\ &\Rightarrow x \cdot 0 = 0. \end{aligned}$$

1.7. Нет! Хотя $f(x+y) = 2(x+y) = 2x+2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$.

1.8. Множество векторов V содержит нулевой вектор $\mathbf{0}$ и является, очевидно, абелевой группой по сложению, а операция \times векторного умножения связана со сложением дистрибутивными законами

$$\mathbf{x} \times (\mathbf{y} + \mathbf{z}) = \mathbf{x} \times \mathbf{y} + \mathbf{x} \times \mathbf{z}, \quad (\mathbf{y} + \mathbf{z}) \times \mathbf{x} = \mathbf{y} \times \mathbf{x} + \mathbf{z} \times \mathbf{x}.$$

Кольцо $\langle V, +, \times, \mathbf{0} \rangle$ некоммутативно: $\mathbf{x} \times \mathbf{y} \neq \mathbf{y} \times \mathbf{x}$ и неассоциативно: $\mathbf{x} \times (\mathbf{y} \times \mathbf{z}) \neq (\mathbf{x} \times \mathbf{y}) \times \mathbf{z}$.

Однако в рассматриваемом кольце выполняются тождества, заменяющие, в некотором смысле коммутативность и ассоциативность:

$$\begin{aligned} \mathbf{x} \times \mathbf{y} &= -\mathbf{y} \times \mathbf{x} \quad (\text{антикоммутативность}), \\ (\mathbf{x} \times \mathbf{y}) \times \mathbf{z} + (\mathbf{y} \times \mathbf{z}) \times \mathbf{x} + \\ &+ (\mathbf{z} \times \mathbf{x}) \times \mathbf{y} = \mathbf{0} \quad (\text{тождество Якоби}). \end{aligned}$$

1.9. В кольце \mathbb{Z}_6 классы вычетов по идеалу $(3) = \{0, 3\}$ суть

$$\begin{aligned} 0 + (3) &= 3 + (3) = (0, 3), \\ 1 + (3) &= 4 + (3) = (1, 4), \\ 2 + (3) &= 5 + (3) = (2, 5). \end{aligned}$$

1.10. Нет! В \mathbb{Z}_2 : $1 + 1 = 0$, а в \mathbb{Z}_5 : $1 + 1 = 2$, то есть операция сложения в \mathbb{Z}_5 неустойчива при переходе к своему подмножеству $\{0, 1\}$.

2. Конечные кольца и поля

2.1. Вычислять x^{-1} в кольцах \mathbb{Z}_n можно используя соотношение Безу (подбором коэффициентов или расширенным алгоритмом Евклида). В некоторых очевидных случаях (напр. в пункте в)) можно обойтись без вычислений.

а) $1 = 2 \cdot 3 - 1 \cdot 5$, $2 \cdot 3 = 1 + 1 \cdot 5$, $2 \cdot 3 \equiv_5 1$, $3^{-1} \equiv_5 2$;

б) $1 = 2 \cdot 14 - 3 \cdot 9$, $(-3) \cdot 9 = 1 - 2 \cdot 14$,
 $(-3) \cdot 9 \equiv_{14} 1$, $9^{-1} = -3 = 11 \pmod{14}$;

в) $x \cdot 1 \equiv 1 \Rightarrow 1^{-1} = 1$ по любому модулю;
 $1^{-1} \equiv_{118} 1$;

г) $1 = 2 \cdot 4 - 1 \cdot 7$, $2 \cdot 4 = 1 + 1 \cdot 7$, $2 \cdot 4 \equiv_7 1$,
 $4^{-1} \equiv_7 2$, $3 \cdot 4^{-1} = 3 \cdot 2 = 6 \pmod{7}$;

д) $-3 \equiv_7 4$, в пункте г) вычислено $4^{-1} \equiv_7 2$, значит,
 $(-3)^{-1} = 4^{-1} = 2 \pmod{7}$;

е) $1 = 2 \cdot 6 - 1 \cdot 11$, $2 \cdot 6 = 1 + 1 \cdot 11$, $2 \cdot 6 \equiv_{11} 1$,
 $6^{-1} \equiv_{11} 2$, $6^{-2} = (6^{-1})^2 = 2^2 = 4 \pmod{11}$;

ж) $1 = 3 \cdot 3 - 8$, $3 \cdot 3 = 1 + 8$, $3 \cdot 3 \equiv_8 1$,
 $3^{-1} \equiv_8 3$, $3^{-3} = (3^{-1})^3 = 3^3 = 27 = 3 \pmod{8}$.

2.2. а) $x = 7^{-1} \cdot 11 = 18 \cdot 11 = 198 = 23 \pmod{25}$;

б) $x = 9^{-1} \cdot 3 = (-1)^{-1} = 3 = -3 = 7 \pmod{10}$;

в) $6x \equiv_7 1$, $x = 6^{-1} = -1 = 6 \pmod{7}$;

г) $6x \equiv_9 1$ решений нет: элемент 6 не обратим в \mathbb{Z}_9 ;

д) $6x \equiv_9 2$; решений нет: сравнение можно сократить — $3x \equiv_9$, но элемент 3 не обратим в \mathbb{Z}_9 ;

- е) $6x \equiv_9 3$. Такое равенство можно сократить на 3 вместе с модулем: $2x \equiv_3 1$, откуда $x = 2^{-1} = 2 \pmod{3}$. Множество решений — $\{2, 5, 8\} \pmod{9}$.

2.3. Имеем

$$F = \mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1 = \alpha^3, \alpha, \alpha + 1 = \alpha^2\},$$

где α — порождающий элемент мультипликативной группы F^* . Поэтому

$$\begin{aligned} P &= \prod_{i=1}^3 (x - \beta_i) = (x + 1)(x + \alpha)(x + \alpha + 1) = \\ &= (x + 1)(x^2 + \alpha x + x + \alpha x + \alpha^2 + \alpha) = \\ &= (x + 1)(x^2 + x + \alpha^2 + \alpha) = \\ &= (x^3 + (\alpha + 1)x^2 + (\alpha + 1)x^2 + (\alpha^2 + \alpha + 1)x + \\ &\quad + \alpha^2 + \alpha) = x^3 + 1, \end{aligned}$$

и по теореме 2.4: $(x - \beta_1) \cdots (x - \beta_{p^n-1}) = x^{p^n-1} - 1$.

2.4. Все элементы \mathbb{F}_p^* суть корни уравнения

$$x^{p-1} - 1 = 0,$$

их сумма по теореме Виета есть коэффициент при x^{p-2} в этом уравнении, то есть 0.

2.5. При $p = 2$ утверждение тривиально.

При $p > 2$ порядки всех элементов мультипликативной циклической группы $\mathbb{F}_p^* = \{1, \dots, p-1\}$ делят её порядок то есть все они являются корнями уравнения

$$x^{p-1} - 1 = 0. \quad (*)$$

Других корней у этого уравнения нет (многочлен степени $p - 1$ имеет не больше $p - 1$ корней). По теореме Виета их произведение равно свободному члену многочлена $(*)$, то есть -1 .

