МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМЕНИ М. В. ЛОМОНОСОВА
Факультет Вычислительной математики и
кибернетики
кафедра Математических методов прогнозирования

Конспект лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

алгебраические основы кодирования и шифрования

группы 320–325, 327, 328
осенний семестр 2019/2020 уч. года

Лектор — доцент к.ф.-м.н. *С. И. Гуров*
ассистент *Д. А. Кропотов*

2019

Оглавление

Глава 1

Классические алгебраические структуры

1.1 Группы

Определения и примеры групп

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

$\left[0)\right.$ $x \circ y \in G$ — *устойчивость* носителя;$\left.\right]$

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 обратных элементов* ко всем $x \in G$.

При отсутствии неясностей, группы обозначают $\langle G, \circ \rangle$ или[1)] просто символом носителя G.

[1)] как и все прочие алгебраические системы

Вместо $\circ$ во многих случаях пишут $\cdot$, или этот символ вообще опускают (*мультипликативная запись* групповой операции), обратный к x элемент обозначают x^{-1}, нейтральный называют *единицей*, и когда группа имеет числовой характер, обозначают последний символом 1.

Степень элемента при мультипликативной записи:

$$a^0 = e,\ a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ символов } a},\ n \in \mathbb{N},$$

при которой справедливы обычные свойства степени:

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

Если $|G| = n$, то G — *конечная группа* и n — её *порядок*, противном случае группа *бесконечная*.

В конечной группе небольшого порядка групповую операцию удобно задавать *таблицей умножения* (*таблицей Кэли*).

Пример 1.2. Таблица умножения группы 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 1.3. 1. Четверная группа Клейна абелева.

2. *Числовые группы* — все они абелевы:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *сложения*.
- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$, то есть все целые, кратные $n \in \mathbb{N}_0$. — абелева группа по сложению.
- *Ненулевые* элементы множеств $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — группы относительно *умножения*.

3. *Бинарные наборы* $\widetilde{\alpha} = (\alpha_1, \dots, \alpha_n) \in \{0,1\}^n = B^n$ (*единичный куб*) относительно покомпонентной суммы по $\bmod 2$ — абелева группа, её нуль — $\widetilde{0} = (0, \dots, 0)$.

4. *Симметрическая группа* S_n — все перестановки элементов линейно упорядоченного n-элементного множества X относительно композиции $(*)$ перестановок. Нейтральный элемент S_n — единичная перестановка 1_X. Ясно, что $|S_n| = n!$.

Легко показывается, что S_n *не абелева при* $n > 2$: пусть $X = \{1,2,3\}$ и для S_3 получим[2)]

$$(1,2,3) * (2,3) = (1,2) \neq (1,3) = (2,3) * (1,2,3).$$

Прямой суммой $H \oplus G$ абелевых групп H и G называется группа, определённая на носителях H и G с заданным покомпонентно операцией сложения:

$$(h_1, g_1) + (h_2, g_2) = (h_1 + h_2, g_1 + g_2),$$
$$h_1, h_2 \in H,\ g_1, g_2 \in G.$$

Ясно, что прямая сумма — абелева группа.

Может оказаться, что для элемента a группы $\langle G, \cdot, e\rangle$ при некотором $n > 0$ справедливо

[2)] Перестановки записываются в виде из разложения на циклы (в данном случае имеем одноцикловые перестановки), сначала выполняется 2-я перестановка, потом — 1-я.

$$a^n = e.$$

Тогда наименьшее такое n называют *порядком* этого элемента, символически $\operatorname{ord} a$; иначе данному элементу приписывают бесконечный порядок. Например, в группе $G = \{\, 0, 1, 2, 3, 4, 5 \,\}$ и сложением по $\bmod 6$ в качестве групповой операции порядки элементов суть

$$\operatorname{ord} 1 = \operatorname{ord} 5 = 6, \quad \operatorname{ord} 2 = \operatorname{ord} 4 = 3, \quad \operatorname{ord} 0 = 1.$$

Подгруппы, смежные классы, изоморфизмы. 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 $H \leqslant G$.

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

Если a — элемент порядка n группы $\langle G, \cdot, e\rangle$, то он порождает в G подгруппу, обозначаемую $\langle a\rangle$:

$$\langle a\rangle = \{\, a, a^2, \ldots, a^{n-1}, a^n = a^0 = e \,\} \leqslant G.$$

Определение левого xH и правого Hx *смежных классов группы* $\langle G, \cdot, e\rangle$ *по подгруппе* H *с представителем* $x \in G$:

$$xH = \{\, x \cdot h \mid h \in H \,\}, \quad Hx = \{\, h \cdot x \mid h \in H \,\}.$$

Утверждение 1.4 (*о разложении группы на смежные классы*). *Левые смежные классы с разными представителями либо не пересекаются, либо совпадают и в совокупности составляют всю группу. То же справедливо и для правых смежных классов.*

Если $\forall\, x \in G$ всегда $xH = Hx$, то подгруппу H называют *нормальной*. Ясно, что, например, *в абелевой группе все подгруппы нормальны.*

Заметим, что независимо от выбора элементов $x \in aH$ и $y \in bH$ результат $x \circ y$ находится в $(a \circ b)H$. Поэтому операцию над элементами можно расширить до операции над смежными классами.

Определение 1.5. Множество смежных классов группы $\langle G, \circ \rangle$ по её нормальной подгруппе H, снабжённое операцией $\bullet$

$$(aH) \bullet (bH) = (a \circ b)H,$$

называется *факторгруппой*, символически G/H.

Допуская вольность речи, элементы факторгрупп числовых групп будем также называть числами.

Определение 1.6. Для групп $\langle G, \circ, e \rangle$ и $\langle G', \cdot, e' \rangle$ отображение $\varphi : G \to G'$ 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 $G \cong G'$.

Теорема 1.7 (*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.

Поскольку смежные классы группы по подгруппе либо не пересекаются, либо совпадают, то отображение $ah \leftrightarrow bh$, $h \in H \leqslant G \ni a, b$ является биекцией, откуда следует равномощность всех классов по данной подгруппе.

Теорема 1.8 (*Лагранж*). *Порядок подгруппы H конечной группы G делит порядок самой группы:*

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

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

Следствие. Порядок любого элемента конечной группы делит порядок группы.

Например, в 6-элементной группе S_3 перестановок множества $\{a, b, c\}$ нейтральный элемент имеет порядок 1, три транспозиции (ab), (ac), (bc) — порядок 2, и два 3-цикла (abc), (acb) — порядок 3.

Для коммутативных групп имеется усиление.

Теорема 1.9. *Пусть m — максимальный порядок элемента в конечной абелевой группе G. Тогда порядок любого элемента G делит m.*

Циклические группы. Если окажется, что *каждый* элемент группы C есть степень некоторого элемента a, то есть

$$C = \{\, a^n \mid a \in C,\, n \in \mathbb{Z} \,\},$$

то такая группа называется *циклической*, а сам элемент a — *порождающим* (*образующим, генератором*), символически $\langle a \rangle = C$.

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

Пример: группа $\left\langle \frac{2\pi}{n} \right\rangle$ поворотов n-угольника вокруг своего центра на указанный угол — циклическая.

Для циклических групп возможны два случая.

1. *Порождающий элемент a имеет бесконечный порядок* — тогда группа бесконечна и состоит из элементов

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

то есть она изоморфна группе $\langle\, \mathbb{Z},\ +,\ 0\,\rangle$ целых чисел *по сложению*. В ней два генератора: -1 и $+1$.

2. *Порождающий элемент a имеет конченый порядок n*, и тогда получаем конечную абелеву группу

$$C = \langle a \rangle \ \text{ и } \ \operatorname{ord} a = |C| = n.$$

Данная группа, очевидно, изоморфна аддитивной группе

$$\langle\, \{0, 1, \ldots, n-1\},\ +,\ 0\,\rangle = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z},$$

в которой результат сложения берётся по $\bmod n$.

Итак, любая бесконечна циклическая группа изоморфна $\mathbb{Z}$, а конечная порядка n изоморфна $\mathbb{Z}_n$, откуда следует, что *все конечные циклические группы одного порядка изоморфны друг другу*.

Ясно, что в $\mathbb{Z}_n$ все элементы порядка n суть порождающие. Поэтому их число совпадает с количеством натуральных чисел, взаимно простых с n.

Значение *функции Эйлера* $\varphi(n)$ натурального аргумента n — количество чисел из интервала $[\,1,\ \ldots,\ n-1\,]$, взаимно простых с n и, по определению, $\varphi(1) = 1$.

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

Ясно, что циклическая группа порядка n имеет ровно $\varphi(n)$ порождающих элементов.

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
$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$
— *мультипликативность* функции Эйлера;
- $\sum\limits_{d|n} \varphi(d) = n$;
- при $n > 2$ значения функция Эйлера чётные, и, следовательно, $\varphi(n) > 2$.

Иллюстрация свойств:

$$\varphi(12) = \varphi(2^2 \cdot 3) = 2^1 \cdot 1 \cdot 2 = 4,$$
$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8,$$
$$\varphi(16) = \varphi(2^4) = 2^3 \cdot \varphi(2) = 8,$$
$$\varphi(36) = \varphi(4 \cdot 9) = 2^1 \cdot 1 \cdot 3^1 \cdot 2 = 12,$$
$$\varphi(99) = \varphi(3^2 \cdot 11) = 3 \cdot 2 \cdot 10 = 60,$$

$n = 6$, $D(6) = \{\, 1, 2, 3, 6 \,\}$ — множество делителей 6,

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

1.2 Кольца и поля

Кольца: определение, основные свойства

Определение 1.10. 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*

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

$\varphi(n)$	+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

Дистрибутивные законы обеспечивают тот факт, что нейтральный элемент по сложению 0 будет являться одновременно нулём по умножению: $\forall x \in R : x \cdot 0 = 0$[3)].

Отметим, что в кольце деление не постулируется. Классический пример кольца — целые числа $\mathbb{Z}$ с обычными операциями сложения и умножения.

- Важный случай — *ассоциативно-коммутативные кольца* с указанными свойствами операции умножения.
- Если в кольце имеется нейтральный элемент 1 по умножению ($x \cdot 1 = 1 \cdot x = x$), то кольцо называется *кольцом с единицей* или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$.

[3)] Поэтому любую аддитивную группу G можно превратить в кольцо, если задать на ней нулевое умножение: $\forall x, y \in G : x \cdot y = 0$.

- *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, что хотя бы один из сомножителей a и b равен 0.

  Кольцо квадратных матриц имеет делители нуля:
  $$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Определение 1.11. Нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля называется *целостным*.

Пример 1.12. 1. Кольцо $\mathbb{Z}$ целостно.

2. Кольцо чётных $2\mathbb{Z}$ — ассоциативно–коммутативное кольцо без единицы и делителей нуля.
3. Кольцо $\mathbb{Z}_n$, $n \geqslant 2$, унитально и ассоциативно–коммутативно, но нецелостно при составном n: например в $\mathbb{Z}_6$ получим $3 \cdot 2 = 0$.

В унитальном коммутативном кольце элементы a и b называют *обратимыми*, если
$$a \cdot b = 1$$
(случай $a = b$ не исключается). Например, в кольце целых $\mathbb{Z}$ обратимы порождающие элементы $+1$ и -1.

Совокупность всех обратимых элементов кольца R обозначают R^*. Ясно, что это группа по умножению.

Также понятно, что $\mathbb{Z}_n^*$ — суть числа, взаимно простые с n и всего их $\varphi(n)$. Например, в кольце $\mathbb{Z}_6$ обратимы только элементы 1 и 5.

Если p — простое число, то обратимы все ненулевые элементы кольца $\mathbb{Z}_p$, и $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Определение 1.13. Необратимый элемент p *целостного* кольца называется *неприводимым* или *неразложимым*, если из равенства $p = a \cdot b$ следует, что либо a, либо b обратимы.

Например, в кольце целых $\mathbb{Z}$ неразложимы только простые числа и противоположные к ним.

Определение 1.14. Целостное кольцо, в котором каждый ненулевой элемент либо обратим, либо однозначно с точностью до умножения на обратимые элементы представляется в виде произведения *неразложимых* элементов, называется *факториальным.* или *кольцом с однозначным разложением на множители.*

Классический пример факториального кольца — кольцо $\mathbb{Z}$: для любого целого n справедливо *примарное* (по простым) *разложение* $n = \pm 1 \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.

Кольцо $\left\{ m \pm i\sqrt{3} \mid m \in \mathbb{N} \right\}$ не факториально, т. к., например, число 4 имеет два представления в виде произведения неразложимых: $4 = 2 \cdot 2 = \left(1 + i\sqrt{3}\right) \cdot \left(1 - i\sqrt{3}\right)$.

Некоторое подмножество L кольца $\langle R, +, \cdot, 0 \rangle$ вновь окажется кольцом и будет его *подкольцом*, если L есть подгруппа *аддитивной группы* $\langle R, +, 0 \rangle$ и устойчиво относительно умножения.

Например, при любом $n \in \mathbb{N}_0$ множество $n\mathbb{Z}$ является подкольцом $\mathbb{Z}$.

Подкольцо *собственное*[4], если оно не совпадает со всем кольцом.

Идеалы колец и факторкóльца. Важнейшими подкольцами являются так называемые идеалы. Их роль в теории колец аналогична роли нормальных подгрупп в теории групп.

Определение 1.15. Подкольцо I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ называется его *(двусторонним) идеалом*, символически $I \lhd R$, если

$$\forall i \in I \, \forall r \in R : i \cdot r \in I.$$

Пример идеала в кольце $\mathbb{Z}$: все чётные числа $2\mathbb{Z}$.

Само кольцо и его нуль 0 — *тривиальные идеалы* кольца.

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

Определение 1.16. Идеал I, символически (a), унитального коммутативного кольца $\langle R, +, \cdot, 0, 1 \rangle$ называется *главным и порождённым элементом* $a \in R$, если

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

Легко видеть, что множество $I = \{ a \cdot r \mid r \in R \}$ действительно является идеалом.

Во-первых, замкнутость I относительно операций сложения и умножения очевидна, а дистрибутивность

[4] Кстати, термин *собственный* — неудачный перевод английского слова *proper*; следовало бы говорить *правильный* или *настоящий*.

умножения относительно сложения сохраняется. Таким образом, I — подкольцо R. Во-вторых, $x \in I \Leftrightarrow x = ua$, $y \in R \Rightarrow x \cdot y = uya \in I$.

Нулевой идеал всегда главный: $\{0\} = (0)$.

Целостные кольца, в которых все идеалы главные, называют *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 $\mathbb{Z}_n$ — любой ненулевой идеал содержит НОД своих ненулевых элементов и им порождается.
  Например, для $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$: $\mathbb{Z}_6 = (1)$, $\{0, 2, 4\} = (2)$, $\{0, 3\} = (3)$ и $\{0\} = (0)$.

Все КГИ факториальны.

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.

Определение 1.17. *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 1.18. В кольце $\mathbb{Z}$

- идеалы (2) и (3) максимальны;

- идеал (6) не максимален, так как он содержится и в идеале (2), и в идеале (3): любое число, делящееся на 6 делится также и на 2, и на 3.

Вывод: в $\mathbb{Z}$ максимальные идеалы имеют вид (p), где p — простое число.

Определение 1.19. *Классом вычетов по модулю идеала I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ с представителем $r \in R$*, символически $\overline{r}_I$, называют множество

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

Если идеал фиксирован, пишут просто $\overline{r}$.

Классы вычетов разных представителей по модулю данного идеала либо совпадают, либо не пересекаются и в объединении дают всё кольцо.

В качестве образующего класса вычетов $r + I$ может быть выбран любой элемент $r \in R \setminus I$, а остальные элементы данного класса вычетов получают сложением r с каждым элементом идеала по его модулю последнего.

Например, в кольце целых $\mathbb{Z}$ класс вычетов по идеалу (n) с представителем $0 \leqslant r \leqslant n - 1$ есть

$$\overline{r} = \{ r, r \pm n, r \pm 2n, \dots \} = r + n\mathbb{Z}$$

— 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 кольцевыми операциями над представителями, а результаты опера-

ций берутся по модулю идеала. При этом совокупность всех классов вычетов кольца R по модулю идеала I образуют *факторкольцо*, символически R/I.

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

$$\mathbb{Z}/(2) = \{\overline{0}, \overline{1}\} \cong \mathbb{Z}_2,$$

где $\overline{0}$ — все чётные числа, а $\overline{1}$ — все нечётные.

Факторкольцо по максимальному идеалу является полем. Поэтому $\mathbb{Z}_p$ при простом p есть поле.

Евклидовы кольца. В кольце целых $\mathbb{Z}$ возможно деление чисел друг на друга с остатком (когда делитель не 0). При этом остаток либо равен нулю (случай делимости нацело), либо его модуль строго меньше модуля делителя.

Желание обеспечить деление элементов в кольцах приводит к понятию евклидового кольца.