Ещё одно Решение. Для $p = 2, 3$ утверждение тривиально. При $p \geq 5$ обозначим

$$1 \cdot \underbrace{2 \cdot \dots \cdot (p-2)}_{=\pi} \cdot (p-1) = (p-1)!,$$

и заметим, что $(p-1)^2 = p^2 - 2p + 1 \equiv_p 1$.

Легко видеть, что произведение $\pi = 1$: каждый из элементов $2, \dots, p-2$ поля \mathbb{F}_p имеет единственный обратный, и он входит в $\pi = 1$, т. к. элемент $p-1$ обратен сам себе.

Отсюда $(p-1)! = p-1$, или $(p-1)! \equiv_p -1$.

2.6. Это поле \mathbb{F}_2^2 , оно может быть построено как факторкольцо $\mathbb{F}_2[x]/(a(x))$, где $a(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$ степени 2. Но такой многочлен только один: $x^2 + x + 1$.

Следовательно, $\mathbb{F}_2^2 = \{0, 1, x, x+1\}$ и $x^2 = x+1$ (черту над элементами не пишем).

Таблицы сложения и умножения в построенном поле (операции с 0 опускаем):

+	1	x	$x+1$
1	0	$x+1$	x
x	$x+1$	0	1
$x+1$	x	1	0

\times	1	x	$x + 1$
1	1	x	$x + 1$
x	x	$x + 1$	1
$x + 1$	$x + 1$	1	x

2.7. Воспользуемся алгоритмом Евклида:

$$x^5 + x^2 + x + 1 = (x^2 + x)(x^3 + x^2 + x + 1) + \underline{(x^2 + 1)},$$

$$x^3 + x^2 + x + 1 = (x + 1)\underline{(x^2 + 1)}.$$

Ответ: $x^2 + 1$.

2.8. Поле $F = \mathbb{F}_2[x]/(x^3 + x + 1)$ содержит 8 элементов: 0 и степени 1, ..., 7 порождающего элемента α . Можно полагать $x = \alpha$, т. к. $a(x)$ — примитивный многочлен.

1. Таблица соответствий между полиномиальным и степенным представлением его ненулевых элементов:

$x^3 = x + 1$	степень x	1	x	x^2
	x	(0	1	0)
	x^2	(0	0	1)
	$x^3 = x + 1$	(1	1	0)
	$x^4 = x^2 + x$	(0	1	1)
	$x^5 = x^2 + x + 1$	(1	1	1)
	$x^6 = x^2 + 1$	(1	0	1)
	$x^7 = 1$	(1	0	0)

2. Таблица умножения:

\times	x	x^2	x^3	x^4	x^5	x^6
x	x^2	$x + 1$	$x^2 + x$	$x^2 + x + 1$	$x^2 + 1$	1
x^2	$x + 1$	$x^2 + x$	$x^2 + x + 1$	$x^2 + 1$	1	x
x^3	$x^2 + x$	$x^2 + x + 1$	$x^2 + 1$	1	x	x^2
x^4	$x^2 + x + 1$	$x^2 + 1$	1	x	x^2	$x + 1$
x^5	$x^2 + 1$	1	x	x^2	$x + 1$	$x^2 + x$
x^6	1	x	x^2	$x + 1$	$x^2 + x$	$x^2 + x + 1$

3. Обратные элементы:

x	x^2	$x + 1$	$x^2 + x$	$x^2 + x + 1$	$x^2 + 1$
$x^2 + 1$	$x^2 + x + 1$	$x^2 + x$	$x + 1$	x^2	x

4. Поле F имеет $\varphi(7) = 6$ порождающих элементов: все кроме 0 и 1.

5. Находим м. м. элементов поля. Ясно, что

- $m_0(x) = x$;
- $m_1(x) = x + 1$;
- остальные элементы F суть порождающие его мультипликативной группы, и их м. м. будут совпадать с $a(x)$.

2.9. Поле \mathbb{F}_p^n содержит подполе \mathbb{F}_p^k если и только если $k \mid n$, поэтому подполями $GF(2^{30})$ будут поля $GF(2^k)$, $k \in D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$, $GF(2)$ — простейшее и $GF(2^{30})$ — несобственное подполя.

2.10. В поле \mathbb{F}_2 имеем $x - 1 = x + 1$.

1. $f(1) = 0 \Rightarrow 1$ — корень f .
2. Делим $f(x)$ на $x + 1$, получаем

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

3. $f_1(1) = 0 \Rightarrow 1$ — корень f_1 ; $\frac{f_1}{x+1} = x^3 + 1 = f_2(x)$.
4. $f_2(1) = 0 \Rightarrow 1$ — корень f_2 ; $\frac{f_2}{x+1} = x^2 + x + 1$.
5. Многочлен $x^2 + x + 1$ неприводим.

Ответ: $x^5 + x^3 + x^2 + 1 = (x + 1)^3(x^2 + x + 1)$.

2.11. 1. $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$,
 $(x - 2) \equiv_5 (x + 3)$

2.

$$\begin{array}{r|l} x^3 + 2x^2 + 4x + 1 & x + 3 \\ x^3 + 3x^2 & \hline 4x^2 + 4x & \\ 4x^2 + 2x & \\ \hline 2x + 1 & \\ 2x + 1 & \\ \hline 0 & \end{array}$$

3. Перебором убеждаемся, что многочлен $x^2 + 4x + 2$ неприводим в \mathbb{F}_5 .

Ответ: $x^3 + 2x^2 + 4x + 1 = (x + 3)(x^2 + 4x + 2)$.

2.12. 1. $0, 1, 2$ — не корни $f(x) \Rightarrow f(x)$ линейных делителей не содержит.

2. Неприводимые многочлены над \mathbb{F}_3 степени 2:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2.$$

3. Подбором получаем

$$\text{Ответ: } f(x) = x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2).$$

2.13. 1. $f(x) \neq 0$ ни при каком $x = 0, 1, 2, 3, 4$, то есть $f(x)$ не имеет линейных делителей.

2. Перебирая неприводимые многочлены степени 2 над \mathbb{F}_5 , получаем

$$\text{Ответ: } f(x) = (x^2 + x + 1)(x^2 + 2x + 4).$$

2.14. Вычисляя значения при $x = 0, 1$ всех нормированных многочленов 3-й степени из $\mathbb{F}_2[x]$, определяем их линейные делители и получаем, что

$$f_1(x) = x^3 = x \cdot x \cdot x,$$

$$f_2(x) = x^3 + 1 = (x + 1)(x^2 + x + 1),$$

$$f_3(x) = x^3 + x = x(x + 1)^2,$$

$$f_4(x) = x^3 + x^2 = x^2(x + 1),$$

$$f_5(x) = x^3 + x + 1 \text{ — неприводим,}$$

$$f_6(x) = x^3 + x^2 + 1 \text{ — неприводим,}$$

$$f_7(x) = x^3 + x^2 + x = x(x^2 + x + 1),$$

$$f_8(x) = x^3 + x^2 + x + 1 = (x + 1)^3.$$

2.15. Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

Перебором коэффициентов $b, c \in \{0, 1, 2\}$ в выражении $x^2 + bx + c$, находим подходящие многочлены:

$$\begin{aligned}f_1(x) &= x^2 + 1, \\f_2(x) &= x^2 + x + 2, \\f_3(x) &= x^2 + 2x + 2.\end{aligned}$$

2.16. Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

$$\begin{aligned}f_1(x) &= x^3 + 2x + 1, \\f_2(x) &= x^3 + 2x + 2, \\f_3(x) &= x^3 + x^2 + 2, \\f_4(x) &= x^3 + 2x^2 + 1, \\f_5(x) &= x^3 + x^2 + x + 2, \\f_6(x) &= x^3 + x^2 + 2x + 1, \\f_7(x) &= x^3 + 2x^2 + x + 1, \\f_8(x) &= x^3 + 2x^2 + 2x + 2.\end{aligned}$$

2.17. 1. Перебором элементов из \mathbb{F}_5 —

$$a(0) = 4, \quad a(1) = 2, \quad a(2) = 1, \quad a(3) = 2, \quad a(4) = 1,$$

убеждаемся, что квадратный многочлен $a(x)$ неприводим.

Следовательно, факторкольцо $\mathbb{F}_5[x]/(x^2 + 2x + 4)$ является полем; в нём $x^2 = -2x - 4 = 3x + 1$.

$$\begin{aligned}2. \quad a(4x^2 + 1) &= (2(2x^2 + 1))^3 + 2 \cdot 2(2x^2 + 1) + 4 = \\&= 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 = \\&= 4(3x + 1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + \\&x + x^2 + 1 = 0 \text{ — да, является.}\end{aligned}$$

2.18. 1. $a(x) = x^2 + x - 1$, $a(0) = 6$, $a(1) = 1$, $a(2) = 5$, $a(3) = 4$, $a(4) = 6$, $a(5) = 1$, $a(6) = 6$, то есть многочлен $a(x)$ — неприводим в \mathbb{F}_7 и F — поле ($\cong \mathbb{F}_7^2$).

$$2. \quad \mathbb{F}_7^2 = \{ ax + b \mid a, b \in \mathbb{F}_7, x^2 = 1 - x = 6x + 1 \}$$

$$(ax + b) \cdot (6x + 1) = \dots = (2a + 6b)x + (6a + b) = 1$$

$$\begin{cases} 6a + b = 1 \\ a + 3b = 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

Ответ: $(1 - x)^{-1} = x + 2$ в F .

$$2.19. \quad \beta = x + x^2 = x(x + 1).$$

Мультипликативная группа указанных полей состоит из $2^4 - 1 = 15$ элементов.

Примарное разложение 15: $15 = 3 \cdot 5$, поэтому равенство $\beta^d = 1$ нужно проверить для $d = 15/5 = 3$ и $d = 15/3 = 5$.

$$1. \quad \underline{x^4 = x + 1}$$

$$\beta^2 = x^2(x + 1)^2 = x^4 + x^2 = x^2 + x + 1,$$

$$\begin{aligned} \beta^3 &= x(x + 1)(x^2 + x + 1) = x(x^3 + 1) = \\ &= x^4 + x = x + 1 + x = 1. \end{aligned}$$

Ответ: В поле F_1 $\text{ord } \beta = 3$.

$$2. \quad \underline{x^4 = x^3 + 1}$$

$$\beta^2 = x^4 + x^2 = x^3 + x^2 + 1,$$

$$\begin{aligned} \beta^3 &= x(x + 1)(x^3 + x^2 + 1) = \\ &= x(x^4 + x^2 + x + 1) = x(x^3 + x^2 + x) = \\ &= x^4 + x^3 + x^2 = x^2 + 1 \neq 1, \end{aligned}$$

$$\begin{aligned} \beta^5 &= x^2x^3 = (x^3 + x^2 + 1)(x^2 + 1) = \\ &= (x^5 + x^4 + x^2 + x^3 + x^2 + 1) = \dots \end{aligned}$$

$$\dots = (x^3 + 1)x = x^4 + x = x^3 + x + 1 \neq 1.$$

Ответ: В поле F_2 $\text{ord } \beta = 15$.

2.20. Мультипликативная группа поля

$$\mathbb{F}_2[x]/(x^6 + x^3 + 1)$$

состоит из $2^6 - 1 = 63$ элементов.

Простые делители $63 = 3^2 \cdot 7$ суть 3 и 7, поэтому равенство $x^d = 1$ нужно проверить только для $d = 21 = \frac{63}{3}$ и $d = 9 = \frac{63}{7}$.

В рассматриваемом поле $x^6 = x^3 + 1$ и

$$x^9 = x^6 x^3 = (x^3 + 1)x^3 = x^6 + x^3 = x^3 + 1 + x^3 = 1.$$

Т.о. $\text{ord } x = 9 \neq 63$ и многочлен $f(x)$ не примитивен.

2.21.

$$\sum_{d|n} d \cdot ((d)) = p^n.$$

1. $((7))$ над \mathbb{F}_2

$$\sum_{d|7} d \cdot ((d)) = 2^7 = 1 \cdot ((1)) + 7 \cdot ((7)) = 128.$$

$((1)) = 2$: это x и $x + 1$, отсюда $((7)) = \frac{128-2}{7} = 18$.

2. $((6))$ над \mathbb{F}_5

$$\begin{aligned} ((6)) &= \frac{1}{6} \sum_{d|6} \mu(d) 5^{\frac{6}{d}} = \frac{1}{6} [\mu(1)5^6 + \mu(2)5^3 + \\ &+ \mu(3)5^2 + \mu(6)5] = \frac{15625 - 125 - 25 + 5}{6} = 2580. \end{aligned}$$

2.22. $\text{char } F = 3$, поэтому $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

$F = \mathbb{F}_3^2$, F^* содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1, 8}$ примитивного элемента α .

Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в \mathbb{F}_3^2 проводятся по $\text{mod } a(x)$, будем иметь

$$x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1.$$

Найдём порядок элемента x : т.к. $8 = 2^3, \frac{8}{2} = 4$, проверим равенство $x^4 = 1$:

$$x^4 = (x^2)^2 = (2x + 1)^2 = x^2 + x + 1 = 2x + 1 + x + 1 = 2 \neq 1,$$

то есть x — примитивный элемент F : $\text{ord } x = 8, x^8 = 1$.

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над \mathbb{F}_3 , иначе примитивный элемент поля F пришлось бы искать.