Определение 1.20. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$ называется *евклидовым*, если для каждого его *ненулевого* элемента a определена *норма* $N(a) \in \mathbb{N}$ такая, что для любого элемента $b \neq 0$ существуют такие элементы q и r, что

$$a = q \cdot b + r, \text{ и либо } r = 0, \text{ либо } N(r) < N(b).$$

В большинстве пособий на норму накладывается ещё одно требование — $N(a) \leqslant N(ab)$. Однако это условие носит технический характер: для такой нормы легче доказываются некоторые свойства евклидовых колец, и её легко получить из нормы, определённой выше. Основные же свойства евклидовых колец остаются в силе и без этого дополнительного свойства.

Пример 1.21.

- Классический пример евклидова кольца — *кольцо целых чисел* $\mathbb{Z}$; норма — абсолютная величина числа.
- Кольца многочленов от формальной переменной с коэффициентами из некоторого поля, евклидово, норма — степень многочлена.
  Например — кольцо $\mathbb{R}[x]$ многочленов с действительными коэффициентами.
- Кольцо *целых гауссовых чисел* $\mathbb{Z}[i]$ (комплексные числа, у которых и вещественная, и мнимая части целые); норма $N(a+ib) = a^2 + b^2$.

Все евклидовы кольца — КГИ.

Поля

Определение 1.22. Целостное кольцо, в котором все ненулевые элементы обратимы, называется *полем*.

Поле также можно определить как такую пятёрку $\langle K, +, \cdot, 0, 1 \rangle$, что её *редукты* $\langle K, +, 0 \rangle$ — абелева группа по сложению, а $\langle \{K \setminus \{0\}, \cdot, 1 \rangle = K^*$ — абелева группа по умножению, причём эти группы связаны 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 K образуют группу K^* относительно *умножения*, её называют *мультипликативной группой* данного поля;
2) факторкольцо R/I является полем если и только если идеал I кольца R *максимальный*.

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 — $\mathbb{Z}_p$, если p — простое число.

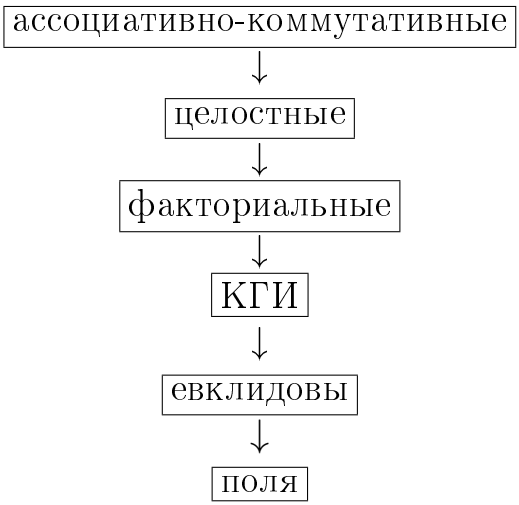
Поле, не обладающее никаким собственным подполем, называется *простым*.

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 1.23. *В каждом поле содержится только одно простое подполе, которое изморфно либо* $\mathbb{Q}$, *либо* $\mathbb{Z}_p$, p *— простое.*

Иерархия колец:



1.3 Векторные пространства, гомоморфизмы, сравнения

Абстрактные векторные пространства

Определение 1.24. *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* («числá») *из* K *на вектор из* V: $K \times V \xrightarrow{\cdot} V$,

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) $1 \cdot v = v$.

Пусть $V = K^n$ — *множество наборов длины* n элементов поля K. Сложение и умножение элементов из V на число из K определим покомпонентно. Получившаяся структура есть *линейное векторное пространство*, которое называют *n-мерным координатным пространством* над полем K.

Например, булев куб $B^n = \{0,1\}^n$ — n-мерное координатное пространство над полем $\mathbb{Z}_2 = \{0,1\}$ с операциями сложения $+$ и умножения $\&$ и нулевым элементом $\widetilde{0}$.

n-мерное координатное пространство V над полем K имеет *базис* из n векторов, например

$\boldsymbol{e}_1 = [\,1,\,0,\,\ldots,\,0\,], \ldots, \boldsymbol{e}_n = [\,0,\,0,\,\ldots,\,1\,]$ — базис. Линейная оболочка совпадает со всем пространством V, иными словами, любой вектор $\boldsymbol{x} \in V$ есть (единственная) линейная комбинация базисных векторов:

$$\boldsymbol{x} = \sum_{i=1}^{n} \alpha_i \boldsymbol{e}_i, \quad \alpha_i \in K,\ i = 1, \ldots, n.$$

Удаляя из базиса некоторые элементы и рассматривая соответствующую линейную оболочку, получаем *линейные подпространства* исходного пространства.

Если в приведённом выше определении «поле K» заменить на «кольцо R» (как правило — целостное) получим определение *модуля над* R, который сохраняет многие свойства векторного пространства.

Гомоморфизмы. Группы, кольца, поля, векторные пространства — примеры алгебраических структур (АС) различных типов.

Напомним частично уже нами использованную терминологию, связанную с взаимными отображениями однотипных структур. Пусть $\varphi : A \to B$ — отображение алгебраических систем. Элементы A, отображающиеся в нулевой вектор B образуют *ядро отображения* $\operatorname{Ker}\varphi$, а элементы B, в которые отображается хотя бы один вектор из A, составляют *образ отображения* $\operatorname{Im}\varphi$.

Гомоморфизмами называют непрерывные отображения между однотипными АС, сохраняющие, структуру образа, то есть основные операции (и основные отношения). Например, отображение φ кольца $\langle\, R,\, +,\, \cdot \,\rangle$ в кольцо $\langle\, R',\, \oplus,\, \otimes \,\rangle$ называется их *гомоморфизмом*, если для любых элементов $r_1, r_2 \in R$ справедливы равенства

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

Гомоморфизмами векторных пространств являются линейные отображения между ними. Если V_m и V_n — координатные пространства, то линейное отображение $\varphi : V_m \to V_n$ задаётся $n \times m$-матрицей.

В общем случае, однозначные (инъективные) гомоморфизмы АС называют *мономорфизмами* или *вложениями*. Символ мономорфизма — $\hookrightarrow$.

Эпиморфизмом называют сюръективной гомоморфизм (отображение «на»), а взаимно однозначный (биективный) гомоморфизм — *изоморфизмом*. Символ изоморфного отношения — $\cong$.

Изоморфизм АС в себя называют *автоморфизмом*. Ясно, например, что все автоморфизмы линейного векторного пространства образуют группу относительно операции их композиции.

Сравнения. Напомним, что сравнимость целых чисел a и b записывается формулой

$$a \equiv b \pmod{m}, \qquad \text{или } a \equiv_m b, \tag{1.1}$$

которая означает что a и b при делении на *модуль* m имеют один и тот же остаток. При фиксированном известном m допустима запись $a \equiv b$. Ясно, что (1.1) эквивалентно

$$a = b + mt, \quad a - b = mt, \qquad t \in \mathbb{Z}.$$

Сравнение обладает свойствами рефлексивности, симметричности и транзитивности, то есть является отношением эквивалентности.

Отметим основные свойства сравнений (все сравнения в 1) — 3) — по единому модулю):

1) $\left\{ \begin{array}{l} a \equiv b \\ c \equiv d \end{array} \right. \Rightarrow \left\{ \begin{array}{l} a + c \equiv b + d, \\ a \cdot c \equiv b \cdot d \end{array} \right.$;

2) к обеим частям сравнения можно прибавить одно и то же число c:

$$a \equiv b \;\Rightarrow\; a + c \equiv b + c;$$

3) можно перенести число из одной части сравнения в другую со сменой знака:

$$a \equiv (b + c) \;\Leftrightarrow\; (a - c) \equiv b.$$

4) можно делить обе части сравнения на число, взаимно простое с модулем:

$$\begin{cases} ad \equiv_m bd, \\ \text{НОД}\,(d, m) = 1 \end{cases} \;\Rightarrow\; a \equiv_m b;$$

5) можно одновременно разделить обе части сравнения и модуль на их общий делитель:

$$ac \equiv_{mc} bc \;\Rightarrow\; a \equiv_m b.$$

1.4 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) нелые 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 $1, 2, \ldots, n$ 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 $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений?

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

1.3. Вычислите функцию Эйлера для:

а) 375; б) 720; в) 988.

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

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

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

1.6. 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?

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

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

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

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

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

Глава 2

Конечные кольца и поля

2.1 Поля Галуа

Простые поля Галуа — поля классов вычетов

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

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

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 $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ — *поле*. Его называют *простым полем Галуа* и обозначают $\mathbb{F}_p$ или $GF(p)$[1)]. Вообще

[1)] В честь Эвари́ста Галуа́ (Evariste Galois, 1811–1832); первым обозначением обычно пользуются математики, а вторым — специалисты по информатике.

полем Галуа называют любое конечное поле.

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

$\mathbb{F}_3$:

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

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/(4)$:

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

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Заметьте, в факторкольце $\mathbb{Z}/(4)$ имеем $2 \times 2 = 0$[2)], однако поле из 4-х элементов существует...

Характеристика поля. Пусть K — какое-либо поле. Будем складывать его единицы. В конечном поле всегда найдётся наименьшее p такое, что

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

Это значение p (порядок аддитивной группы поля K) называют *характеристикой поля* и обозначают $\mathrm{char}\ K$.

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

[2)] Говорят, что элемент 2 есть *нильпотент индекса 2* в кольце $\mathbb{Z}/(4)$.

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

Ясно, что $\{0, 1, \ldots, p-1\} \cong \mathbb{Z}_p$ — минимальное подполе любого поля K характеристики $p > 0$.

Существуют и бесконечные поля положительной характеристики.

Таким будет, например, поле $K(x)$ *рациональных функций* над конечном полем K, элементами которого являются "дроби" P/Q, где P и Q $(Q \neq 0)$ — 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.

Если в качестве K взять $\mathbb{F}_p$, то $\mathbb{F}_p(x)$ — *бесконечное поле положительной характеристики* p.

Будем рассматривать далее исключительно конечные поля.

В конечном поле возможно сильное упрощение вычисления степеней сумм.

Теорема 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 степени бинома

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

в которой при $i = 1, \ldots, p-1$ числители коэффициентов $C_p^i = \frac{p!}{i!\cdot(p-i)!}$ делятся на p, а знаменатели — нет, и поэтому все они равны $0 \pmod p$. □

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. В соответствии с введенным на с. 13 обозначением, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ — мультипликативная группа q-элементного поля Галуа $\mathbb{F}_q$.

Теорема 2.2. *$\mathbb{F}_q^*$ — циклическая по умножению группа порядка $q-1$.*

Доказательство. При $q = 2$ утверждение теоремы тривиально; считаем далее, что $q > 2$.

Поскольку $|\mathbb{F}_q^*| = q-1$ и порядок любого элемента x конечной группы делит порядок группы, или $x^{q-1} = 1$, то все её элементы удовлетворяют уравнению

$$f(x) = x^{q-1} - 1 = 0.$$

Но у многочлена $f(x)$ не более $q-1$ корней, следовательно, все элементы $\mathbb{F}^*$ — его корни. Один из них — 1. Но так как $\varphi(q) > 2$, то в $\mathbb{F}_q^*$ существует ещё один элемент такой, что его порядок совпадает с порядком группы. □

Поскольку все конечные циклические группы одного порядка изоморфны друг другу, получаем, что, в частности, мультипликативная группа $\mathbb{F}_p^*$ изоморфна группе $\mathbb{Z}_{p-1}$ (по сложению).

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

$$\mathbb{F}_q = \Big\{ 0, \underbrace{\alpha, \alpha^2, \ldots, \alpha^{q-2}, \overbrace{\alpha^{q-1}}^{=\alpha^0} = 1}_{\mathbb{F}_q^*} \Big\}.$$

Найдём примитивные элементы поля $\mathbb{F}_{11}$; их должно быть $\varphi(10) = 4$. Проверяем элемент 2:

k	1	2	3	4	5	6	7	8	9	10
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

— мы перебрали все ненулевые элементы поля, и поэтому элемент 2 — примитивный. Проверяем 3:

k	1	2	3	4	5
$3^k \pmod{11}$	3	9	5	4	1

— то есть $\operatorname{ord} 3 = 5 \neq 10$ и 3 — не примитивный.

Как ускорить процесс нахождения примитивных элементов простого поля Галуа?
Если примарное разложение числа $p-1$

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

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

Примеры: 1) $p = 11$ (наш случай), $p-1 = 10 = 2 \cdot 5$, проверяем степени $t = 2, 5$ элементов $\mathbb{F}_{11}^*$:

$2^2 = 4 \neq 1,\ 2^5 = 10 \neq 1 \ \Rightarrow\ 2$ — *примитивный*,

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

2) Для $GF(37)$ имеем $p-1 = 36 = 2^2 \cdot 3^2$. 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*, то эффективных алгоритмов не найдено; используют заранее составленные 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 $p-1 = |\mathbb{F}_p^*|$. В нашем примере 2 — примитивный элемент $\mathbb{F}_{11}$, $k \in \{1, 3, 7, 9\}$ — взаимно простые с 10 и получим

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6,$$

то есть 6, 7 и 8 — также примитивные элементы $\mathbb{F}_{11}$:

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 128 \equiv_{11} 7, \quad 2^9 = 512 \equiv_{11} 6.$$

Кольца многочленов: деление, корни. Легко видеть, что множество всех многочленов с коэффициентами из некоторого поля K образует коммутативное евклидово кольцо, обозначаемое $K[x]$ и называемое *кольцом многочленов над* K.

Далее будем рассматривать кольца многочленов $\mathbb{F}_p[x]$ над простыми полями Галуа $\mathbb{F}_p$. На рис. 2.1 приведён пример деления «уголком» многочленов над $\mathbb{F}_2$.

Корнем многочлена $f(x) \in K[x]$ называется такой элемент $a \in K$, что $f(a) = 0$.

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

Рис. 2.1. Пример деления многочленов из $\mathbb{F}_2[x]$.

Из разложения для многочленов

$$f(x) = (x-a)\cdot q(x) + r, \quad r \text{ — константа},$$

следует, что a — корень $f(x)$ если и только если $x-a$ делит $f(x)$. Как следствие получаем, что многочлен степени n имеет не более n корней.

Неприводимые многочлены

Определение 2.3. Многочлен над некоторым 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 нормированные неприводимые многочлены в кольцах $\mathbb{F}_p[x]$, то есть вида

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$
$$a_i \in \mathbb{F}_p,\ i = \overline{0, n-1} \quad \deg f(x) = n.$$

Найдём все неприводимые многочлены степеней от 2 до 5 над $\mathbb{F}_2$.

Вторая степень: $x^2 + ax + b$.

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$, то есть 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

$$a + b = 1 \ \Leftrightarrow\ \text{либо } a = 0 \text{ и } b = 1,\ \text{либо } a = 1 \text{ и } b = 0.$$

Проверкой устанавливаем, что оба эти варианта подходят и 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	$x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$ — *приводим*
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

$$a + b + c + d = 1$$

— получаем 8 вариантов. Далее исключая делимость на неприводимые многочлены 2 и 3-й степеней (их один и два соответственно, а их произведения дают два многочлена) находим 6 неприводимых многочленов 5-й степени:

$$x^5 + x^2 + 1, \qquad x^5 + x^3 + 1,$$
$$x^5 + x^3 + x^2 + x + 1, \qquad x^5 + x^4 + x^2 + x + 1,$$
$$x^5 + x^4 + x^3 + x + 1, \qquad x^5 + x^4 + x^3 + x^2 + 1.$$

Теорема 2.4 (о существовании неприводимых многочленов). *Для любых натурального n и простого p в $\mathbb{F}_p[x]$ существует неприводимый многочлен степени n.*

— докажем позже (см. с. 59).

Отметим, что для нахождения неприводимых многочленов в $\mathbb{F}_p[x]$ *нет эффективных алгоритмов*, а задача факторизации многочленов значительно более сложна, чем для чисел.

Расширения простых полей. С помощью идеалов неприводимых многочленов над простыми полями можно строить *новые конечные поля*, *расширения* последних.

Для этого в кольце многочленов $\mathbb{F}_p[x]$ нужно выбрать некоторый неприводимый многочлен $a(x)$ и построить факторкольцо $\mathbb{F}_p[x]/(a(x))$ по модулю его идеала. Элементы этого факторкольца суть совокупности $\overline{r(x)}$ многочленов, дающих при делении на $a(x)$ остаток $r(x)$. Если $\deg a(x) = n$, то степени всех таких многочленов не выше $n-1$, то есть таких остатков p^n.

Построенное факторкольцо *будет являться полем* относительно сложения и умножения вычетов по модулю $(a(x))$, поскольку кольцо $\mathbb{F}_p[x]$ евклидово, а идеал $(a(x))$ — максимальный[3)].

Данное поле обозначают $\mathbb{F}_p^n$ и называют *расширением n-й степени* простого поля $\mathbb{F}_p$. Альтернативные обозначения: $GF(p^n)$, $GF(q)$, $q = p^n$.