Теперь вычислим значение заданного выражения. Имеем $2^8 = 256 \equiv_3 1, x + 2 = -x^2, x^4 = 2$ и далее:

$$\begin{aligned} S &= \frac{1}{2x + 1} - \frac{(2x)^7(2)}{(x)^9(x + 2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} = \\ &= x^6 + x^4 = (x^2)^3 + 2 = (2x + 1)^3 + 2 = 2x^3 + 1 + 2 = \\ &= 2x(2x + 1) = x^2 + 2x = 2x + 1 + 2x = x + 1. \end{aligned}$$

2.23. В данном 9-элементном поле

$$x^2 + 1 = 0 \Rightarrow x^2 = -1 \equiv_3 2.$$

1. Найдём порядок элемента x , для чего проверим равенство $x^4 = 1$ (т. к. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = (x^2)^2 = 4 \equiv_3 1.$$

Следовательно $\text{ord } x = 4$ и элемент x не является генератором группы F^* (и $x^2 + 1$ — не есть примитивный многочлен над \mathbb{F}_3 :

$$x^4 - 1 = x^4 + 2 = (x^2 + 1)(x^2 + 2)).$$

2. Проверим на примитивность элемент $x + 1$:

$$\begin{aligned} (x + 1)^4 &= (x + 1)(x + 1)^3 = (x + 1)(x^3 + 1) = \\ &= (x + 1)(2x + 1) = 2x^2 + x + 2x + 1 = 4x + 1 = 2 \neq 1 \end{aligned}$$

то есть $\alpha = x + 1$ оказался примитивным элементом. Его степени:

$$\begin{aligned} \alpha^1 &= x + 1, & \alpha^5 &= 2(x + 1) = 2x + 2, \\ \alpha^2 &= x^2 + 2x + 1 = 2x, & \alpha^6 &= \alpha^2 \cdot \alpha^4 = 4x = x, \\ \alpha^3 &= 2x(x + 1) = 2x + 1, & \alpha^7 &= x(x + 1) = x + 2, \\ \alpha^4 &= 4x^2 = x^2 = 2, & \alpha^8 &= (\alpha^4)^2 = 4 = 1. \end{aligned}$$

Замечание: вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

2.24. 1. Сначала проверим, является ли многочлен $f(x) = x^2 + x + 2$ делителем $x^4 + 1$?

$$x^4 + 1 = (x^2 + x + 2) \cdot (x^2 + 2x + 2) \quad \text{— да, является}$$

Поэтому искомым идеал составят многочлены из R , кратные $f(x)$:

$$(x^2 + x + 2) = \{ (x^2 + x + 2)(ax + b) \mid a, b \in \mathbb{F}_3, x^4 = 1 \}.$$

2. Проведём умножение:

$$(x^2 + x + 2)(ax + b) = ax^3 + (a + b)x^2 + (2a + b)x + 2b.$$

Теперь, перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $(x^2 + x + 2)$:

a	b	$ax^3 + (a + b)x^2 + (2a + b)x + 2b$
0	0	0
0	1	$x^2 + x + 2$
0	2	$2x^2 + 2x + 1$
1	0	$x^3 + x^2 + 2x$
1	1	$x^3 + 2x^2 + 2$
1	2	$x^3 + x + 1$
2	0	$2x^3 + 2x^2 + x$
2	1	$2x^3 + 2x + 2$
2	2	$2x^3 + x^2 + 1$

А если бы $f(x) \nmid a(x)$? Тогда в R существует идеал, порождённый элементом НОД $(f(x), a(x))$.

2.25. Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ с учётом $x^2 = 2x + 2$:

$$\begin{aligned} \det M &= (3x + 4)(3x + 2) - (x + 2)(x + 3) = \\ &= 4x^2 + 3x + 3 - x^2 - 1 = \\ &= 3x^2 + 3x + 2 = 3(2x + 2) + 3x + 2 = 4x + 3. \end{aligned}$$

2. Найдём обратный к $4x + 3$ элемент, решая соотношение Безу

$$(x^2 + 3x + 3)a(x) + (4x + 3)b(x) = 1$$

с помощью расширенного алгоритма Евклида:

Шаг 0. // Инициализация

$$r_{-2}(x) = x^2 + 3x + 3,$$

$$r_{-1}(x) = 4x + 3,$$

$$y_{-2}(x) = 0,$$

$$y_{-1}(x) = 1.$$

Шаг 1. // Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком

$$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$$

$$q_0(x) = 4x + 4,$$

$$r_0(x) = 1, \quad // \quad \deg r = 0 \Rightarrow \text{ОСТАНОВ}$$

$$\begin{aligned} y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = \\ &= -q_0(x) = -4x - 4 = x + 1. \end{aligned}$$

3. Вычислим обратную матрицу

$$M^{-1} = (x + 1) \begin{pmatrix} 3x + 2 & 4x + 2 \\ 4x + 3 & 3x + 4 \end{pmatrix} = \begin{pmatrix} x + 2 & 1 \\ 4x & 3x \end{pmatrix}.$$

2.26. 1. $f(0) = f(1) = 1$, и значит $f(x)$ не имеет корней в \mathbb{F}_2 то есть не имеет линейных множителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.

Таковых над \mathbb{F}_2 только один — $x^2 + x + 1$.

При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = (x^2 + x + 1) \times \underbrace{(x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1)}_{g(x)}.$$

Делим частное $g(x)$ на $x^2 + x + 1$:

$$\begin{aligned} g(x) &= x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^2 + x + 1) \cdot (x^7 + x^4 + x^3 + x^2 + x + 1) + x \end{aligned}$$

— не делится нацело, то есть $x^2 + x + 1$ — делитель $f(x)$ кратности 1.

3. Неприводимых многочленов 3-й степени над \mathbb{F}_2 только два: $x^3 + x + 1$ и $x^3 + x^2 + 1$.

Пробуем поделить $g(x)$ на $x^3 + x + 1$:

$$\begin{aligned} x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 &= \\ = (x^3 + x + 1) \underbrace{(x^6 + x^5 + x^3 + x^2 + 1)}_{h(x)} &\quad \text{— делится!} \end{aligned}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

$$\begin{aligned} x^6 + x^5 + x^3 + x^2 + 1 &= \\ &= (x^3 + x + 1) \cdot (x^3 + x^2 + x + 1) + x^2, \\ x^6 + x^5 + x^3 + x^2 + 1 &= (x^3 + x^2 + 1) \cdot x^3 + x^2 + 1. \end{aligned}$$

Поскольку многочлен $h(x)$ 6-й степени не имеет делителей 3-й и меньших степеней, то он является неприводимым.

Ответ: В $\mathbb{F}_2[x]$ справедливо разложение

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = (x^2 + x + 1)(x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

2.27. 1. Найдём разложение многочлена $f(x)$ на неприводимые множители над \mathbb{F}_3 .

- Ищем корни: $f(0) = 2$, $f(1) = 1$, $f(2) = 0$.
Поскольку $x - 2 \equiv_3 x + 1$, то $f(x) = (x + 1)(x^2 + 2x + 2)$.
- Многочлен $g(x) = x^2 + 2x + 2$ не имеет корней в \mathbb{F}_3 , его степень 2, т. е. он неприводим.
- Окончательно: $f(x) = (x + 1)(x^2 + 2x + 2)$.

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над \mathbb{F}_p , то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —

$$g(x) = (x - \alpha) \cdot (x - \alpha^p) \cdot (x - \alpha^{p^2}) \cdot \dots \cdot (x - \alpha^{p^{n-1}}),$$
 где α — произвольный корень $g(x)$ в F ;
- не имеет корней ни в каком конечном поле, содержащем менее, чем p^n элементов.

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$.

В этом поле если α — корень $g(x)$, то и α^3 — тоже его корень. Вычисляем:

$$\begin{aligned}\alpha^2 &= -2\alpha - 2 = \alpha + 1, \\ \alpha^3 &= \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1\end{aligned}$$

Построенное поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ содержит найденный ранее корень 2, поэтому многочлен $f(x)$ в этом поле раскладывается на следующие линейные множители:

$$f(x) = x^3 + x + 2 = (x - 2)(x - \alpha)(x - 2\alpha - 1) = (x + 1)(x + 2\alpha)(x + \alpha + 2).$$

4. Определить корни многочлена

$$g(x) = (x - \alpha)(x - 2\alpha - 1)$$

в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ легко: всегда можно взять $\alpha = x$, откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

Ответ: многочлен $f(x) = x^3 + x + 2$ имеет корни 2, x , $2x + 1$ в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2) = GF(3^2)$.

$$2.28. \quad \beta \in \{0, 1, \alpha, \dots, \alpha^{14}\} = F, \quad x^4 = x + 1.$$

$$\beta = 0: m_0(x) = x.$$

$$\beta = 1: m_1(x) = x + 1.$$

$$\begin{aligned}\beta = \alpha: \text{сопряжённые с } \alpha \text{ элементы } - \alpha^2, \alpha^4, \alpha^8 \text{ и} \\ (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = \dots \\ \dots = x^4 + x + 1 = 0.\end{aligned}$$

Это означает, что $x^4 + x + 1$ — примитивный многочлен и $m_\alpha(x) = x^4 + x + 1$.

$\beta = \alpha^3$: сопряжённые с α^3 элементы суть $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$, их м. м. —

$$\begin{aligned} m_{\alpha^3}(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = \\ &= x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + \\ &+ (\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12})x^2 + \\ &+ (\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12})x + \\ &+ (\alpha^3\alpha^6\alpha^9\alpha^{12}) = x^4 + (\alpha^3 + (\alpha^3 + \alpha^2) + (\alpha^3 + \alpha) + \\ &+ (\alpha^3 + \alpha^2 + \alpha + 1))x^3 + (\dots)x^2 + (\dots)x + \alpha^{30} = \\ &= x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

$\beta = \alpha^5$: единственный сопряжённый с α^5 элемент — α^{10} (т. к. $\alpha^{20} = \alpha^5$), их м. м. —

$$m_{\alpha^5}(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1.$$

$\beta = \alpha^7$: сопряжённые с α^7 элементы — $\alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{56} = \alpha^{11}$, их м. м. —

$$\begin{aligned} m_{\alpha^7}(x) &= (x - \alpha^7)(x - \alpha^{11})(x - \alpha^{13})(x - \alpha^{14}) = \\ &= x^4 + x^3 + 1. \end{aligned}$$

2.29. 1. Любой многочлен в поле характеристики 5 вместе с корнем α^3 содержит все сопряжённые с ним $(\alpha^3)^5 = \alpha^{15}, (\alpha^3)^{5^2} = \alpha^{75}, (\alpha^3)^{5^3} = \alpha^{375}$ и т. д.

2. В поле F имеем $\alpha^{5^2-1} = \alpha^{24} = 1$, и сопряжённым с α^3 будет только элемент α^{15} , т. к. $\alpha^{75} = \alpha^3$. Поэтому минимальный многочлен элемента α^3 — квадратный:

$$m_{\alpha^3}(x) = (x - \alpha^3)(x - \alpha^{15}) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}.$$

3. Найдём коэффициенты данного многочлена, учитывая $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha + 3) = 4\alpha^2 + 3\alpha = \\ &= 4(4\alpha + 3) + 3\alpha = 4\alpha + 2,\end{aligned}$$

$$\begin{aligned}\alpha^{15} &= (\alpha^3)^5 = (4\alpha + 2)^5 = 4\alpha^5 + 2 = \\ &= 4\alpha^2\alpha^3 + 2 = 4(4\alpha + 3)(4\alpha + 2) + 2 = \\ &= 4(\alpha^2 + 1) + 2 = 4(4\alpha + 4) + 2 = \alpha + 3,\end{aligned}$$

$$\alpha^3 + \alpha^{15} = 4\alpha + 2 + \alpha + 3 = 0,$$

$$\begin{aligned}\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha + 2)(\alpha + 3) = \\ &= 4(4\alpha + 3) + 4\alpha + 1 = 3.\end{aligned}$$

Ответ: $m(x) = x^2 + 3$.

2.30. 1) Поскольку $|F_1^*| = 2^3 - 1 = 7$ — простое число, то каждый неединичный элемент мультипликативной группы F^* — её генератор, в т. ч. и x . Это означает, что x — примитивный элемент поля F и м.м. многочлен $a(x)$ примитивен.

2) Поскольку $|F_2^*| = 2^4 - 1 = 15 = 3 \cdot 5$, то для определения значения $\text{ord } x$ нужно проверить на равенства $x^3 = 1$ и $x^5 = 1$.

Первое равенство явно не имеет места, поэтому вычисляем с учётом $x^4 = x^3 + x^2 + x + 1$:

$$\begin{aligned}x^5 &= x \cdot x^4 = x \cdot (x^3 + x^2 + x + 1) = \\ &= x^4 + x^3 + x^2 + x = (x^3 + x^2 + x + 1) + x^3 + x^2 + x = 1.\end{aligned}$$

Это означает, что $\text{ord } x = 5 \neq 15$, x — не есть примитивный элемент F , а м.м. $a(x)$ не примитивен.

2.31. Вычисление значений $f(x)$ для $x = 0, 1, \dots, 4$, показывает, что $f(3) = 0$, т. е. $x = 3$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 3$ (или на $x + 2$), получим $x^3 + 3x^2 + 4x + 4 = (x - 3) \cdot (x^2 + x + 2)$.

Перебором элементов $x \in GF(5)$ убеждаемся, что $f_2(x) = x^2 + x + 2$ — неприводимый многочлен.

В поле $\mathbb{F}_5[x]/(x^2 + x + 2)$ корни многочлена $f_2(x) = 0$ суть $\{x, x^5\}$ и $x^2 = -x - 2 = 4x + 3$.

Вычисляем:

$$\begin{aligned} x^5 &= (x^2)^2 x = x(4x + 3)^2 = x(x^2 + 4x + 4) = \\ &= x(4x + 3 + 4x + 4) = x(3x + 2) = 3x^2 + 2x = \\ &= 2x + 4 + 2x = 4x + 4. \end{aligned}$$

Ответ: $\{3, x, 4x + 4\}$.

2.32. Подстановкой в $f(x)$ всех элементов $0, \dots, 4$ поля \mathbb{F}_5 убеждаемся, что данный многочлен 2-й степени не имеет линейных делителей и, следовательно, неприводим.

Порядок мультипликативной группы $GF(5^2)$ есть $24 = 2^3 \cdot 3$. Определим порядок элемента её x , для которого $x^2 = -x - 2 = 4x + 3$.

Поскольку простые делители 24 суть 2 и 3, проверим равенство $x^d = 1$ для $d \in \left\{ \frac{24}{2} = 12, \frac{24}{3} = 8 \right\}$.

Имеем:

$$x^4 = (x^2)^2 = (4x + 3)^2 = x^2 + 4x + 4 = \dots$$

$$\begin{aligned}
 \dots &= 3x + 2 \neq 1, \\
 x^8 &= (x^4)^2 = (3x + 2)^2 = -x^2 + 2x + 4 = \dots \\
 \dots &= 3x + 1 \neq 1. \\
 x^{12} &= x^8 x^4 = (3x + 1)(3x + 2) = -x^2 + 4x + 2 = \dots \\
 \dots &= 4 \neq 1.
 \end{aligned}$$

Следовательно $\text{ord } x = 24$ и рассматриваемый многочлен примитивен в поле $\mathbb{F}_5[x]/(x^2 + x + 2)$.