Может возникнуть вопрос: *почему в обозначении*

[3)] Иногда говорят, что элементы $f, g \in \overline{r(x)}$ *сравнимы по двойному модулю* — p и $a(x)$:

$$a(x), f(x), g(x) \in \mathbb{F}_p[x], \quad f(x) \equiv_{a(x)} g(x).$$

поля $\mathbb{F}_p^n$ не используется многочлен $a(x)$, с помощью которого оно построено? Потому, что любые два поля, содержащие p^n элементов, изоморфны (будет показано позже). Таким образом, для построения расширения $\mathbb{F}_p^n$ простого поля $\mathbb{F}_p$ может быть выбран *любой неприводимый в $\mathbb{F}_p[x]$ многочлен n-й степени.*

Пример 2.5. 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

$$\mathbb{F}_3^2 \cong \mathbb{F}_3[x]/\big(x^2+1\big) = \\ = \big\{\,\overline{0},\,\overline{1},\,\overline{2},\,\overline{x},\,\overline{x+1},\,\overline{x+2},\,\overline{2x},\,\overline{2x+1},\,\overline{2x+2}\,\big\}.$$

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

$$\overline{x+1}+\overline{x+2} = \overline{2x}, \qquad \overline{x}\cdot\overline{2x} = \overline{4} = \overline{1},$$
$$\overline{2x+1}+\overline{x} = \overline{1}, \quad \overline{2x+1}\cdot\overline{x} = \overline{x+1}, \quad \text{и т. д.}$$

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

Пример 2.6. В кольце $\mathbb{R}[x]$ многочленов с действительными коэффициентами возьмём неприводимый многочлен x^2+1 и построим поле

$$\mathbb{R}[x]/(x^2+1) = \{\,ax+b \mid a,b\in\mathbb{R},\ x^2=-1\,\}.$$

Заменяя x на i получим привычное обозначение для элементов поля $\mathbb{C}$ комплексных чисел.

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 $(a - kb, b)$, то вместо $a - kb$ можно взять остаток r, $0 \leqslant r < b$, 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 НОД $(a, b) = r$.

Алгоритм Евклида[4] *нахождения НОД* (a, b), $a \geqslant b$, $a, b \in \mathbb{N}$

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

Пример 2.7. Найдём НОД $(252, 105)$ по алгоритму Евклида.

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

[4] дважды описан в «Началах» Евклида, но не был им открыт: упоминается в «Топике» Аристотеля, появившейся на 50 лет ранее «Начал»

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

Теорема 2.8 (соотношение Безу[5]). *Для любых натуральных a, b и $d = НОД(a,b)$ найдутся целые коэффициенты Безу x, y такие, что*

$$d = ax + by.$$

Доказательство. Остаток r от деления целых u на v выражается их линейной комбинацией $r = u + (-q)v$. Это справедливо для каждого шага алгоритма Евклида, откуда следует указанное представление. □

Замечание. Коэффициенты Безу могут быть выбраны неоднозначно, например

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

Обобщённый (расширенный) алгоритм Евклида находит по двум *натуральным числам* a *и* b, $a \geqslant b$, их *натуральный* НОД d и два *целых* коэффициента Безу x, y таких, что $|x| < |b/d|$, $|y| < |a/d|$.

Обобщённый алгоритм Евклида решения соотношения $ax + by = d$, $a, b \in \mathbb{N}$, $a \geqslant b$ в кольце $\mathbb{Z}$

0. Зададим матрицу $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ и $r = b$.

[5] Для взаимно простых чисел открыто Клодом Гаспаром Баше (Bachet de Mezeriac Gaspar Klod, 1581–1638) и опубликовано в 1624 г., за 106 лет до рождения Этьена Безу (Etienne Bezout, 1730–1783), который обобщил данное соотношение на кольцо многочленов (см. с. 43). Онлайн-калькулятор коэффициентов соотношения Безу доступен по адресу *http://wims.unice.fr/wims/wims.cgi*.

1. Перевычислим r как остаток от деления чисел a на b: $a = bq + r$, $0 \leqslant r < b$.

   Если $r = 0$, то второй столбец матрицы E дает вектор $[x,\ y]^T$ решений заданного соотношения, а d есть последнее ненулевое значение r.

2. Иначе заменим матрицу E матрицей

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

3. Заменим пару чисел (a, b) парой (b, r) и перейдем к шагу 1.

Пример 2.9. Обобщённым алгоритмом Евклида найдём натуральное d и целые x и y такие, что

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

0. Зададим $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ и $r = 105$.

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

2. Заменяем матрицу E матрицей

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

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

4. Вычисляем $r = 105 - 42 \cdot 2 = 21 \neq 0$.

5. Заменяем матрицу E матрицей

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

6. Заменям 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 $d = 21$.

Действительно, $252 \cdot (-2) + 105 \cdot 5 = -504 + 525 = 21$.

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

Обобщённый алгоритм Евклида GE-InvZm нахождения элемента c^{-1}, обратного к c в кольце $\mathbb{Z}_m$ при условии НОД$(c, m) = 1$ (что гарантирует существование решения).

1. Запишем исходные данные в виде двухстрочной таблицы

$$\begin{array}{rr} m & 0 \\ c & 1 \end{array}$$

2. Вычислим частное q от деления друг на друга элементов первого столбца, то есть m на c: $m = q \cdot c + r$, $0 \leqslant r < c$.

3. Вычтем из 1-й строки 2-ю, домноженную на q и запишем результат в качестве 3-й строки таблицы.

4. Проводим аналогичные действия с двумя последними строками таблицы, пока в очередной строке не получим первый элемент 0. Тогда второй элемент *предпоследней* строки есть c^{-1}.

Пример 2.10. Решим в поле $\mathbb{Z}/(101)$ сравнение

$$4y = 1.$$

Применим алгоритм GE-InvZm, для удобства нумеруя строки и записывая значения частных и вычитаемые строки:

1	101	0	
2	4	1	$q = 25 \quad (\ 100\ 25\ )$
3	1	$\mathbf{-25}$	$q = 4$
4	0		

Найдено $y^{-1} = -25 \equiv_{101} 76$.
Действительно, $76 \cdot 4 = 304 = 3 \cdot 101 + 1$.

Алгоритм Евклида и его обобщённая версия позволяет решить относительно $y(x)$ соотношения вида

$$b(x) \cdot y(x) = d(x) \pmod{a(x)}, \tag{2.1}$$

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

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

$$a(x) \cdot \chi(x) + b(x) \cdot y(x) = d(x), \tag{2.2}$$

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 обобщённым алгоритмом Евклида соотношения (2.2) позволяет вычислить обратный к $y(x)$ элемент в поле $\mathbb{F}_p[x]/(a(x))$.

Ясно, что при этом нет необходимости вычислять $\chi_i(x)$, т. к. нас интересует только значения $y_i(x)$, $i = 0, 1, \ldots$. Удобна следующая форма алгоритма.

Обобщённый алгоритм Евклида GE-InvP нахождения в кольце $\mathbb{F}_p[x]/(a(x))$ элемента $y(x)$, обратного к $b(x)$, $\deg a(x) \geqslant \deg b(x)$, НОД $(a(x), b(x)) = 1$.

Шаг 0. Задаём начальные значения:
$r_{-2}(x) = a(x),\ r_{-1}(x) = b(x)$,
$y_{-2}(x) = 0,\ y_{-1}(x) = 1$.

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 2.11. Найдём $\bigl(x^2+x+3\bigr)^{-1}$ в поле

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

Для этого обобщённым алгоритмом Евклида решим соотношение Безу

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

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

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

Шаг 2: $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
$q_1(x) = 4x$,
$r_1(x) = \mathbf{3}, \quad \deg r_1(x) = 0$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) =$
$= 1 + 4x\bigl(x^2+5\bigr) = 4x^3+6x+1$.

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

2.3 Поля Галуа как векторные пространства

Поле $GF(p^n)$ построенно как факторкольцо $\mathbb{F}_p[x]/\,(a(x))$ кольца $\mathbb{F}_p[x]$ по модулю неприводмого многочлена $a(x)$ степени n и его элементами являются многочлены над $GF(p)$ степени не выше n:

$$GF(p^n) = \left\{ b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} \mid b_i \in GF(p),\ i = \overline{0, n-1} \right\}.$$

Установим взаимнооднозначное сооветствие между многочленами из $GF(p^n)$ и векторами из координатного пространства над $GF(p)$

$$b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} \ \leftrightarrow\ [\, b_0,\, b_1, \ldots\, b_{n-1}\,].$$

Отсюда следует, что поле $GF(p^n)$ можно рассматривать как n-мерное координатное векторное пространство над простым полем Галуа $GF(p)$.

Базисом этого пространства являются векторы

$$[\,1,\,0,\,0,\,\ldots,\,0\,], [\,0,\,1,\,0,\,\ldots,\,0\,], \ldots, [\,0,\,0,\,\,0,\,\ldots,\,1\,]$$

или же, переходя к многочленам —

$$1,\ x,\ \ldots,\ x^{n-1}.$$

Далее, легко установить, что для каждых 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.

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

степень α $\qquad\qquad$ $\alpha^4 = \alpha + 1$	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
$\alpha^{10} = \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2$	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 перемножить x^3+x+1 на x^2+x+1. Используя таблицу это сделать значительно легче, чем прямым перемножением многочленов:

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

Теорема 2.12. *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 $K_2 = \mathbb{F}_p^n$. 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. □

2.4 Корни многочленов над конечным полем

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

Определение 2.13. *Минимальным многочленом (м. м.)* элемента $\beta \in \mathbb{F}_p^n$ называется нормированный многочлен $m_\beta(x) \in \mathbb{F}_p[x]$ 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

$$a(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Убедимся, что многочлен $a_n^{-1}a(x)$ — минимальный для элемента $x = [\,0,\,1,\,0,\,\ldots,\,0\,] \in F$.

Во-первых, x — корень $a(x)$, а значит и корень $a_n^{-1}a(x)$.

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

$$b(x) \;=\; b_0 + b_1 x + \ldots + b_{n-1}x^m \;=\; 0,$$

то это означает линейную зависимость между элементами базиса $1,\ x,\ \ldots,\ x^{n-1}$ поля F, что невозможно.

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

Теорема 2.14. *Для каждого элемента β поля $\mathbb{F}_p^n$ существует м. м. и его степень не превосходит n.*

Доказательство. Рассмотрим элементы $1,\ \beta,\ \beta^2,\ \ldots,\ \beta^n$ 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 $c_0,\ \ldots,\ c_n$, что

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

Поэтому β — корень многочлена

$$c(x) = c_0 + c_1 x + \ldots + c_n x^n.$$

М. м. для β будет некоторый нормированный неразложимый делитель $c(x)$. □

Теорема 2.15. *Минимальные многочлены неразложимы.*

Доказательство. Пусть $m_\beta(x)$ — м. м. для β и

$$m_\beta(x) = m_1(x) \cdot m_2(x),$$

где $m_1(x)$ и $m_2(x)$ — не константы. 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. □

Теорема 2.16. *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:

$$f(x) = q(x) \cdot m_\beta(x) + r(x), \quad 0 \leqslant \deg r(x) < \deg m_\beta(x).$$

Подставляя в это равенство β вместо x, получаем

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

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

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, то есть эти многочлены совпадают.

Определение 2.17. Минимальный многочлен примитивного элемента поля называется *примитивным многочленом.*

Ясно, что данный нормированный неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$ примитивен, если x — порождающий элемент мультипликативной группы поля $\mathbb{F}_p[x]/(f(x))$.

Пример 2.18. 1. Многочлен

$$a(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$$

неприводим, нормирован, но не примитивен для своего корня x, поскольку x не является порождающим элементом мультипликативной группы поля $\mathbb{F}_2[x]/(a(x))$: в этом поле

$$\begin{aligned} x^4 &= x^3 + x^2 + x + 1, \\ x^5 &= x^4 + x^3 + x^2 + x = \\ &= (x^3 + x^2 + x + 1) + x^3 + x^2 + x = 1, \\ &\text{и } \operatorname{ord} x = 5. \end{aligned}$$

2. Для своего корня x многочлен

$$b(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$$

примитивен, поскольку он неприводим, нормирован и x является порождающим элементом мультипликативной группы поля $\mathbb{F}_2[x]/(b(x))$: легко проверить, что в этом поле $\operatorname{ord} x = 15$ (поскольку ни x^3, ни $x^5 = x^3 + x + 1$ не равны 1).

Свойства многочленов над конечным полем

Полем разложения (расширения) многочлена $f(x) \in \mathbb{F}_p[x]$ 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 2.19. *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 $x\,(x^q - 1) = x^q - x = 0$. □

Поскольку $q = p^n$, получим следующие

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

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

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

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

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

3. В случае $n = 1$ получаем доказательство *малой теоремой Ферма: любой элемент* $a \in \mathbb{F}_p$, *взаимно простой с* p, *удовлетворяет сравнению*

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

Теорема 2.20 (о делимости биномов). *В любом кольце многочленов*

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

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

- Если $m \vdots n$, то $m = kn$ и имеем
$$x^m - 1 = y^k - 1 = (y-1)\cdot(y^{k-1} + y^{k-2} + \ldots + y + 1).$$
- Если $m \not\vdots n$, то $m = kn + r$, $1 \leqslant r < n$ и имеем
$$x^m - 1 = x^r y^k - 1 = x^r \underbrace{(y^k - 1)}_{\substack{\text{делится} \\ \text{на } y-1}} + \underbrace{x^r - 1}_{\substack{\text{не делится} \\ \text{на } y-1}}.$$

□

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

Пример 2.21. Многочлен $x^{15} + 1$ над $\mathbb{F}_2$ (где $-1 = +1$) делится на $x^3 + 1$ и на $x^5 + 1$:

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

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

Теорема 2.22. *Все неприводимые многочлены n-й степени над $\mathbb{F}_p$ делят бином $x^{p^n} - x$.*

Доказательство. $\underline{n = 1}$. Убеждаемся, что $(x - a)$ делит $(x^p - x)$, 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 $\mathbb{F}_p[n]$ и строим поле $\mathbb{F}_p[x]/\big(f(x)\big) \cong \mathbb{F}_p^n$.

В нём x — корень и своего м. м. $f(x)$, и, по теореме 2.19, бинома $x^{p^n-1} - 1$.

По свойствам м. м. (утверждение 2.16) $x^{p^n-1} - 1$ делится на $f(x)$. □

Пример 2.23. 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 $x^{16} - x$ и, 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,

$$x^{15} + 1 = \big(x^4 + x + 1\big) \cdot \big(x^4 + x^3 + 1\big) \times \\ \times \big(x^4 + x^3 + x^2 + x + 1\big) \cdot \underline{\big(x^3 + 1\big)}.$$

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: $x^2 + x + 1$.

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

$$x^{15} + 1 = (x + 1) \cdot \big(x^2 + x + 1\big) \times \\ \times \big(x^4 + x + 1\big) \cdot \big(x^4 + x^3 + 1\big) \cdot \big(x^4 + x^3 + x^2 + x + 1\big).$$

Теорема 2.24. *Любой неприводимый многочлен, делящий бином* $x^{p^n} - x$, *имеет степень, не выше* n.

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

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

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

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

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

Возводим обе части этого равенства в степень p^n. Из тождества Фробениуса (см. теорему 2.1 на с. 29) и $\alpha^{p^n} = \alpha$ для любого $\alpha \in F$ получим

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

то есть β — корень $(*)$. Но у $(*)$ не более p^n различных корней, а в построенном поле F имеется p^k элементов. Поэтому $p^n \geqslant p^k$ и $n \geqslant k$. □

Корни неприводимого многочлена

Теорема 2.25 (о корнях неприводимого многочлена). *Пусть* $\beta \in \mathbb{F}_p^n$ — *корень неприводимого многочлена* $f(x) \in \mathbb{F}_p[x]$. *Тогда* β, β^p, β^{p^2}, …, $\beta^{p^{n-1}}$ *все различны и исчерпывают список всех* n *его корней.*

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

С помощью тождества Фробениуса и свойства $a^p = a \pmod p$ устанавливаем, что

$$f(\beta) = 0 \;\Rightarrow\; (f(\beta))^p = 0 \;\Leftrightarrow$$
$$\Leftrightarrow\; (a_0 + a_1\beta + \ldots + a_n\beta^n)^p = 0 \;\Leftrightarrow$$
$$\Leftrightarrow\; a_0 + a_1\beta^p + \ldots + a_n(\beta^p)^n = 0 \;\Leftrightarrow\; f(\beta^p) = 0.$$

Поэтому $\beta^p, \ldots, \beta^{p^{n-1}}$ — также корни $f(x)$.

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

Предположим противное и пусть $\beta^{p^k} = \beta^{p^\ell}$ для $0 \leqslant k \leqslant \ell \leqslant n-1$. Если α — примитивный элемент мультипликативной группы поля $\mathbb{F}_p^n$, то $\beta = \alpha^s$ для некоторого s, $1 \leqslant s \leqslant p^n - 1$. Тогда $\alpha^{sp^k} = \alpha^{sp^\ell}$, а это равенство влечёт сравнение

$$sp^k \equiv sp^\ell \pmod{(p^n - 1)}.$$

Будем пользоваться далее свойствами сравнения (см. с. 24).