2.33. Поскольку $n = 40 = 5 \cdot 8$, то корни бинома $x^{40} - 1$ суть все корни $x^8 - 1$ (они все различны), но 5-й кратности.

Рассмотрим разложение многочлена $x^8 - 1$ над \mathbb{F}_5 . Относительно умножения на 5 вычеты по модулю 8 $\{\bar{0}, \bar{1}, \dots, \bar{7}\}$ разбиваются на орбиты:

$$\{\bar{0}\}, \{\bar{1}, \bar{5}\}, \{\bar{2}\}, \{\bar{3}, \bar{7}\}, \{\bar{4}\}, \{\bar{6}\}.$$

Пояснение: $5 \cdot 5 = 25 \equiv_8 1$, $2 \cdot 5 = 10 \equiv_8 2$ и т. д.

Поэтому:

- бином $x^8 - 1 \in \mathbb{F}_5[x]$ разлагается в произведение четырёх линейных и двух неприводимых квадратных многочленов;
- бином $x^{40} - 1 = (x^8 - 1)^5$ разлагается в произведение двадцати многочленов степени 1 (четырёх кратности 5 каждый) и десяти неприводимых многочленов степени 2 (двух кратности 5 каждый);
- максимальная степень неприводимых делителей-многочленов есть 2, следовательно полем расширения данного бинома будет \mathbb{F}_5^2 .

Замечание. В данном случае разложение бинома $x^8 - 1 \in \mathbb{F}_5[x]$ на неприводимые множители легко находится (первые три равенства справедливы в любом кольце):

$$x^8 - 1 = (x^4 - 1)(x^4 + 1),$$

$$x^4 - 1 = (x^2 - 1)(x^2 + 1),$$

$$x^2 - 1 = (x - 1)(x + 1),$$

$$x^2 + 1 \equiv_5 x^2 - 4 = (x - 2)(x + 2),$$

$$x^4 + 1 \equiv_5 x^4 - 4 = (x^2 - 2)(x^2 + 2).$$

Итого в $\mathbb{F}_5[x]$:

$$x^8 - 1 = (x + 1)(x - 1)(x + 2)(x - 2)(x^2 + 2)(x^2 - 2).$$

И далее

$$x^{40} - 1 = (x + 1)^5(x - 1)^5(x + 2)^5(x - 2)^5(x^2 + 2)^5(x^2 - 2)^5.$$

2.34. $\deg f(x) = 2$ и поэтому $f(x)$ имеет 2 корня.

(1) Полином $f(x)$ неприводим над $\mathbb{F}_2 \Rightarrow$ его корни суть x и x^2 .

(2) Полином $f(x)$ приводим над \mathbb{F}_3 :

$$x^2 + x + 1 = x^2 - 2x + 1 = (x - 1)^2,$$

поэтому $f(x)$ над \mathbb{F}_3 имеет корень 1 степени 2.

(3) Полином $f(x)$ неприводим над $\mathbb{F}_5 \Rightarrow$ его корни x и x^5 .

2.35. Вычисляем значения $f(x)$ для всех x из $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$: $f(0) = 4$, $f(1) = 1$, $f(2) = 0$ и т. о. $x = 2$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 2 = x + 3$, получим $2x^4 + x^3 + 4x^2 + 4 = (x + 3) \cdot (2x^3 + 4x + 3)$.

Для удобства нормируем частное $2x^3 + 4x + 3$: т. к. $2^{-1} = 3$, то вместо уравнения $2x^3 + 4x + 3 = 0$ можно решать уравнение

$$f_2(x) = 3 \cdot (2x^3 + 4x + 3) = x^3 + 2x + 4 = 0.$$

Перебором элементов $x \in \mathbb{F}_5$ —

$$f(0) = 4, f(1) = 2, f(2) = 1, f(3) = 2, f(4) = 1,$$

убеждаемся, что $f_2(x) = x^3 + 2x + 4$ — неприводимый многочлен¹²⁾.

В поле $\mathbb{F}_5[x]/(x^3 + 2x + 4)$ корнями многочлена $f_2(x) = 0$ будут x, x^5, x^{25} .

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 &= x^2(3x + 1) = 3x^3 + x^2 = 4x + 3 + x^2 = \\ &= x^2 + 4x + 3; \end{aligned}$$

$$\begin{aligned} x^{25} &= (x^5)^5 = (x^2 + 4x + 3)^5 = x^{10} + 4^5 x^5 + 3^5 = \\ &= x^{10} + 4(x^2 + 4x + 3) + 3 = x^{10} + 4x^2 + x. \end{aligned}$$

(поскольку $4^5 = 2^{10} = 1024$ и $3^5 = 81 \cdot 3 = 243$).

Найдём отдельно x^{10} :

$$\begin{aligned} x^{10} &= (x^5)^2 = (x^2 + 4x + 3)^2 = \\ &= x^4 + x^2 + 3^2 + 3x^3 + 4x + x^2 = \\ &= x^4 + 3x^3 + 2x^2 + 4x + 4 = \end{aligned}$$

¹²⁾ а если бы это был многочлен 4-й степени?

$$= 3x^2 + \cancel{x} + \cancel{4x} + 3 + \cancel{2x^2} + 4x + 4 = 4x + 2.$$

Продолжаем:

$$x^{25} = x^{10} + 4x^2 + x = \cancel{4x} + 2 + 4x^2 + \cancel{x} = 4x^2 + 2.$$

Ответ: уравнение $f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0$, где $f(x) \in \mathbb{F}_5[x]$ имеет корни $2, x, x^2 + 4x + 3, 4x^2 + 2$ в поле $F = \mathbb{F}_5[x]/(x^3 + 2x + 4)$ (поскольку корень $2 \in F$).

2.36. В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над \mathbb{F}_2 многочленов:

$$x^8 + x^4 + x^2 + x + 1 = \underbrace{(x^4 + x^3 + 1)}_{f_1(x)} \cdot \underbrace{(x^4 + x^3 + x^2 + x + 1)}_{f_2(x)}.$$

Уравнения $f_1(x) = 0$ и $f_2(x) = 0$ ранее были решены: их корни соответственно суть

$$x, x^2, x^3 + 1, x^3 + x^2 + x$$

в поле $F_1 = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$

и

$$x, x^2, x^3, x^3 + x^2 + x + 1$$

в поле $F_2 = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$.

Степени обоих расширений поля $GF(2)$ совпадают (=4) и поля F_1 и F_2 изморфны, т. о. все 8 корней уравнения $f(x) = 0$ лежат в поле $GF(2^4)$.

Для записи данных корней выберем представление F_1 поля $GF(2^4)$. Тогда запись корней $f_1(x)$ останется без изменений, а корни $f_2(x)$ надо представить как элементы F_1 .