Если s не делит $p^n - 1$, то справедливо сравнение

$$p^k \equiv p^\ell \pmod{(p^n - 1)}$$

и, так как $p \nmid p^n - 1$, то, сокращая это сравнение k раз на p, получим

$$p^{\ell-k} \equiv 1 \pmod{(p^n - 1)}$$

Поскольку $p^{\ell-k} < p^n - 1$, это означает, что $\ell = k$.

Если же $p^n - 1 = s \cdot t$, то справедливо сравнение

$$p^k \equiv p^\ell \pmod{t},$$

и далее, поскольку $p \nmid t$, то также $\ell = k$. □

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

Корни β, β^p, β^{p^2}, $\ldots$, $\beta^{p^{n-1}}$ 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 $x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}$.*

Действительно, 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 2.25.

Пример 2.26. 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

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

Корни найдены: это x, x^2, $x^3 + 1$ и $x^3 + x^2 + x$.

2. Найдём 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:

$$x^4 + 2x^3 + x^2 + x + 1 = (x - 1) \cdot \left(x^3 + x + 2\right).$$

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

$$x^3 + x + 2 = (x - 2) \cdot \left(x^2 + 2x + 2\right).$$

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 минимальном 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 β^p, β^{p^2}, ..., пока на некотором шаге d окажется, что

1) $\beta^{p^d} = \beta$, тогда

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

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

Пример 2.27. Найдём минимальные многочлены для элементов

$$\beta_1 = x^2 + x \quad \text{и} \quad \beta_1 = x + 1$$

поля $\mathbb{F}_2[x]/\left(x^4 + x + 1\right)$.

В этом поле $x^4 = x + 1$.

1. $\underline{\beta = \beta_1 = x^2 + x}$. Вычисляем элементы, сопряжённые с β:

$$\beta^2 = \left(x^2 + x\right)^2 = x^4 + x^2 = x^2 + x + 1,$$
$$\beta^4 = \left(x^2 + x + 1\right)^2 = x^4 + x^2 + 1 = x + \not{1} + x^2 + \not{1} = x^2 + x = \beta.$$

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:

$$\beta^2 + \beta = \left(x^2 + x + 1\right) + \left(x^2 + x\right) = 1,$$
$$\beta^3 = \left(x^2 + x + 1\right)\left(x^2 + x\right) = \ldots = (x + 1) + x = 1,$$

и окончательно $m_\beta(x) = x^2 + x + 1$[6)].

2. $\underline{\beta = \beta_2 = x + 1}$. 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 I_p^n обозначим число нормированных неприводимых многочленов степени n из $\mathbb{F}_p[x]$.

[6)] 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.

Теорема 2.28 (Гаусс). $\sum\limits_{d|n} d \cdot I_p^d = p^n$.

Найдём, например, I_2^7. По формуле Гаусса

$$\sum_{d|7} d \cdot I_2^d = 1 \cdot I_2^1 + 7 \cdot I_2^7 = 2^7 = 128.$$

Далее, $I_2^1 = 2$: имеется два линейных над $\mathbb{F}_2$ многочлена — это x и $x+1$; отсюда $I_2^7 = (128-2)/7 = 18$.

Из формулы Гаусса имеются важные

Следствия. 1. Из очевидного $0 < I_p^n$ следует существование неприводимых многочленов любой степени над любым полем.

2. Это, в свою очередь, влечёт существование для любого n поля $GF(p^n)$ как факторкольца по идеалу, образованному неприводимым многочленом.

Приведём прямую формулу для определения I_p^n.

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

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

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 2.29 (формула Гаусса).

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

Например: $I_2^4 = \frac{1}{4}\big[\underbrace{\mu(1)}_{=1}\cdot 2^4 + \underbrace{\mu(2)}_{=-1}\cdot 2^2 + \underbrace{\mu(4)}_{=0}\cdot 2\big] = 3.$

$$I_2^5 = \tfrac{1}{5}\big[\,\mu(1)\cdot 2^5 + \mu(5)\cdot 2\,\big] = \tfrac{1}{5}\big[32-2\big] = 6.$$

$$I_3^6 = \tfrac{1}{6}\big[\,\mu(1)\cdot 3^6 + \mu(2)\cdot 3^3 + \mu(3)\cdot 3^2 + \mu(6)\cdot 3\big] = 116.$$

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).

Если многочлен f неприводим, то R — поле, что уже рассмотрено. Но в любом случае R — векторное пространство над $\mathbb{F}_p$.

Теорема 2.30. *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. Имеем

$$(\varphi) = \{\, g \in R \mid g = u\varphi \pmod f,\ u \in R \,\}.$$

1. То, что (φ) есть идеал следует из определения главного идеала кольца (см. с.15).

2. Пусть $g = u\varphi \pmod f$. Тогда из $\deg g = \deg \varphi$ следует, что u — константа, и при $u = 1$ получим $g = \varphi$, при $u \neq 1$ многочлен g не нормирован.

3. Во-первых, идеал (φ) как подкольцо R — конечное векторное пространство.

Во-вторых, $\deg f = n$, $\deg \varphi = k$ и $g = u\varphi \pmod f$ означает, что что $\deg u = n - k$, откуда следует требуемое. □

Пример 2.31. Рассмотрим два многочлена над $\mathbb{F}_2$: приводимый $f(x) = x^4 - 1 = x^4 + 1$ и его неприводимый делитель $\varphi(x) = x + 1$.

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

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

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

Перечислим элементы этого идеала:

$a\ b\ c$	элементы (φ)
0 0 0	0
0 0 1	$x + 1 = \varphi(x)$
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	$x^3 + 1$

Циклическое пространство

Определение 2.32. Подпространство координатного линейного пространства F^n над полем F называется *циклическим*, если вместе с вектором $[a_0, \ldots, a_{n-1}]$ оно содержит вектор $[a_{n-1}, a_0, \ldots, a_{n-2}]$.

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

Циклический сдвиг координат в этом базисе равносилен умножению на x:

$$\begin{aligned}\left(a_0 + a_1x + \ldots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}\right)\cdot x \;&= \\ = \; a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{=1} \;&= \\ = \; a_{n-1} + a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1}.&\end{aligned}$$

Теорема 2.33. *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 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

$$g\cdot x,\; g\cdot x^2,\; \ldots$$

также принадлежат I. Значит, $g\cdot f \in I$ для любого многочлена f, поэтому I — идеал. □

Факторизация бинома $x^n - 1$. Покажем, как можно найти число и степени неприводимых делителей бинома $x^n - 1 \in \mathbb{F}_p[x]$.

Пусть $n = t \cdot p$. Поскольку тогда $x^{tp} - 1 = (x^t - 1)^p$, то корнями бинома $x^n - 1$ будут все корни $x^t - 1$, но кратности p. Это означает, что если неприводимый полином $f(x)$ делит бином $x^n - 1$, то его делит и $(f(x))^p$.

Поэтому далее будем считать, что $p \nmid n$ и бином $x^n - 1$ разлагается в произведение k неприводимых многочленов:

$$x^n - 1 \;=\; f_1(x) \cdot \ldots \cdot f_k(x).$$

Пусть эти многочлены имеют степени $d_1, \ldots, d_k$ соответственно и $d_1 + \ldots + d_k = n$.

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

Пример 2.34. 1. Вернёмся к примеру с разложением бинома $x^{15} + 1 \in \mathbb{F}_2[x]$. Относительно умножения на 2 вычеты по модулю $n = 15$ 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. Найдём разложение бинома $x^{23}-1$ 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 n некратном p есть $\mathbb{F}_p^m$, где m — максимальная степень неприводимого многочлена, его делящего: $m=\max\{d_1,\ldots,d_k\}$[7]. 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. С помощью алгоритма Евклида вычислите НОД (a,b)

$a)$ $a=589$, $b=43$; $b)$ $a=6188$, $b=4709$;

[7] нетрудно видеть, что m есть число элементов в орбите, порождаемой вычетом 1.

c) $a = 12606$, $b = 6494$; *d*) $a = 20989$, $b = 2573$.

2.2. 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) $3^{-3} \pmod 8$.

2.3. Решите сравнение

а) $7x = 11 \pmod{25}$;
б) $9x = 3 \pmod{10}$;
в) $6x + 2 = 3 \pmod 7$;
г) $6x + 2 = 3 \pmod 9$;
д) $6x + 2 = 4 \pmod 9$;
е) $6x + 1 = 4 \pmod 9$.

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

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

где β_1, β_2, β_3 — все ненулевые элементы поля.

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

2.6 (Теорема Вильсона). Доказать, что

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

2.7. Построить поле из 4-х элементов.

2.8. В кольце $\mathbb{Z}_2[x]$ найти

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

2.9. 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.

2.10. Перечислить все подполя поля $GF\left(2^{30}\right)$.

2.11. Пусть $p > 2$ — простое число. Сколько существует способов раскрасить вершины правильного p-угольника в r цветов (раскраски, получающиеся совмещением при вращении многоугольника вокруг центра, считаются одинаковыми)?

Выведете из полученной формулы малую теорему Ферма: *если целое a не делится на простое число p, то* $a^{p-1} \equiv_p 1$.

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

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

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

2.15. Многочлен

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

разложить на неприводимые множители.

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

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

2.18. 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 $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

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

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

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

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

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

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

2.22. Найти количество нормированных неприводимых многочленов

1) степени 7 над полем $\mathbb{F}_2$;

2) степени 6 над полем $\mathbb{F}_5$.

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

С её помощью вычислить выражение

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

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

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

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

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

2.27. Разложить на неприводимые множители многочлен

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

2.28. 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.

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

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

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

2.31. Найти число I_2^6 неприводимых многочленов степени 6 среди $\mathbb{F}_2[x]$.

2.32. Примитивен ли элемент x в полях

1) $\mathbb{F}_2[x]/\left(x^3+x+1\right) = F_1$?
2) $\mathbb{F}_2[x]/\left(x^4+x^3+x^2+x+1\right) = F_2$?

2.33. Найти корни многочлена

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

2.34. Является ли многочлен

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

примитивным?

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

2.36. 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) $f(x) \in \mathbb{F}_5[x]$.

2.37. Найти корни многочлена

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

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

2.39. Найти корень многочлена

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

2.40. Найти корни многочлена $f(x) = x^5+x^2+1 \in \mathbb{F}_2[x]$.

Глава 3

Коды, исправляющие ошибки

3.1 Блоковое кодирование

Задача помехоустойчивого кодирования. Поток *битовой* информации проходит по каналу с шумом, вследствие чего возникают ошибки. Канал может быть пространственным (линия связи) или же временны́м (хранение информации).

- *Модель ошибок*: биты случайно, независимо и с равными вероятностями могут оказаться инвертированными, то есть вставок или выпадения битов нет (*двоичный симметричный канал*).
- *Задача*: обеспечить автоматическое исправление ошибок, построив *помехозащищённый код*.

Подход к решению (один из возможных!):

1) весь поток информации разбить на *сообщения* — последовательные непересекающиеся блоки фиксированной длины k;
2) каждый блок *кодировать* (модифицировать) —

   а) по единому правилу и независимо от других — *блоковое кодирование*;

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

Далее рассматриваем только *блоковое кодирование*. Введём основные понятия и терминологию.

- $S = \{0,1\}^k$ — пространство всех возможных *сообщений* длины k каждое.
- *Кодом* будем называть совокупность C всех кодовых слов, $|C| = Q = 2^k$ — *мощность кода*;
- Для обеспечения помехозащищённости вместо сообщений передают *кодовые слова* бóльшей длины $n = k + m$, $m > 0$, и поэтому рассматриваемое кодирование называют *избыточным*. Если $m = 0$ или $k = 0$ говорят о *тривиальных кодах*.
- *Кодированием* будем называть взаимно-однозначное преобразование сообщения в кодовое слово[1)].

  Кодирование, при котором биты сообщения переходят в заранее фиксированные позиции кодового слова, называют *систематическим* или *разделимым*. Тогда соответствующие k бит кодового слова называют *информационными*, а остальные m — *проверочными*.
- *Декодирование* — восстановление сообщения по принятому, возможно искажённому, слову.

[1)] часто именно это отображение и называют кодом

- $R = k/n$ — *скорость* кода, m/n — его *избыточность*.

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

Кодовое расстояние

Определение 3.1. Минимальное хемингово расстояние между словами кода C называется его *кодовым расстоянием*[2], символически $d(C)$ или просто d.

Хемингово расстояние $\rho(\widetilde{\alpha}, \widetilde{\beta})$ между бинарными векторами $\widetilde{\alpha}$ и $\widetilde{\beta}$, напомним, есть вес их суммы:

$$\rho(\widetilde{\alpha}, \widetilde{\beta}) \;=\; \big\|\widetilde{\alpha} + \widetilde{\beta}\big\|.$$

Ясно, что код может исправить до r ошибок, если в B^n шары радиусов r с центрами в кодовых словах не пересекаются. Действительно, если в векторе $\widetilde{\alpha}$ искажено не более r бит, то набор останется в данном шаре и искомое кодовое слово есть центр шара, ближайший к полученному набору. *Следовательно, у кода, исправляющего до r ошибок, кодовое расстояние d должно быть не менее $2r + 1$.*

Определение кодового расстояния произвольного кода C крайне трудоёмкая задача: показана её NP-трудность. В общем случае для нахождения $d(C)$ требуется перебрать все $(2^k(2^k - 1))/2$ пар кодовых слов,

[2] часто — *минимальным кодовым расстоянием*

что практически невозможно уже начиная с $k = 50$. Поэтому важной задачей является построение кодов с кодовым расстоянием не менее заданного.

Блоковое кодирование и декодирование. Рассмотрим элементарный пример. Блоки содержат по одному биту, то есть пространство сообщений есть $S = \{0, 1\}$.

Элементарный код-повторение $a \mapsto \overbrace{a \ldots a}^{2r+1 \text{ раз}}$, очевидно, исправит до r ошибок. Простейший вариант — *утраивание*: $0 \mapsto 000$, $1 \mapsto 111$. Ясно, однако, что такое кодирование крайне неэффективно.

Кодирование. Все векторы далее мы будем считать вектор-столбцами[3]. Обозначения:

- сообщение — вектор

$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ \ldots \\ u_k \end{bmatrix} \in \{0,1\}^k = S;$$

- кодовое слово — вектор $\boldsymbol{v} \in \{0,1\}^n = B^n$;
- совокупность C всех кодовых слов — (n, k)-*код*, или, с кодовым расстоянием — (n, k, d)-*код*.

Пример 3.2. Избыточный код $(5, 2)$-код мощности $Q = 4$:

$$C = \{\, c_1 = (00000),\, c_2 = (10101),\, c_3 = (01110),\, c_4 = (11011) \,\}.$$

[3] Часто используют вектор-строки — будьте внимательны!

Блоковое кодирование всегда можно осуществить, используя таблицу размера $2^k \times n$. Однако такое кодирование требует большой памяти: на практике значения n и k могут достигать сотен тысяч.

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

$$\boldsymbol{v} \;\to\; \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e},$$

где $\boldsymbol{e} \in \{0,1\}^n$ — *вектор ошибок*, содержащий 1 в ошибочных битах и 0 в остальных.

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

Декодирование (n, k, d)-кода *обычно значительно сложнее* кодирования. Декодирование принятого слова $\boldsymbol{w}$ проводится в два этапа:

1-й этап: Определение кодового слова $\widehat{\boldsymbol{v}}$ как ближайшего в метрике Хэмминга слову к $\boldsymbol{w}$, то есть нахождение центра соответствующего шара (*декодирование по максимуму правдоподобия*).
Если произошло не более $r = \lfloor (d-1)/2 \rfloor$ ошибок, то $\widehat{\boldsymbol{v}} = \boldsymbol{v}$.

2-й этап: Восстановление исходного сообщения $\boldsymbol{u}$ по найденному кодовому слову.
Систематическое кодирование делает этот этап тривиальным: исходное сообщение получится удалением из кодового слова проверочных бит.

Ясно, что 1-й этап может быть выполнен перебором 2^n строк в $(2^n \times k)$-таблице кодовых слов. Это говорит о том, что 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 определённые ограничения на множество кодовых слов, можно сократить объёмы вычислений при кодировании/декодировании. Эти ограничения приводят к использованию кодов специального вида: *линейных*, а из линейных — *циклических*.

Плотная упаковка шаров в единичный куб

Теорема 3.3. *1. Мощность Q кода длины n, исправляющего до $r < n/2$ ошибок, ограничена сверху:*

$$Q \leqslant \frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^r} \tag{3.1}$$

— граница Хэмминга (англ. volume bound).

2. Существуют коды длины n, исправляющие до $r < n/2$ ошибок мощности

$$Q \geqslant \frac{2^n}{C_n^0 + C_n^1 + \ldots + C_n^{2r}}$$

— граница Гильберта.