Приравнивая многочлены, порождающие данные поля, получим

$$x^4 + x^3 + 1 = x^4 + x^3 + x^2 + x + 1 \Rightarrow x^2 + x = x(x+1) = 0.$$

Ясно, что при подстановке $x \mapsto x + 1$ полученное равенство останется справедливым. Применим данную подстановку для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле F_1 :

$$\begin{aligned} x &\mapsto x + 1, \\ x^2 &\mapsto (x + 1)^2 = x^2 + 1, \\ x^3 &\mapsto (x + 1)^3 = x^3 + x^2 + x + 1, \\ x^3 + x^2 + x + 1 &\mapsto (x^3 + x^2 + x + 1) + (x^2 + 1) + \\ &\quad + (x + 1) + 1 = x^3. \end{aligned}$$

Проверим, что, например, $x^2 + 1$ — корень $f(x)$:

$$\begin{aligned} f(x^2+1) &= (x^2+1)^8 + (x^2+1)^4 + (x^2+1)^2 + (x^2+1) + 1 = \\ &= (x^{16} + 1) + (x^8 + 1) + (x^4 + 1) + x^2. \end{aligned}$$

Очевидно $x^{16} = x$, $x^4 = x^3 + 1$ и $x^8 = (x^3 + 1)^2 = x^6 + 1$.

Поскольку $x^5 = x^4 + x = x^3 + x + 1$, то

$x^6 = x^4 + x^2 + x = x^3 + x^2 + x + 1$ и $x^8 = x^3 + x^2 + x$.

Подставляя в выражение для $f(x^2+1)$ полученные полиномиальные представления степеней x , получим

$$f(x^2 + 1) = (x + 1) + (x^3 + x^2 + x + 1) + x^3 + x^2 = 0.$$

Ответ: многочлен $f(x) = x^8 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$ имеет в поле $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$ корни x , x^2 , $x^2 + 1$, x^3 , $x^3 + 1$, $x^3 + x^2 + x$, $x + 1$, $x^3 + x^2 + x + 1$.

2.37. Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных:

$$\begin{aligned} f(x) &= x^4 + 2x + 2 = (x^2 + ax + b)(x^2 + cx + d) = \\ &= x^4 + cx^3 + dx^2x + ax^3 + acx^2 + adx + bx^2 + bcx + bd = \\ &= x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd. \end{aligned}$$

Отсюда

- 1) $c = -a$ и коэффициент при x^2 есть $b - a^2 + d = 0$;
- 2) из $bd = 2$ следует, что либо $b = 1$ и $d = 2$, либо $b = 2$ и $d = 1$, то есть в любом случае $b + d = 3 = 0$;
- 3) но тогда из п. (1) $a^2 = 0$, то есть $a = c = 0$ и коэффициент при x равен $0 \Rightarrow$ противоречие.

Т.о. полином $f(x)$ над \mathbb{F}_3 неприводим.

Теперь рассмотрим поле $\mathbb{F}_3[x]/(x^4 + 2x + 2)$.

В нём $f(x) = x^4 + 2x + 2 = 0$, то есть $x^4 = x + 1 = 0$, и корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3} .

Вычислим x^9 и x^{27} :

$$\begin{aligned} x^9 &= (x^4)^2 x = (x + 1)^2 x = x^3 + 2x^2 + x; \\ x^{27} &= (x^9)^3 = (x^3 + 2x^2 + x)^3 = x^9 + 2x^6 + x^3 = \\ &= \dots = x^3 + x^2 + x. \end{aligned}$$

Ответ: полином $f(x) = x^4 + 2x + 2$ имеет корни $x, x^3, x^3 + 2x^2 + x, x^3 + x^2 + x$ в поле $\mathbb{F}_3[x]/(f)$.

2.38. Поскольку $f(0) = f(1) = 1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

$$x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + x^2) + 1,$$

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$. В нём $f(x) = x^5 + x^2 + 1 = 0$, то есть $x^5 = x^2 + 1 = 0$ и его корни суть $x, x^2, x^{2^2}, x^{2^3}, x^{2^4}$.

Вычислим x^8 и x^{16} :

$$\begin{aligned}x^8 &= x^5 x^3 = (x^2 + 1)x^3 = x^5 + x^3 = x^3 + x^2 + 1; \\x^{16} &= (x^8)^2 = (x^3 + x^2 + 1)^2 = x^6 + x^4 + 1 = \\&= x^5 x + x^4 + 1 = (x^3 + x) + x^4 + 1 = \\&= x^4 + x^3 + x + 1.\end{aligned}$$

Ответ: в поле $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

имеет корни $x, x^2, x^4, x^3 + x^2 + 1, x^4 + x^3 + x + 1$.

3. Коды, исправляющие ошибки

3.1. Проверочная матрица H имеет размерность 3×7 , и код при длине $n = 7$ содержит $m = 3$ проверочных и $k = 7 - 3 = 4$ информационных бит.

Порождающая матрица кода G , обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_4 \end{bmatrix}$.

Матрицу P можно получить, если привести проверочную матрицу H к виду $[I_3 \ P]$, преобразуя строки:

$$\begin{aligned} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} &\xrightarrow{(1) \leftrightarrow (3)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow \\ &\xrightarrow{(1)+(3) \mapsto (1)} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\mathbf{u}_1 = [1101]^T$ и $\mathbf{u}_2 = [1001]^T$:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [\mathbf{v}_1, \mathbf{v}_2] = G \times [\mathbf{u}_1, \mathbf{u}_2] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Очевидно был задан $(7, 4)$ -код Хэмминга.

3.2. Для определения кодового расстояния найдём все кодовые слова:

$$\begin{aligned} v(x) &= g(x)(ax^2+bx+c) = (x^6+x^3+1)(ax^2+bx+c) = \\ &= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c. \end{aligned}$$

В векторном виде все кодовые слова представляются как

$$[a, b, c, a, b, c, a, b, c].$$

Очевидно, это тривиальный код трёхкратного повторения и $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$\begin{aligned} u(x) &\mapsto v(x) = x^6u(x) + r(x), \\ x^6u(x) &= x^6(x^2 + x) = x^8 + x^7. \end{aligned}$$

Находим остаток $\deg r(x)$ от деления $x^6u(x)$ на $g(x)$:

$$\begin{array}{r|l} x^8 + x^7 & x^6 + x^3 + 1 \\ x^8 & + x^2 \\ \hline & x^7 + x^5 + x^2 \\ & x^7 & + x^4 & + x \\ \hline & & x^5 + x^4 + x^2 + x \end{array}$$

Т. о. $r(x) = x^5 + x^4 + x^2 + x$ и

$$v(x) = x^8 + x^7 + x^5 + x^4 + x^2 + x \leftrightarrow [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ \underline{0 \ 1 \ 1}]^T.$$

3.3. Декодирование систематического кода Хэмминга можно провести делением принятого полинома на порождающий: остаток от деления определяет синдром s с учётом таблицы соответствий между полиномиальным и степенным представлением элементов рассматриваемого поля со с. 152):

Находим позицию ошибки j .

$$1. \quad x^6 + x^2 + x = (x^3 + x + 1)^2 + \underline{x + 1}, \quad j = 3.$$

Действительно,

$$\begin{aligned} w(\alpha) &= \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ &= \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1. \end{aligned}$$

$$\begin{aligned} 2. \quad x^6 + x^5 + x^3 + x^2 + x &= \\ &= (x^3 + x^2 + x + 1)(x^3 + x + 1) + \underline{x^2 + x + 1}, \quad j = 5; \end{aligned}$$

Действительно,

$$\begin{aligned} w(\alpha) &= \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha = \\ &= \alpha^2 + 1 + \alpha^5 + \alpha + 1 + \alpha^2 + \alpha = \alpha^5. \end{aligned}$$

$$3. \quad x^6 + x^3 + x^2 + x = (x^3 + x)(x^3 + x + 1) + \underline{0}, \quad \text{т. е.}$$

ошибки не произошло.