Доказательство известно читателю из курса Дискретной математики. □

Из неравенства 3.1 следует, что параметры блокового (n, k, d)-кода связаны соотношением

$$\log_2 \sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} C_n^i \leqslant n - k.$$

В области малых значений скорости кода (больших значений d/n) граница Хэмминга является довольно грубой.

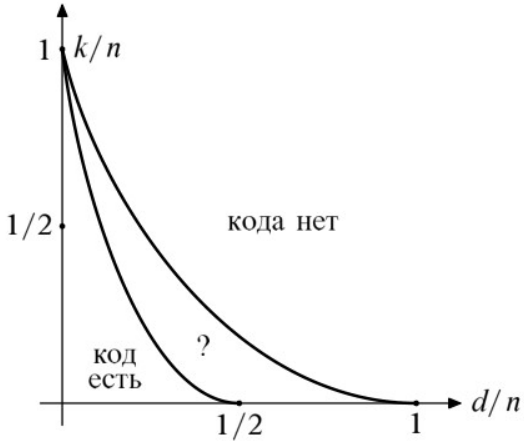


Рис. 3.1. Границы Гильберта (левая) и Хэмминга (правая) для $n \gg 1$.

Чтобы построить блоковый (n, k)-код, исправляющий данное количество r ошибок и имеющий минимальную избыточность, нужно вложить в единичный куб B^n максимально возможное число k не пересекающихся шаров радиуса r. Это *задача плотной упаковки*: неравенство 3.1 должно обращаться в равенство и граница Хэмминга достигаться.

При каких же n и r в куб B^n можно уложить непересекающиеся шары радиуса r «плотно», «без зазоров»? Оказывается, такое удаётся только в двух нетривиальных случаях, когда получаются *совершенные* или *экстремальные коды*:

1) $n = 2^m - 1$, $r = 1$ — *коды Хэмминга*;
   у них $k = 2^m - 1 - m$, $m = 2, 3, \ldots$;

2) $n = 23$, $r = 3$ — *код Голея* (см. с. 88);
   у него $k = 12$ и $m = 11$.

Пример 3.4. Код из примера 3.2 не является совершенным: для него $Q = 4 < \frac{2^5}{1+5} = 5\frac{1}{3}$.

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

Образуем сначала единичную матрицу порядка

$$k = 2^m - 1 - m.$$

Затем припишем к ней справа все бинарные наборы длины m, содержащие не менее двух единиц, их будет как раз k. В результате получим таблицу

$$\underbrace{\left\{\begin{array}{ll} 100\ldots000 & 1100\ldots000 \\ 010\ldots000 & 1010\ldots000 \\ 001\ldots000 & 1001\ldots000 \\ \quad\ldots & \quad\ldots \\ 000\ldots001 & 1111\ldots111 \end{array}\right.}_{k=2^m-(m+1)} \quad \underbrace{\qquad\qquad}_{m}$$

Просуммировав по mod 2 все совокупности строк таблицы и добавив нулевую строку, получим мощность кода

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

Найдём кодовое расстояние построенного кода C. Для этого надо оценить вес сумм по $\bmod 2$ всех непустых совокупностей строк полученной таблицы.

Замечаем, что в каждой строке таблицы имеется не менее трёх единиц. Если же сложить по $\bmod 2$ две строки, то в левой части будет находится две единицы, а в правой — хотя бы одна. Отсюда следует, что расстояние между кодовыми словами всегда не менее $3 = d(C)$.

Заметим, что при таком кодировании исходное сообщение окажется в первых k позициях кодового слова.

Пример 3.5. Положим $m = 3$, тогда $n = 2^3 - 1 = 7$. 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

Сложение по $\bmod 2$ всех (включая пустую) совокупностей строк даёт все $Q = 2^4 = 16$ слов $(7, 4, 3)$-кода Хэмминга.

3.2 Линейные коды

Линейные коды: определение, свойства. Бóльшая часть теории блокового кодирования относится к линейным кодам, позволяющим в ряде случаев реализовывать алгоритмы кодирования/декодирования, приемлемые по эффективности.

Определение 3.6. Блоковый (n, k)-код C называется *линейным*, если он образует линейное векторное подпространство размерности k координатного пространства $\{0,1\}^n$ всех возможных принятых слов W, символически $C = \{0,1\}^k \leqslant \{0,1\}^n = W$.

Линейный код обладает следующими свойствами.

Во-первых, в рассматриваемом двоичном случае множество кодовых слов линейного кода образует абелеву группу относительно операции «сумма по $\bmod 2$» $(+)$. Действительно, векторное подпространство гарантирует устойчивость операции $+$, а её свойствами обеспечивается ассоциативность, существование нуля $\widetilde{0}$ и противоположных элементов. Поэтому линейные двоичные коды называют *групповыми*.

Пример 3.7. Нетрудно убедиться, что код из примера 3.2 — групповой.

Во-вторых, кодовое расстояние d группового кода C есть число единиц в кодовом слове $\widetilde{\gamma}$ минимального веса:

$$d = \min_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho(\widetilde{\alpha}, \widetilde{\beta}) = \min_{\widetilde{\alpha}+\widetilde{\beta}=\widetilde{\gamma}\neq\widetilde{0}} \left\| \widetilde{\alpha} + \widetilde{\beta} \right\|,$$

где $\widetilde{\alpha}$, $\widetilde{\beta}$, $\widetilde{\gamma} \in C$, и оценка достигается при $\widetilde{\beta} = \widetilde{0}$.

Пример 3.8. В примере 3.2 вес наборов c_2 и c_3 минимален и равен 3, таким образом $d(C) = 3$.

Из доказанного следует, что для вычисления кодового расстояния группового кода нужно перебрать только $2^k - 1$ кодовых слов (экспоненциальная сложность процесса сохраняется).

Для двоичных систематических линейных (n, k, d)-кодов легко получить оценку Синглтона: $d \leqslant n - k + 1$. Действительно, кодовое слово, соответствующее сообщению веса 1, содержит не более $n - k + 1$ единиц: одну в информационных разрядах и максимально — во всех $n-k$ проверочных (возможность преобразования произвольного линейного кода к систематическому виду показана ниже). К сожалению, не существует двоичных нетривиальных систематических кодов, для которых *граница Синглтона* (равенство в приведённом неравенстве) достигается.

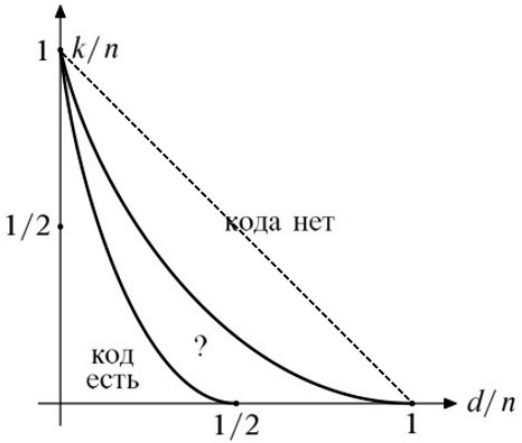


Рис. 3.2. Границы Гильберта, Хэмминга и Синглтона (пунктир) для $n \gg 1$.

И, в-третьих, существует базис $\{ \boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1} \}$ линейного кода C, состоящий из векторов $\boldsymbol{g}_i \in \{0,1\}^n$, $i = 0, \ldots, k-1$. Поэтому любой вектор $\boldsymbol{v} \in C$ (кодовое слово) может быть представлен в виде линейной комбинацией базисных векторов кода:

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

Порождающая матрица. Составим из векторов некоторого базиса кода матрицу

$$G_{n\times k} = [\, \boldsymbol{g}_0\ \boldsymbol{g}_1\ \cdots\ \boldsymbol{g}_{k-1}\,]$$

Её называют *порождающей матрицей* линейного кода C. Она осуществляет кодирование, математически описываемое вложением $G : S \hookrightarrow \{0,1\}^n$ множества сообщений S в W:

$$\boldsymbol{v} = G\boldsymbol{u}. \tag{3.2}$$

Пример 3.9. Код из примера 3.2 линейный: он порождается матрицей

$$G = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Заметим, что при использовании векторов-строк порождающей матрицей считают транспонированную матрицу G и соотношение (3.2) записывают в виде $\boldsymbol{v} = \boldsymbol{u}G$.

Понятно, что сама матрица G определена с точностью до *элементарных преобразований столбцов* — базисных векторов (их перестановкам и сложению по $\bmod 2$ данного столбца с любым другим). Такие преобразования эквивалентны переходу к другому базису *того же* кода (как набора элементов из B^n).

Из порождающей матрицей G произвольного линейного (n,k)-кода с помощью элементарных преобразований столбцов может быть получена матрица G', у которой *первые k строк образуют единичную подматрицу* I_k. Тогда при кодировании матрицей G' первые k бит сообщения перейдут в первые биты кодового слова, обеспечивая систематическое кодирование.

Пример 3.10. Код из примеров 3.2 и 3.9 порождается также матрицей G', получающейся из G перестановкой столбцов. Первые две строки G' образуют единичную матрицу 2-го порядка.

Ясно также, что любой линейный код можно преобразовать в эквивалентный ему систематический с произвольно заданными позициями информационных бит.

Пример 3.11. В примере 3.5 была получена таблица, сложением различных совокупностей строк которой получаются все кодовые слова некоторого кода Хэмминга. Порождающая матрица этого кода получается транспонированием этой таблицы:

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

— порождающая матрица в систематической форме: при кодировании биты сообщения помещаются в первые 4 бита кодового слова

Если к порождающей матрице линейного кода добавить единичную строку, получим *расширенный код*, в результате чего кодовые слова пополнятся битом чётности. При этом код исправляющий r ошибок будет также способен *обнаруживать* ошибки кратности $r+1$.

Подчеркнём ещё раз, что для того, чтобы узнать кодовое расстояние линейного кода, в обществе необходимо перебрать все его элементы. Для этого можно

умножить порождающую матрицу на всевозможные ненулевые векторы сообщений

$$\boldsymbol{v} \;=\; G\boldsymbol{u},\;\; \boldsymbol{u} \in S = B^k \setminus \widetilde{0}$$

и определить минимальный вес кодовых слов $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2^k-1}$.

Ортогональное дополнение к коду и проверочная матрица. Элементы $\{0,1\}^n$, ортогональные всем кодовым словам линейного (n,k)-кода C образуют *ортогональное линейное подпространство* $C^\perp$ пространства W:

$$\underset{C}{\forall}\boldsymbol{v}\;\; \underset{C^\perp}{\forall}\boldsymbol{w}:\;\; \boldsymbol{v}^T \times \boldsymbol{w} \;=\; 0.$$

У (n,k)-кода $\dim C = k$ и $\dim C^\perp = n - k = m$. При этом $W = \{0,1\}^n$ *не есть прямая сумма* подпространств C и $C^\perp$: произвольный вектор из W 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 $\{0,1\}^n$ не следует их линейной независимости, как это имеет место в евклидовом пространстве.

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

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

называется *проверочной матрицей* кода C. Она осуществляет сюръективное отображение $H : W \to C^{\perp}$.

Ясно, что H определена с точностью до элементарных преобразований *строк* — базисных векторов $C^{\perp}$.

Объединяя сказанное ранее, утверждаем, что имеется *короткая точная последовательность* векторных пространств и гомоморфизмов

$$0 \to \underbrace{\{0,1\}^k}_{S} \xrightarrow{G} \underbrace{\{0,1\}^n}_{W} \xrightarrow{H} \underbrace{\{0,1\}^{n-k}}_{C^{\perp}} \to 0.$$

Здесь G — мономорфизм, H — эпиморфизм и ядро H совпадает с образом C преобразования G:

$$\operatorname{Im} G \;=\; C \;= \operatorname{Ker} H$$

(см. рис. 3.3). Иными словами, для всех $\boldsymbol{u} \in S$ спра-

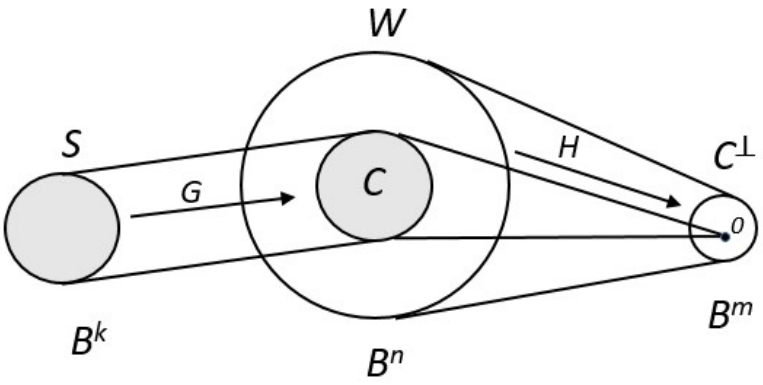


Рис. 3.3. Преобразования: G — сообщений в линейный код C и H — принятых слов в $C^{\perp}$.

ведливо

$$G\boldsymbol{u} = \boldsymbol{v} \in C \leqslant W \quad \text{и} \quad H\boldsymbol{v} = \boldsymbol{0} \in C^{\perp}.$$

Это означает, что $HG = O$ — *нулевая* $m \times k$ *матрица.*

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 $H = \begin{bmatrix} P_{m\times k} & I_m \end{bmatrix}$ будет проверочной.

Действительно, в этом случае

$$HG = \begin{bmatrix} P & I \end{bmatrix} \times \begin{bmatrix} I \\ P \end{bmatrix} = P + P = O$$

— нулевая $m \times k$ матрица.

Пример 3.12. Для построенной в примере 3.11 порождающей матрицы $G_{7\times 4}$ проверочной будет

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

Мы видим, что столбцами проверочной матрицы кода Хэмминга являются все ненулевые векторы длины $m = 3$.

Ясно, что если систематическое кодирование таково, что сообщение попадает в последние биты кодового слова, то порождающая и проверочная матрицы имеют вид

$$G = \begin{bmatrix} P \\ I \end{bmatrix}, \quad H = \begin{bmatrix} I & P \end{bmatrix}.$$

Итак, линейный (n, k)-код C задаётся либо порождающей матрицей $G_{n\times k}$, либо проверочной матрицей

$H_{m\times n}$. 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 задаёт G и H однозначно.

Если строки единичной матрицы I произвольно расположены в порождающей матрице G, то легко указать соответствующее правило построения матрицы H, аналогичное вышеприведённому.

Пример 3.13. Пусть линейный $(6,3)$-код C 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. Кодом C осуществить несистематическое и систематическое кодирование векторов
$$\boldsymbol{u}_1 = [0\ 1\ 1]^T \quad \text{и} \quad \boldsymbol{u}_2 = [1\ 0\ 1]^T.$$
2. Построить проверочную матрицу H' для систематического кодирования.
3. Определить кодовое расстояние d кода C.

Решение. 1. *Несистематическое кодирование* находим непосредственно:

$$\boldsymbol{v}_1 = G\boldsymbol{u}_1 = [\,1\ 1\ 0\ 0\ 1\ 0\,]^T,$$
$$\boldsymbol{v}_2 = G\boldsymbol{u}_2 = [\,1\ 0\ 1\ 0\ 1\ 1\,]^T.$$

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

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

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

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

$$\boldsymbol{v}'_1 = G'\boldsymbol{u}_1 = [\,1\,1\,0\,0\,1\,0\,]^T,$$
$$\boldsymbol{v}'_2 = G'\boldsymbol{u}_2 = [\,1\,0\,1\,1\,0\,0\,]^T.$$

2. Для построения проверочной матрицы H' сначала сформируем матрицу $P_{3\times3}$ из строк G', *отличных от строк единичной подматрицы*:

$$P_{3\times3} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Далее нужно

1) последовательно разместить *столбцы* P соответственно в 3, 5 и 1-м столбцах H;
2) остальные 2, 4 и 6-й столбцы H должны образовывать единичную подматрицу.

В итоге получим проверочную матрицу

$$H'_{3\times6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

3. Найдем кодовое расстояние d. Для этого закодируем все $2^3 - 1 = 7$ ненулевых сообщений и найдем минимальный хэммингов вес кодовых слов:

$$C = [\,\boldsymbol{v}_1 \ldots \boldsymbol{v}_7\,] = G' \times [\,\boldsymbol{u}_1 \ldots \boldsymbol{u}_7\,] =$$

$$= G' \times \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & \mathbf{1} & 0 & 1 \\ 1 & 0 & 1 & \mathbf{1} & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 1 & 1 \\ 1 & \mathbf{1} & 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & \mathbf{1} & 1 & 0 & 0 & 1 & 1 \\ 1 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 1 \end{bmatrix}.$$

Получаем $d = 3$.

Код Голея. М. Голей[4] обнаружил в 1949 г., что

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

Это позволило предположить, что существует совершенный $(23, 12, 7)$-код, содержащий $2^{12} = 4\,096$ кодовых слов и исправляющий до 3-х ошибок, который и был им указан. Код оказался линейным, и более того — циклическим (см. далее).

Доказано, что других пар (n, r), для которых $2^n / \left(C_n^0 + \ldots + C_n^r\right)$ — целое, кроме кодов Хэмминга и тривиальных, не существует.

3.3 Синдромное декодирование линейных кодов

Было установлено, что если H — проверочная матрица линейного кода, а $\boldsymbol{v}$ — кодовое слово, то

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

[4] *Марсель Жюль Эдуард Голей* (Marcel J. E. Golay, 1902–1989) — швейцарский и американский математик, физик и информационный теоретик.

Если же при передаче произошли ошибки, будет принято слово $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}$ и тогда

$$H\boldsymbol{w} = H\boldsymbol{v} + H\boldsymbol{e} \stackrel{\text{def}}{=} \boldsymbol{s}.$$

Определение 3.14. *Синдром слова* $\boldsymbol{w}$, принятого при передаче сообщения, закодированного линейным кодом с проверочной матрицей H, есть вектор $\boldsymbol{s} = H\boldsymbol{w}$.

Ясно, что если $\boldsymbol{s} = \boldsymbol{0}$, то $\boldsymbol{w}$ — кодовое слово, и в этом случае считаем, что ошибок не произошло. Точнее, это означает лишь отсутствие *ошибок определённого типа*, а не их отсутствие вообще; это замечание относится к синдромному декодированию всех кодов.

Если же ошибки произошли, то

$$\boldsymbol{s} = \underbrace{H\boldsymbol{v}}_{=0} + H\boldsymbol{e} = H\boldsymbol{e}.$$

Это означает, что вектор ошибок $\boldsymbol{e}$ удовлетворяет неоднородной недоопределенной СЛАУ

$$H\boldsymbol{e} = \boldsymbol{s}, \tag{3.3}$$

а кодовые слова являются решениями соответствующей однородной системы

$$H\boldsymbol{v} = \boldsymbol{0}. \tag{3.4}$$

Таким образом, вектор $\boldsymbol{e}$ может быть представлен как частное решение неоднородной системы (3.3) и общее решение однородной (3.4).

Определение ошибок по синдрому. Поскольку и принятый вектор $\boldsymbol{w}$, и соответствующий ему вектор ошибок $\boldsymbol{e}$ имеют одинаковые синдромы, можно попытаться восстановить неизвестный вектор $\boldsymbol{e}$, используя тот факт, что он является решением системы (3.3).

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

Данный метод потребует хранения проверочной матрицы размера $m \times n$, словаря синдромов размера $2^m \times n$ и остаётся экспоненциально трудоёмким.

Декодирование кода Хэмминга. 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* 3.11 получена матрица

$$H_{3\times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$
$$\begin{matrix} 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{matrix}$$

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

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

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

Пример 3.15. Для рассматриваемого $(7,4)$-кода Хэмминга получаем матрицу

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

Тогда порождающая матрица есть

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

При кодировании матрицей G биты сообщения помещаются последовательно в 3, 5, 6 и 7-ю позиции кодового слова, а остальные три бита являются проверочными.

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

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

Пусть при передаче ошибка произошла в 5-м бите, то есть получено слово

$$\boldsymbol{w} = [\,0\,1\,0\,0\,\underline{0}\,0\,1\,]^T.$$

Тогда синдром

$$\boldsymbol{s} = H'\boldsymbol{w} = [\,1\,0\,1\,]^T = 5_2.$$

указывает позицию ошибки.

В общем случае задача декодирования линейных кодов является NP-сложной.

Поскольку $HG = O = G^T H^T$, то можно использовать H^T как порождающую, а G^T — как проверочную матрицу некоторого другого кода и из линейного (n, k)-кода получить $(n, n-k)$-код. Коды, связанные таким образом, называются *дуальными* или *двойственными* друг другу.

Если исходный код был получен так, чтобы иметь минимальную избыточность при заданной исправляющей способности, то гарантировать хорошее качество дуального ему кода уже нельзя: обычно дуальный код имеет то же кодовое расстояние, как и исходный, но бóльшую избыточность.

Код, двойственный к расширенному коду Хэмминга, называется *кодом Макдональда*.

3.4 Циклические коды

Определение и построение циклических кодов

Определение 3.16. Линейный блоковый код называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов своих кодовых слов.

Теорема 2.33 утверждает, что циклическое пространство образуют элементы идеала I в кольце классов вычетов по модулю многочлена $x^n - 1$. Такой идеал в кольце $\mathbb{F}_p[x]/(x^n - 1)$ задаётся делителем $g(x)$ бинома $x^n - 1$: элементы I составляют многочлены из $\mathbb{F}_p[x]$, кратные $g(x)$ (по $\pmod{x^n - 1}$).

Имеется биективное соответствие векторов и полиномов, введённое на с. 45:

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

Последнее соотношение описывает элементы образованного циклического пространства.

Поэтому построить циклический (n, k)-код[5)] можно следующим образом.

1. Задаёмся нечётным (чтобы обеспечить взаимную простоту с $p = 2$) значением n и выбираем *любой* делитель $g(x)$ бинома $x^n - 1$.
   Многочлен $g(x)$ называют *порождающим* или *образующим* код; $\deg g(x) = m < n$.

   Порождающий многочлен полностью определяет циклический код.

2. Идеал $(g(x))$ кольца $R = \mathbb{F}_2[x]/(x^n - 1)$ состоит из всех многочленов вида

   $$f(x) \cdot g(x), \quad 0 \leqslant \deg f(x) < n - m = k.$$

   Многочлены из этого идеала задаются *векторами своих коэффициентов, которые и будут кодовыми словами.*

При удачном выборе порождающего полинома получается код с приемлемым кодовым расстоянием d,

[5)] избыточный циклический код — англ. CRC, *Cyclic Redundancy Code*

однако определение d остаётся чрезвычайно трудоёмкой задачей.

Пример 3.17. Построим циклический код длины 23. В п. 2 примера 2.34 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, либо двойственный к нему.

Коды Хэмминга могут быть циклическими. Построенная в примере 3.5 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 циклический (n, k)-код C задаётся порождающим полином $g(x)$, делящим $x^n - 1$, $\deg g(x) = m = n - k$.

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий:

$$u(x) \;\mapsto\; v(x) \;=\; g(x)u(x) \in C.$$

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 поместит 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

$$x^m u(x) + r(x) \;=\; g(x)q(x) \;=\; v(x) \in C.$$

Пример 3.18. 1. Построим циклический код длины $n = 7$.

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени его неприводимых делителей, для чего применим способ разбиения $\mathbb{Z}_7$ на орбиты относительно умножения на 2 (см. с. 63):

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

С учётом теорем 2.19 и 2.25, заключаем, что все 7 ненулевых элементов $\alpha^0 = 1, \alpha, \ldots, \alpha^6$ поля разложения бинома $x^7 - 1$, или, что то же, его корни, разбиваются на классы сопряжённых корней

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

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 $x - 1 = x + 1$, а остальные делители единственны, получаем разложение

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

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* Ясно, это код Хэмминга.

Определяя конкретный код, выберем

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

Заметим, что при выборе $g(x) = x + 1$ получаем код с проверкой на чётность; при выборе, например $g(x) = (x+1)\left(x^3 + x + 1\right)$ — расширенный код Хэмминга; при выборе $g(x) = x^7 - 1$ — тривиальный код.

2. Закодируем несистематическим и систематическим кодированием сообщение

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

Несистематическое кодирование.

$$v(x) = u(x)g(x) = \left(x^3 + x^2\right)\left(x^3 + x + 1\right) = \\ = x^6 + x^5 + x^4 + x^2 \leftrightarrow [\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ ]^T = \boldsymbol{v}.$$

Систематическое кодирование.
Находим остаток $r(x)$ от деления $x^3 u(x)$ на $g(x)$:

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

то есть $r(x)=x$ и поэтому

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

Декодирование циклических кодов

Определение 3.19. *Синдромом* $s(x)$ *слова* $w(x)$, принятого при передаче сообщения, закодированного циклическим кодом, называют остаток от деления $w(x)$ на многочлен $g(x)$, порождающий код.

Ясно, что если $s(x)=0$, то $w(x)$ — кодовое слово.
Схема синдромного декодирования слова $w(x)$:

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

Примеры синдромного декодирования циклических кодов, а также альтернативные декодеры (Меггита, Касами–Рудольфа, пороговый, мажоритарный и др.) мы рассматривать не будем; отметим только, что все они имеют экспоненциальную трудоёмкость.

3.5 Коды БЧХ. Кодирование

Коды Боуза-Чоудхури-Хоквингема (BCH, БЧХ) — подкласс циклических кодов, исправляющих *не менее заранее заданного* числа ошибок[6)].

Циклотомические классы

Определение 3.20. Ненулевые элементы поля $\mathbb{F}_p^t$, имеющие общий минимальный многочлен, называют *сопряженными*. Все сопряжённые элементы составляют *циклотомический класс*.

Ясно, что циклотомические классы $C_0 = \{1\}$, C_1, ... либо совпадают, либо не пересекаются, и в совокупности образуют *разбиение* мультипликативной группы поля $\mathbb{F}_2^t$, или, как говорят, её *разложение на классы* над $\mathbb{F}_2$.

Поскольку в поле характеристики p значения любого полинома в точках α и α^p одинаковы, то циклотомические классы можно получать возведением в степень p какого-то одного его элемента. Это совпадает с построением орбиты отображения (см. с. 63)

$$\ell \mapsto 2\ell \mod (2^t - 1)$$

элементов мультипликативной группы поля $\mathbb{F}_2^t$.

Заметим, что если α — *примитивный элемент* поля $\mathbb{F}_2^t$, то его циклотомический класс *содержит ровно* t

[6)] Коды предложены Раджем Чандра Боузом (Raj Chandra Bose, 1901–1987) и Двайджендра Камар Рей-Чоудхури (Dwijendra Kumar Ray-Chaudhuri, 1933) в 1960 г. независимо от опубликованной на год ранее работы Алексиса Хоквингема (Alexis Hocquenghem, 1908?–1990).

элементов: поскольку $\alpha^{2^t-1} = 1$, то $\alpha^{2^t} = \alpha$ и данный класс есть

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

Пример 3.21. Пусть $t = 4$ и α — примитивный элемент поля $F = \mathbb{F}_2^4$. Тогда $F^* = \{ \alpha, \alpha^2, \ldots, \alpha^{14}, \alpha^{15} = 1 \}$ разлагается над $\mathbb{F}_2$ на циклотомические классы

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

БЧХ-коды: определение, синдромы. Выберем параметр t, определяющий длину кода $n = 2^t - 1$. Для бинома $x^n - 1$ рассмотрим поле $\mathbb{F}_2^t$ его разложения с некоторым примитивным элементом α.

Если требуется исправлять не менее r ошибок, зададимся *конструктивным расстоянием* $\delta = 2r + 1 < n$. Степени α, α^2, α^3, $\ldots$, α^{2r} примитивного элемента α поля $\mathbb{F}_2^t$ называют *нулями кода*.

Код БЧХ есть циклический (n, k, d)-код, в котором порождающий многочлен $g(x)$ *является полиномом минимальной степени, имеющим корнями все нули кода*. Как и у всех циклических кодов, для него $\deg g(x) = m$, $k = n - m$, а кодовое расстояние d оказывается *не менее* выбранного конструктивного расстояния δ.

Поскольку нули кода являются корнями $g(x)$, а полиномы всех кодовых слов циклического кода делятся $g(x)$, то нули кода суть также корни любого кодового слова.

Определение 3.22. *Синдромами* $s_1, \ldots, s_{2r}$ принятого полинома $w(x)$ при кодировании БЧХ-кодом с нулями $\alpha, \ldots, \alpha^{2r}$ назовём набор значений $w(x)$ в нулях кода: $s_i = w(\alpha^i)$, $i = 1, \ldots, 2r$.

Поскольку $w(x) = v(x) + e(x)$, то для всех $i = 1, \ldots, d-1$ справедливо $s_i = w(\alpha^i) = e(\alpha^i)$, и если все синдромы равны нулю, то $w(x)$ — кодовое слово.

Построение БЧХ-кода. БЧХ (n, k)-код, как и любой циклический, задаётся порождающим полиномом $g(x)$, делящим бином $x^n - 1$, $k = n - \deg g(x)$.

Алгоритм построения двоичного кода БЧХ, исправляющего не менее r ошибок

1. Выбрать величину t, определяющую длину кода $n = 2^t - 1 > 2r + 1$.
2. Выбрать неприводимый полином $a(x)$ степени t, определив поле $\mathbb{F}_2^t = \mathbb{F}_2[x]/(a(x))$ с некоторым примитивным элементом α.
3. Найти циклотомические классы поля $\mathbb{F}_2^t$ над $\mathbb{F}_2$, в которые попадают $2r$ нулей кода $\alpha, \alpha^2, \ldots, \alpha^{2r}$; пусть таких классов h.
4. Найти минимальные многочлены $g_1(x)$, $\ldots$, $g_h(x)$ каждого циклотомического класса.
5. Вычислить порождающий полином кода
$$g(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_h(x).$$

Пример 3.23. Выберем $t = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

Для этого возьмём неприводимый над $\mathbb{F}_2$ многочлен $a(x) = x^3 + x + 1$ и образуем поле

$$F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^3.$$

Поскольку многочлен $a(x)$ — примитивный, и, как показано в п. 1 примера 3.18 на с. 95, F^* разбивается на следующие циклотомические классы ($\alpha = x$):

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

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 $2r = 2$ и нули кода α, α^2 попадают в один циклотомический класс C_1.

Минимальный многочлен элементов этого класса — $a(x)$, поэтому порождающий полином $g(x) = a(x)$, $m = 3$ и в результате получаем уже известный $(7, 4, 3)$-код Хэмминга (см. пример 3.18).

2. *Код БЧХ длины $n = 7$, исправляющий не менее $r = 2$ ошибок.* Теперь $2r = 4$. Нули строящегося кода α, α^2, α^3, α^4 входят в циклотомические классы C_1 и C_2 поля F, 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 класса C_2:

$$g_2(x) = \left(x-\alpha^3\right)\left(x-\alpha^5\right)\left(x-\alpha^6\right) = \\ = x^3 + \left(\alpha^3+\alpha^5+\alpha^6\right)x^2 + \left(\alpha^8+\alpha^9+\alpha^{11}\right)x + \alpha^{14}.$$

Вычислим коэффициенты $g_2(x)$:

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

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

$$g(x) = g_1(x)\cdot g_2(x) = \left(x^3+x+1\right)\left(x^3+x^2+1\right) = \\ = x^6+x^5+x^4+x^3+x^2+x+1.$$

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

Пример 3.24. Попытаемся построить лучшие коды, взяв бóльшие их длины: выберем $t = 4$ 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 $t = 4$. Тогда F^* относительно своего примитивного элемента α, как показано в п. 2 примера 3.21, разобьётся на 5 циклотомических классов над $\mathbb{F}_2$:

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

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

В качестве многочлена 4-й степени, определяющего конкретное поле F, 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 до $r = 2$ ошибок.* В этом случае $2r = 4$ и нули α, α^2, α^3, α^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 —

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

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, $d = \delta = 5$, то есть построен БЧХ $(15, 7, 5)$-код со скоростью уже $R = 7/15 > 1/7$.

2. *Код БЧХ длины $n = 15$, исправляющий не более $r = 3$ ошибок.* Теперь $2r = 6$ и нужно найти полином, являющийся м. м. для для классов C_1, C_2 и C_3, в которые попадают нули кода α, α^2, $\ldots$, α^6.

Минимальные многочлены для C_1 и C_2 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

$$g(x) = g_1(x) \cdot g_2(x) \cdot g_3(x) = \\ = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \quad (3.5)$$

Получено $m = 10$, $k = 5$ и можно показать, что $d = \delta = 7$. 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 $\mathbb{F}_2^n$ и $n = 2^t - 1$.

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 $j = 0, 1, \ldots, n-1$.

Пример 3.25. Рассматриваем $(7, 4)$-код Хэмминга, построенный в примере 3.18 для циклических кодов, где был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [\,0\,0\,1\,1\,]^T$:

$$v(x) = x^3 u(x) + x \leftrightarrow [\,0\,1\,0\,\underbrace{0\,0\,1\,1}_{\boldsymbol{u}}\,]^T.$$

Пусть при передаче кодового слова $v(x)$ произошла ошибка в 5-й позиции (считая с 0), 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:

$$s = w(\alpha) = \alpha^6 + \alpha = \left(\alpha^3\right)^2 + \alpha = (\alpha+1)^2 + \alpha = \\ = \alpha^2 + 1 + \alpha \neq 0\,.$$

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 $n = 2^t - 1$ при построении которого для определения порождающего полинома использовалось поле $F = \mathbb{F}_2^t = \mathbb{F}_2[x]/(a(x))$, $\deg a(x) = t$ с примитивным элементом (нулём кода) α.

Пусть при передаче кодового слова произошло $\nu \leqslant r = \lfloor (d-1)/2 \rfloor$ ошибок в позициях $j_1, \ldots, j_\nu$, которые и нужно определить.