3.4. Имеем $\alpha^{31} = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\begin{aligned} &\{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}, \\ &\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}, \{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\}, \\ &\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}, \{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\}, \\ &\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}. \end{aligned}$$

3.5. Будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов данного поля со с. 45.

С её помощью вычислим синдромы:

$$\begin{aligned} s_1 = w(\alpha) &= \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\ &= (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\ &= \alpha^3 + \alpha + 1 = \alpha^7, \end{aligned}$$

$$s_2 = w(\alpha^2) = (w(\alpha))^2 = \alpha^{14},$$

$$s_3 = w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0,$$

$$s_4 = w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{28} = \alpha^{13}.$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7x + 1.$$

Решим удовлетворяет соотношению Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \quad \deg \lambda(x) \leq 2.$$

с помощью расширенного алгоритма Евклида:

$$\begin{aligned} \text{Шаг 0. } r_{-2}(x) &= x^5, \\ r_{-1}(x) &= \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7x + 1, \\ \sigma_{-2}(x) &= 0, \\ \sigma_{-1}(x) &= 1. \end{aligned}$$

$$\begin{aligned} \text{Шаг 1. } r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= \alpha^2x, \\ r_0(x) &= \alpha x^3 + \alpha^9x^2 + \alpha^2x, \\ \sigma_0(x) &= \sigma_{-2}(x) - \sigma_{-1}(x)q_0(x) = \\ &= -q_0(x) = \alpha^2x. \end{aligned}$$

$$\begin{aligned}
 \text{Шаг 2. } r_{-1}(x) &= r_0(x)q_1(x) + r_1(x), \\
 q_1(x) &= \alpha^{12}x + \alpha^5, \\
 r_1(x) &= \alpha^{14}x^2 + 1, \\
 \deg r_1(x) &= 2 \leq r, \\
 \sigma_1(x) &= \sigma_{-1}(x) - \sigma_0(x)q_1(x) = \\
 &= 1 + \alpha^2x(\alpha^{12}x + \alpha^5) = \\
 &= \underbrace{\alpha^{14}x^2 + \alpha^7x + 1}_{\text{полином локаторов ошибок}} = \sigma(x).
 \end{aligned}$$

3.6. Найдём корни (их 2, полином квадратный) полинома локаторов ошибок полным перебором.

Для вычислений удобно пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной в предыдущей задаче.

$$\begin{aligned}
 \sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3, \\
 \sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3, \\
 \sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha, \\
 \sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1, \\
 \sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = \mathbf{0}, \\
 \sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1, \\
 \sigma(\alpha^7) &= \alpha^{16} + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1, \\
 \sigma(\alpha^8) &= \alpha^{18} + \alpha^{14} + 1 = \mathbf{0}.
 \end{aligned}$$

Дальше можно не вычислять: оба корня $\sigma(x)$ найдены. Итак, данный полином локаторов ошибок имеет корни α^5 и α^8 . Определяем позиции ошибок:

$$-5 \equiv_{15} 10, \quad -8 \equiv_{15} 7.$$

3.7. Имеем $n = 31 = 2^5 - 1$, $q = 5$, $d_c - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $C_1 = \{ \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16} \}$.

Нетрудно установить, что эти классы также будут пятиэлементными:

$$C_2 = \{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17} \};$$

$$C_3 = \{ \alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18} \}.$$

На с. 33 были приведены неприводимые многочлены 5-й степени над \mathbb{F}_2 : их шесть —

- | | |
|--------------------------------|----------------------------------|
| 1) $x^5 + x^2 + 1$, | 4) $x^5 + x^4 + x^2 + x + 1$, |
| 2) $x^5 + x^3 + 1$, | 5) $x^5 + x^4 + x^3 + x + 1$, |
| 3) $x^5 + x^3 + x^2 + x + 1$, | 6) $x^5 + x^4 + x^3 + x^2 + 1$. |

Во многих монографиях¹³⁾ есть соответствующие таблицы. В этих таблицах указано, что все эти многочлены являются примитивными, то есть все они могут быть выбраны в качестве порождающего поле полинома $a(x)$.

Положим $a(x) = x^5 + x^3 + 1$ (многочлен № 2) и тогда $g(x) = a(x)$, $\alpha^5 = \alpha^3 + 1$, $\alpha^{31} = 1$.

Определим, какие из остальных многочленов соответствуют циклотомическим классам для α^3 и α^5 .

Имеем:

¹³⁾ например, [2], Том 1, Таблица С.

для многочлена № 3 —

$$(x^5 + x^3 + x^2 + x + 1) \Big|_{x=\alpha^3} = \alpha^{15} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = \\ = (\alpha^3 + 1)^3 + \alpha^4(\alpha^3 + 1) + \alpha(\alpha^3 + 1) + \alpha^3 + 1 = \dots = 0,$$

для многочлена № 5 —

$$(x^5 + x^4 + x^3 + x + 1) \Big|_{x=\alpha^5} = \alpha^{25} + \alpha^{20} + \alpha^{15} + \alpha^5 + 1 = \\ = (\alpha^3 + 1)^5 + (\alpha^3 + 1)^4 + (\alpha^3 + 1)^3 + \alpha^5 + 1 = \dots = 0.$$

Таким образом,

$g_2(x) = x^5 + x^3 + x^2 + x + 1$, $g_{\alpha^5}(x) = x^5 + x^4 + x^3 + x + 1$
и порождающий многочлен для (31, 16, 7)-кода БЧХ
есть

$$g(x) = g_1(x) \cdot g_2(x) \cdot g_3(x) = \\ = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1, \\ \deg g(x) = m = 15, k = n - m = 16.$$

3.8. Для вычислений в поле F нам понадобится таблица, уже построенная на с. 45.

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = (\alpha^3 + \alpha^2) x + 1 : \\ \sigma(\alpha) = \alpha^4 + \alpha^3 + 1 = \alpha + 1 + \alpha^3 \neq 0; \\ \sigma(\alpha^2) = \alpha^5 + \alpha^4 + 1 = \alpha^2 + \alpha + \alpha + 1 + 1 = \alpha^2 \neq 0; \\ \dots \dots \\ \sigma(\alpha^9) = \alpha^{12} + \alpha^{11} + 1 = \\ = (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 = \mathbf{0}.$$

Линейный полином $\sigma(x)$ имеет один корень α^9 , и поэтому позиция единственной ошибки есть $-9 \equiv_{15} 6$.

Список литературы

1. Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.
2. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. — М.: Мир, 1988.
3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.
4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. — М.: Мир, 1976.
5. Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.
6. Токарева Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.
7. Применко Э. А. Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.