Тогда полином ошибок есть

$$e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}.$$

Вычислим синдромы принятого полинома $w(x)$: $s_i = w(\alpha^i) = e(\alpha^i)$, $i = \overline{1, 2r}$. Если все они равны 0, то, считаем, ошибок не произошло. Иначе для $1 \leqslant \nu$ запишем с учётом $(\alpha^i)^j = (\alpha^j)^i$ значения синдромов через степени α:

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_\nu})^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = (\alpha^{j_1})^{2r} + \ldots + (\alpha^{j_\nu})^{2r}. \end{cases}$$

Эту систему надо решить относительно неизвестных ν, j_1, $\ldots$, j_ν.

Введём обозначения $\beta_i = \alpha^{j_i}$, $i = 1, \ldots, \nu$; эти величины называют *локаторами ошибок*.

Перепишем полученную систему:

$$\begin{cases} s_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ s_2 = \beta_1^2 + \beta_2^2 + \ldots + \beta_\nu^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = \beta_1^{2r} + \beta_2^{2r} + \ldots + \beta_\nu^{2r}. \end{cases}$$

Определим *полином локаторов ошибок*

$$\sigma(x) = \prod_{i=1}^{\nu} (1 + \beta_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\nu x^\nu,$$

считая формально $\sigma_0 = 1$ и $\sigma_i = 0$ при $i > \nu$. Корнями этого полинома будут величины $\beta_i^{-1} = \alpha^{-j_i}$, $i = \overline{1, \nu}$.

Связь между коэффициентами полинома $\sigma(x)$ и самими локаторами определяет теорема Виета:

$$\begin{cases} \sigma_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 + \ldots + \beta_{\nu-1}\beta_\nu, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_\nu = \beta_1\beta_2\ldots\beta_\nu. \end{cases}$$

Две последние системы задают величины синдромов и коэффициентов полинома локаторов ошибок как значения *симметрических полиномов*: первая — степенных сумм и вторая — элементарных.

Соотношения между этими двумя типами симметрических полиномов задаются *тождествами Ньютона-Жирара*, последние $2r - \nu$ из которых нашем случае записываются как

$$\begin{cases} s_{\nu+1} + \sigma_1 s_\nu + \cdots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0, \\ s_{\nu+2} + \sigma_1 s_{\nu+1} + \cdots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} + \sigma_1 s_{2r-1} + \cdots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0. \end{cases} \qquad (*)$$

Данные равенства представляют собой СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$. Стандартными методами эта система не может быть решена, поскольку значение ν неизвестно.

Алгоритмы решения системы $(*)$ называют *декодерами*. Например, декодер PGZ[8)] состоит в последовательных попытках решения данных соотношений для $\nu = r, r-1, \ldots$ до тех пор, пока матрица очередной СЛАУ не окажется невырожденной.

Результатом работы декодера является полином локаторов ошибок $\sigma(x)$, степень которого есть число реально произошедших ошибок $\nu = \deg \sigma(x)$.

После нахождения полинома локаторов ошибок $\sigma(x)$, нужно отыскать все ν его корней. Для этого можно перебрать все элементы $\alpha, \alpha^2, \ldots, \alpha^n$ мультипликативной группы F^*, а по ним — позиции ошибок: если α^i — корень $\sigma(x)$, то позиция ошибки j есть $j = -i \pmod n$.

[8)] Peterson-Gorenstein-Zierler, Петерсона-Горенштейна-Цирлера

Алгоритм декодирования (n, k, d)*-кода БЧХ*

с нулём кода α из поля $F = \mathbb{F}_2[x]/(a(x)) = \mathbb{F}_2^t$, $\deg a(x) = t$ и принятого слова $w(x) \in \{0,1\}^n$, $n = 2^t - 1$.

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 переходим к пункту 6.
2. Используя тот или иной декодер, найти полином локаторов ошибок $\sigma(x)$; число ν произошедших ошибок равно его степени.
3. Найти все корни $\sigma(x)$, например, перебором элементов F^*; пусть эти корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
4. Найти позиции ошибок $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
5. Найти полином ошибок $e(x) = x^{j_1} + \ldots + x^{j_\nu}$ и восстановить кодовое слово $v(x) = w(x) + e(x)$.
6. По $v(x)$ восстановить переданное сообщение $u(x)$.

Декодер на основе обобщённого алгоритма Евклида. Определим *синдромный полином*

$$s(x) = 1 + s_1 x + s_2 x^2 + \ldots + s_{2r} x^{2r},$$

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*:

$$s(x)\sigma(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{2r+\nu} x^{2r+\nu}.$$

Его коэффициенты определяются соотношением для произведения многочленов —

$$\lambda_i \;=\; \sum_{j=0}^{i} \sigma_j s_{i-j}, \quad i = 1, \ldots, 2r+\nu.$$

Замечаем, что значения λ_i по данной формуле для $i = \nu{+}1, \ldots, 2r$ 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}:

$$s(x)\cdot\sigma(x) \;=\; \underbrace{1+\lambda_1 x+\lambda_2 x^2+\ldots+\lambda_\nu x^\nu}_{\lambda(x)} + \\ +\; x^{2r+1}\left(\lambda_{2r+1}+\ldots+\lambda_{2r+\nu}x^{\nu-1}\right), \quad 1\leqslant\nu\leqslant r.$$

Это означает, что

$$s(x)\sigma(x) \;=\; \lambda(x) \pmod{x^{2r+1}}.$$

Данное соотношение называют *ключевым уравнением*. Его решение $\sigma(x)$ при $\nu \leqslant r$ 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 обобщённым алгоритмом Евклида в кольце по $\bmod x^{2r+1}$ (см. с. 43) с условием останова «*степень очередного остатка не более* r» и опусканием заключительного шага нормировки.

Пример 3.26. Рассматриваем БЧХ $(15, 5, 7)$-код с полем разложения $\mathbb{F}_2[x]/\left(x^4 + x + 1\right) = F$, построенный в п. 2 примера 3.24. При вычислениях будем пользоваться таблицей со с. 46.

Пусть передаётся сообщение

$$\boldsymbol{u} = [\,0\,1\,1\,0\,1\,]^T \leftrightarrow u(x) = x^4 + x^2 + x\,.$$

При систематическом кодировании порождающим полиномом (3.5) кодовым словом (опустим этот этап) будет

$$\boldsymbol{v} = [\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,\underbrace{0\,1\,1\,0\,1}_{\boldsymbol{u}}\,]^T.$$

Предположим, что при передаче ошибки произошли в 0, 6 и 12-й позициях, то есть принято слово

$$w(x) = x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \leftrightarrow$$
$$\leftrightarrow [\,\underline{1}\,1\,1\,1\,1\,0\,\underline{1}\,0\,1\,0\,0\,1\,\underline{0}\,0\,1\,]^T = \boldsymbol{w}.$$

1. Найдём все $2r = 6$ синдромов:

$$s_1 = w(\alpha) = (\underbrace{\alpha^3 + 1}_{\alpha^{14}}) + (\underbrace{\alpha^3 + \alpha^2 + \alpha}_{\alpha^{11}}) + (\underbrace{\alpha^2 + 1}_{\alpha^8}) +$$
$$+ (\underbrace{\alpha^3 + \alpha^2}_{\alpha^6}) + (\underbrace{\alpha + 1}_{\alpha^4}) + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha,$$
$$s_2 = w(\alpha^2) = (w(\alpha))^2 = s_1^2 = \alpha^2,$$
$$s_3 = \ldots = \alpha^8,$$
$$s_4 = w(\alpha^4) = s_1^4 = \alpha^4,$$
$$s_5 = \ldots = 1,$$
$$s_6 = w(\alpha^6) = s_3^2 = \alpha^{16} = \alpha.$$

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. Применяя декодер на базе обобщённого алгоритма Евклида решаем относительно $\sigma(x)$ соотношение

$$x^7\, b(x) \;+\; s(x)\,\sigma(x) \;=\; \lambda(x).$$

Шаг 0.
$$r_{-2}(x) \;=\; x^7,$$
$$r_{-1}(x) \;=\; s(x),$$
$$\sigma_{-2}(x) \;=\; 0, \quad \sigma_{-1}(x) \;=\; 1.$$

Шаг 1.
$$r_{-2}(x) \;=\; r_{-1}(x)q_0(x) + r_0(x),$$
$$q_0(x) \;=\; \alpha^{14}x + \alpha^{13},$$
$$r_0(x) \;=\; \alpha^8 x^5 + \alpha^{12}x^4 + \alpha^{11}x^3 + \alpha^{13},$$
$$\deg r_0(x) = 5 > 3 = r,$$
$$\sigma_0(x) \;=\; q_0(x).$$

Шаг 2.
$$r_{-1}(x) \;=\; r_0(x)q_1(x) \;+\; r_1(x),$$
$$q_1(x) \;=\; \alpha^8 x + \alpha^2,$$
$$r_1(x) \;=\; \alpha^{14}x^4 + \alpha^3 x^3 + \alpha^2 x^2 + \alpha^{11}x,$$
$$\deg r_1(x) = 4 > 3 = r,$$
$$\sigma_1(x) \;=\; \sigma_{-1}(x) + \sigma_0(x)q_1(x) \;=$$
$$=\; \alpha^7 x^2 + \alpha^{11}x.$$

Шаг 3.
$$r_0(x) \;=\; r_1(x)q_2(x) \;+\; r_2(x),$$
$$q_2(x) \;=\; \alpha^9 x,$$
$$r_2(x) \;=\; \alpha^5 x + \alpha^{13},$$
$$\deg r_2(x) = \mathbf{1} \leqslant \mathbf{3} = r,$$
$$\sigma_2(x) \;=\; \sigma_0(x) \;+\; \sigma_1(x)q_2(x) \;=$$
$$=\; \alpha x^3 + \alpha^5 x^2 + \alpha^{14}x + \alpha^{13}.$$

Это последний шаг алгоритма, т. к. степень остатка $r_2(x)$ не превосходит $r = 3$. Таким образом, найден полином локаторов ошибок

$$\sigma(x) \;=\; \sigma_2(x) \;=\; \alpha x^3 + \alpha^5 x^2 + \alpha^{14} x + \alpha^{13},$$

и установлено их количество $\nu = \deg \sigma(x) = 3$.

3. Найдём корни $\sigma(x)$ перебором элементов F^*.

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 + \alpha^{13} \;=\; \alpha^2 \;\neq\; 0;\\
\sigma(\alpha^2) &= \alpha^7 + \alpha^9 + \alpha + \alpha^{13} \;=\; \alpha^3 + \alpha^2 + \alpha \;\neq\; 0;,\\
\sigma(\alpha^3) &= \alpha^{10} + \alpha^{11} + \alpha^{17} + \alpha^{13} \;=\\
&= \left(\alpha^2 + \alpha + 1\right) + \left(\alpha^3 + \alpha^2 + \alpha\right) + \alpha^2 +\\
&\qquad + \left(\alpha^3 + \alpha^2 + 1\right) \;=\; 0.
\end{aligned}$$

Первый корень полинома $\sigma(x)$ найден. Далее перебирая α^4, α^5, …, α^{15}, находим ещё два корня:

$$\begin{aligned}
\sigma(\alpha^9) &= \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} \;=\; 0,\\
\sigma(\alpha^{15}) &= \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} \;=\; 0.
\end{aligned}$$

4. По найденным корням α^3, α^9, α^{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. Полином ошибок $e(x) = x^{12} + x^6 + 1$ определён и переданное кодовое слово есть

$$v(x) \;=\; w(x) + e(x) \;\leftrightarrow\; [\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\;\underbrace{0\,1\,1\,0\,1}_{\boldsymbol{u}}\,]^T.$$

6. Поскольку применялось систематическое кодирование, исходное сообщение $\boldsymbol{u} = [\;0\;1\;1\;0\;1\;]^T$ восстанавливается элементарно.

Замечания по практическому применению избыточного кодирования

- В современных телекоммуникационных системах предъявляются очень высокие требования к достоверности передачи информации с вероятностью ошибки на символ не более 10^{-9}. В беспроводных каналах такую достоверность практически невозможно получить без применения помехоустойчивого кодирования.
- При небольших n существуют хорошие БЧХ-коды, но, как правило, не лучшие из известных.
- Современные устройства имеют высокие скорости передачи данных, и длина кода не является важным ограничением. Значения избыточности кода 1/2, 2/3, ... считаются приемлемыми.
- При практических поисках лучших кодов замечена степенная зависимость длины кода от кодового расстояния с показателями 2...3.
- Для выполнения алгоритимов кодирования/декодирования применяется как программная, так и схемная (на комбинационно-логических схемах) реализации.
- Исправление ошибок может требоваться не всегда: при передаче сообщений часто достаточно лишь проверить наличие ошибок и при необходимости повторить передачу нужное число раз. В этих случаях применяются коды, предназначенные только для обнаружения ошибок. Ясно, что для *обнаружения* до r ошибок код должен иметь кодовое расстояние не менее $d = r + 1$.

3.7 Задачи

3.1. Построить порождающую G и проверочную H матрицы для

1) тривиального кода утраивания;

2) кода проверки на чётность.

3.2. Для кода Хемминга, 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

$$\boldsymbol{u}_1 = [\,1\,1\,0\,1\,]^T, \ \boldsymbol{u}_2 = [\,1\,0\,0\,1\,]^T.$$

3.3. 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

$$u(x) = x^2 + x \leftrightarrow [\,0\,1\,1\,]^T.$$

3.4. Рассмотрим код Хэмминга систематического кодирования с порождающим примитивным полиномом $a(x) = x^3 + x + 1$.

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,

3) $w_3(x) = x^6 + x^3 + x^2 + x$.

3.5. Пусть $n = 5$ и α — примитивный элемент поля $\mathbb{F}_2^5 = F$. Найти разложение F^* над $\mathbb{F}_2$.

3.6. Пусть α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$. 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 $\sigma(x)$.

3.7. Рассмотрим код БЧХ, нули которого определяются степенями α, где α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$.

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 $w(x)$.

3.8. Построить 31-разрядный БЧХ-код для исправления не менее $r = 3$ ошибок.

3.9. Рассмотрим БЧХ-код, нули которого есть степени примитивного элемента α поля
$F = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$.

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. 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) нелые 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 $1, 2, \ldots, n$ 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 $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений?

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

Любая циклическая 24-элементная группа изоморфна $\mathbb{Z}_{24} = \langle \{ 0, 1, \ldots, 23 \}, +, 0 \rangle$.

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 — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle = C \cong \mathbb{Z}_{24}$;
$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;
$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_8$;
$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_6$;
$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_4$;
$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_3$;
$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_2$;
$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — 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. Они взаимно просты с 24 и суть 1, 5, 7, 11, 13, 17, 19, 23.

1.3. Вычислите функцию Эйлера для:

а) $n = 375$; б) $n = 720$; в) $n = 988$.

а) $\varphi(375) = \varphi(3 \cdot 5^3) = 2 \cdot 5^2 \varphi(5) = 2 \cdot 25 \cdot 4 = 200$.
б) $\varphi(720) = \varphi(2^4 \cdot 3^2 \cdot 5) = 2^3 \cdot 1 \cdot 3 \cdot 2 \cdot 4 = 192$.
в) $\varphi(988) = \varphi(2^2 \cdot 13 \cdot 19) = 2 \cdot 1 \cdot 12 \cdot 18 = 432$.

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

Любая циклическая 24-элементная группа изоморфна $\mathbb{Z}_{24} = \langle \{ 0, 1, \ldots, 23 \}, +, 0 \rangle$.

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 — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle = C \cong \mathbb{Z}_{24}$;

$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;

$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_8$;

$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_6$;

$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_4$;

$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_3$;

$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_2$;

$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — 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 $m = 1, 5, 7, 11, 13, 17, 19, 23$.

1.5. Показать, что если $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ — примарное разложение n, то

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

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) = \\
&= p_1^{\alpha_1 - 1}\varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_k) = \\
&= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_1) \cdot \ldots \cdot \varphi(p_k) = \\
&= \frac{n}{p_1 \cdot \ldots \cdot p_k} \cdot (p_1 - 1) \cdot \ldots \cdot (p_k - 1) = \\
&= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

1.6. 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) Кольцо (обратной матрицы может не быть), (2) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы), (3) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы.

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

По дистрибутивности

$$x\cdot(y+z)=x\cdot y+x\cdot z \;\Rightarrow\; x\cdot(0+0)=x\cdot 0=x\cdot 0+x\cdot 0 \;\Rightarrow$$
$$\Rightarrow\; x\cdot 0=0.$$

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

Нет! Хотя $f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$, но $f(xy)=2xy\neq(2x)\cdot(2y)=f(x)\cdot f(y)$.

1.9. Показать, что множество векторов пространства с операциями сложения и векторного умножения является кольцом.

Является ли оно ассоциативным? коммутативным?

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

$$\boldsymbol{x}\times(\boldsymbol{y}+\boldsymbol{z})=\boldsymbol{x}\times\boldsymbol{y}+\boldsymbol{x}\times\boldsymbol{z},$$
$$(\boldsymbol{y}+\boldsymbol{z})\times\boldsymbol{x}=\boldsymbol{y}\times\boldsymbol{x}+\boldsymbol{z}\times\boldsymbol{x}.$$

Кольцо $\langle V,+,\times,\mathbf{0}\rangle$ некоммутативно: $\boldsymbol{x}\times\boldsymbol{y}\neq\boldsymbol{y}\times\boldsymbol{x}$ и неассоциативно: $\boldsymbol{x}\times(\boldsymbol{y}\times\boldsymbol{z})\neq(\boldsymbol{x}\times\boldsymbol{y})\times\boldsymbol{z}$.

Однако в рассматриваемом кольце выполняются тождества, заменяющие, в некотором смысле коммутативность и ассоциативность:

$$\boldsymbol{x}\times\boldsymbol{y}=-\boldsymbol{y}\times\boldsymbol{x}\ \text{(антикоммутативность)},$$
$$(\boldsymbol{x}\times\boldsymbol{y})\times\boldsymbol{z}+(\boldsymbol{y}\times\boldsymbol{z})\times\boldsymbol{x}+$$
$$+(\boldsymbol{z}\times\boldsymbol{x})\times\boldsymbol{y}=\mathbf{0}\ \text{(тождество Якоби)}.$$

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

В кольце $\mathbb{Z}_6$ классы вычетов по идеалу $(3) = \{0, 3\}$ суть

$$\begin{aligned} 0 + (3) &= 3 + (3) = (0, 3), \\ 1 + (3) &= 4 + (3) = (1, 4), \\ 2 + (3) &= 5 + (3) = (2, 5). \end{aligned}$$

1.11. Является ли поле $\mathbb{Z}_2$ подполем поля $\mathbb{Z}_5$?

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. С помощью алгоритма Евклида вычислите НОД (a, b)

а) $a = 589$, $b = 43$; *б*) $a = 6188$, $b = 4709$;
в) $a = 12606$, $b = 6494$; *г*) $a = 20989$, $b = 2573$.

а) 1, *б*) 17, *в*) 382, *г*) 1.

2.2. 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) $3^{-3} \pmod 8$.

Вычислять x^{-1} в кольцах $\mathbb{Z}_n$ можно используя соотношение Безу (подбором коэффициентов или обобщённым алгоритмом Евклида). В некоторых очевидных случаях (напр. в пункте в)) можно обойтись без вычислений.

а) $1 = 2 \cdot 3 - 1 \cdot 5,\ 2 \cdot 3 = 1 + 1 \cdot 5,\ 2 \cdot 3 \equiv_5 1,\ 3^{-1} \equiv_5 2$;

Или

1	5	0	
2	3	1	$q = 1$
3	2	-1	$q = 1$
4	1	**2**	$q = 2 \quad (\ 2 \ldots)$
5	0		

Таким образом, $3^{-1} = 2$.

б) $1 = 2 \cdot 14 - 3 \cdot 9,\ (-3) \cdot 9 = 1 - 2 \cdot 14,$
$(-3) \cdot 9 \equiv_{14},\ 9^{-1} = -3 = 11 \pmod{14}$;

Или

1	14	0	
2	9	1	$q = 1$
3	5	-1	$q = 1$
4	4	2	$q = 1$
5	1	**-3**	$q = 4 \quad (\ 4 \ldots)$
6	0		

Таким образом, $9^{-1} = -3 \equiv_{14} = 11$.

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) $1 = 3 \cdot 3 - 8,\ 3 \cdot 3 = 1 + 8,\ 3 \cdot 3 \equiv_8 1,$
$3^{-1} \equiv_8 3,\ 3^{-3} = (3^{-1})^3 = 3^3 = 27 = 3 \pmod{8}$.

2.3. Решите сравнение

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 — $\{2, 5, 8\} \pmod{9}$.

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

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

где β_1, β_2, β_3 — все ненулевые элементы поля.

Имеем

$$F = \mathbb{F}_2[x]/\big(x^2 + x + 1\big) = \{\, 0, 1 = \alpha^3, \alpha, \alpha+1 = \alpha^2 \,\},$$

где α — порождающий элемент мультипликативной группы F^*. Поэтому

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

$$= (x+1)\left(x^2+\alpha x+x+\alpha x+\alpha^2+\alpha\right) =$$
$$= (x+1)\left(x^2+x+\alpha^2+\alpha\right) =$$
$$= \left(x^3+(\alpha+1)x^2+(\alpha+1)x^2+(\alpha^2+\alpha+1)x+\right.$$
$$\left.+\alpha^2+\alpha\right) = x^3+1,$$

и по теореме 2.19:

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

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

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.

2.6. Доказать, что

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

При $p=2$ утверждение тривиально.

При $p>2$ порядки всех элементов мультипликативной циклической группы $\mathbb{F}_p^* = \{1,\ldots,p-1\}$ делят её порядок то есть все они являются корнями уравнения

$$x^{p-1}-1 = 0. \qquad (*)$$

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 $p \geqslant 5$ обозначим

$$1\cdot\underbrace{2\cdot\ldots\cdot(p-2)}_{=\pi}\cdot(p-1) = (p-1)!,$$

и заметим, что $(p-1)^2 = p^2 - 2p + 1 \equiv_p 1$.

Легко видеть, что произведение $\pi = 1$: каждый из элементов $2, \ldots, p-2$ 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 $(p-1)! \equiv_p -1$.

2.7. Построить поле из 4-х элементов.

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

2.8. В кольце $\mathbb{Z}_2[x]$ найти

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

Воспользуемся алгоритмом Евклида:

$$x^5 + x^2 + x + 1 = \left(x^2 + x\right)\left(x^3 + x^2 + x + 1\right) + \underline{\left(x^2 + 1\right)},$$

$$x^3 + x^2 + x + 1 = (x+1)\underline{\left(x^2+1\right)}.$$

Ответ: $x^2 + 1$.

2.9. 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.

Поле $F = \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$ содержит 8 элементов: 0 и степени $1, \ldots, 7$ 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 $a(x)$.

2.10. Перечислить все подполя поля $GF\,(2^{30})$.

Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ если и только если $k \mid n$, поэтому подполями $GF\left(2^{30}\right)$ будут поля $GF\left(2^k\right)$, $k \in D(30) = \{1,2,3,5,6,10,15,30\}$, $GF\,(2)$ — *простейшее* и $GF\left(2^{30}\right)$ — *несобственное* подполя.

2.11. Пусть $p>2$ — простое число. Сколько существует способов раскрасить вершины правильного p-угольника в r цветов

(раскраски, получающиеся совмещением при вращении многоугольника вокруг центра, считаются одинаковыми)?

Выведете из полученной формулы малую теорему Ферма: *если целое a не делится на простое число p, то* $a^{p-1} \equiv_p 1$. Если не отождествлять раскраски указанного типа, то всех раскрасок r^p.

Исключим одноцветные раскраски, остальных — $r^p - r$. Вращение раскрашенного более, чем в один цвет p-угольника вокруг своего центра на p углов $\frac{2\pi}{p}$, $2\frac{2\pi}{p}$, ..., 2π даст одинаковые раскраски.

Итого, число различных раскрасок в более, чем один цвет равно $\frac{a^p-a}{p}$, и тогда всех раскрасок — $C = \frac{a^p-a}{p} + a$.

$C = \frac{a\left(a^{p-1}-1\right)}{p} + a$ — целое число. Отсюда, если $a \not\vdots p$, то $(a^{p-1}-1) \vdots p$, т. е. $(a^{p-1}-1) \equiv_p 0$ или $\frac{a^{p-1}-1}{p}$.

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

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: $x^5 + x^3 + x^2 + 1 = (x + 1)^3 \left(x^2 + x + 1\right)$.

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

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. $$\begin{array}{r|l} x^3 + 2x^2 + 4x + 1 & x + 3 \\ \cline{2-2} x^3 + 3x^2 & x^2 + 4x + 2 \\ \cline{1-1} \quad 4x^2 + 4x & \\ \quad 4x^2 + 2x & \\ \cline{1-1} \quad\quad 2x + 1 & \\ \quad\quad 2x + 1 & \\ \cline{1-1} \quad\quad\quad 0 & \end{array}$$
3. Перебором убеждаемся, что многочлен $x^2 + 4x + 2$ неприводим в $\mathbb{F}_5$.

Ответ: $x^3 + 2x^2 + 4x + 1 = (x + 3)\left(x^2 + 4x + 2\right)$.

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

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
   Ответ: $f(x) = x^4 + x^3 + x + 2 = \left(x^2 + 1\right)\left(x^2 + x + 2\right)$.

2.15. Многочлен

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

разложить на неприводимые множители.

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

Ответ: $f(x) = \left(x^2 + x + 1\right)\left(x^2 + 2x + 4\right)$.

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

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:

$$\begin{aligned} f_1(x) &= x^2 + 1, \\ f_2(x) &= x^2 + x + 2, \\ f_3(x) &= x^2 + 2x + 2. \end{aligned}$$

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

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

$$\begin{aligned} f_1(x) &= x^3 + 2x + 1, \\ f_2(x) &= x^3 + 2x + 2, \\ f_3(x) &= x^3 + x^2 + 2, \\ f_4(x) &= x^3 + 2x^2 + 1, \\ f_5(x) &= x^3 + x^2 + x + 2, \\ f_6(x) &= x^3 + x^2 + 2x + 1, \end{aligned}$$

$$f_7(x) = x^3 + 2x^2 + x + 1,$$
$$f_8(x) = x^3 + 2x^2 + 2x + 2.$$

2.18. 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 $\mathbb{F}_5[x]/(x^3 + 2x + 4)$?

1. Перебором элементов из $\mathbb{F}_5$ —

$$a(0) = 4,\ a(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1,$$

убеждаемся, что квадратный многочлен $a(x)$ неприводим.

Следовательно, факторкольцо $\mathbb{F}_5[x]/\big(x^2 + 2x + 4\big)$ *является полем*; в нём $x^2 = -2x - 4 = 3x + 1$.

2. $a(4x^2 + 1) = \big(2(2x^2 + 1)\big)^3 + 2 \cdot 2(2x^2 + 1) + 4 =$
$= 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 =$
$= 4(3x + 1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + x + x^2 + 1 = 0$ — да, является.

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

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

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. $\mathbb{F}_7^2 = \big\{\, ax + b \mid a, b \in \mathbb{F}_7,\ x^2 = 1 - x = 6x + 1 \,\big\}$

$$(ax+b)\cdot(6x+1) = \ldots = (2a+6b)x + (6a+b) = 1$$

$$\begin{cases} 6a+b &= 1 \\ a+3b &= 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

Ответ: $(1-x)^{-1} = x+2$ в F.

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

1) поля $F_1 = \mathbb{F}_2[x]/(x^4+x+1)$;
2) поля $F_2 = \mathbb{F}_2[x]/(x^4+x^3+1)$.

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

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. $\underline{x^4 = x+1}$

$$\begin{aligned} \beta^2 &= x^2(x+1)^2 = x^4 + x^2 = x^2 + x + 1, \\ \beta^3 &= x(x+1)\left(x^2+x+1\right) = x\left(x^3+1\right) = \\ &= x^4 + x = x + 1 + x = 1. \end{aligned}$$

Ответ: В поле F_1 $\operatorname{ord}\beta = 3$.

2. $\underline{x^4 = x^3+1}$

$$\begin{aligned} \beta^2 &= x^4 + x^2 = x^3 + x^2 + 1, \\ \beta^3 &= x(x+1)\left(x^3+x^2+1\right) = \\ &= x\left(x^4+x^2+x+1\right) = x\left(x^3+x^2+x\right) = \\ &= x^4 + x^3 + x^2 = x^2 + 1 \neq 1, \end{aligned}$$

$$\begin{aligned}\beta^5 &= x^2x^3 = \left(x^3+x^2+1\right)\left(x^2+1\right) = \\ &= \left(x^5+x^4+x^2+x^3+x^2+1\right) = \ldots \\ \ldots &= \left(x^3+1\right)x = x^4+x = x^3+x+1 \neq 1.\end{aligned}$$

Ответ: В поле F_2 $\operatorname{ord}\beta = 15$.

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

Мультипликативная группа поля

$$\mathbb{F}_2[x]/\left(x^6+x^3+1\right)$$

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

$$x^9 = x^6x^3 = \left(x^3+1\right)x^3 = x^6+x^3 = \not{x}^3+1+\not{x}^3 = 1.$$

Т.о. $\operatorname{ord} x = 9 \neq 63$ и многочлен $f(x)$ *не примитивен.*

2.22. Найти количество нормированных неприводимых многочленов

1) степени 7 над полем $\mathbb{F}_2$;
2) степени 6 над полем $\mathbb{F}_5$.

$$\sum_{d|n} d\cdot I_p^d = p^n.$$

1. $\underline{((7))\text{ над }\mathbb{F}_2}$

$$\sum_{d|7} d\cdot I_p^d = 2^7 = 1\cdot((1)) + 7\cdot((7)) = 128.$$

$((1)) = 2$: это x и $x+1$, отсюда $((7)) = \frac{128-2}{7} = 18$.

2. $\underline{((6)) \text{ над } \mathbb{F}_5}$

$$((6)) = \frac{1}{6}\sum_{d|6}\mu(d)\,5^{\frac{6}{d}} = \frac{1}{6}\left[\mu(1)5^6 + \mu(2)5^3 + \right.$$

$$\left. + \mu(3)5^2 + \mu(6)5\right] = \frac{15625 - 125 - 25 + 5}{6} = 2\,580.$$

2.23. 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

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

Поскольку $\operatorname{char} F = 3$, то $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

$F = \mathbb{F}_3^2$, 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 $\bmod a(x)$, 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 $x^4 = 1$:

$$x^4 = \left(x^2\right)^2 = (2x+1)^2 = x^2 + x + 1 =$$
$$= \cancel{2}x + 1 + \cancel{x} + 1 = 2 \neq 1,$$

то есть x — примитивный элемент F: $\operatorname{ord} x = 8$ и $x^8 = 1$.

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:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} =$$
$$= x^6 + x^4 = \left(x^2\right)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \not{1} + \not{2} =$$
$$= 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

2.24. 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.

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. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = \left(x^2\right)^2 = 4 \equiv_3 1.$$

Следовательно $\operatorname{ord} x = 4$ и элемент x не является генератором группы F^* (и $x^2 + 1$ — не есть примитивный многочлен над $\mathbb{F}_3$:
$x^4 - 1 = x^4 + 2 = \left(x^2 + 1\right)\left(x^2 + 2\right)$).

2. Проверим на примитивность элемент $x + 1$:

$$(x+1)^4 = (x+1)(x+1)^3 = (x+1)\left(x^3+1\right) =$$

$$= (x+1)(2x+1) = 2x^2 + \not{x} + \not{2}x + 1 = 4+1 = 2 \neq 1$$

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 $\alpha \cdot \alpha^{i+j-1}$.

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

Сначала убедимся, что многочлен $f(x) = x^2+x+2$ неприводим: ни одно из значений $f(x)$, $x \in \mathbb{F}_3$ не равно 0.

Далее проверим, является ли $f(x)$ делителем x^4+1?

$x^4+1 = \left(x^2+x+2\right) t \left(x^2+2x+2\right)$ — да, является

Поэтому искомый идеал составят многочлены из R, кратные $f(x)$:

$$\left(x^2+x+2\right) = \left\{ \left(x^2+x+2\right)(ax+b) \mid a,b \in \mathbb{F}_3, x^4 = 1 \right\}.$$

Теперь проведём умножение:

$$\left(x^2+x+2\right)(ax+b) = ax^3+(a+b)x^2+(2a+b)x+2b.$$

Перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $\left(x^2+x+2\right)$:

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 $f(x) \not| a(x)$? Тогда в R существует идеал, порождённый элементом НОД $(f(x), a(x))$.

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

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

Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \cdot \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

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

$$\left(x^2+3x+3\right)a(x)+(4x+3)b(x) \;=\; 1$$

с помощью обобщённого 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*

$$r_{-2}(x) \;=\; r_{-1}(x)q_0(x)+r_0(x),$$
$$q_0(x) \;=\; 4x+4,$$
$$r_0(x) \;=\; 1, \;\; // \;\; \deg r_0 = 0 \;\Rightarrow\; \mathit{OCTAHOB}$$
$$y_0(x) \;=\; y_{-2}(x)-y_{-1}(x)q_0(x) \;=$$
$$= \;-q_0(x) \;=\; -4x-4 \;=\; x+1.$$

3. Вычислим обратную матрицу

$$M^{-1} \;=\; (x+1)\begin{bmatrix} 3x+2 & 4x+2 \\ 4x+3 & 3x+4 \end{bmatrix} \;=\; \begin{bmatrix} x+2 & 1 \\ 4x & 3x \end{bmatrix}.$$

2.27. Разложить на неприводимые множители многочлен

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

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

$$f(x) \;=\; \left(x^2+x+1\right)\cdot$$

$$\cdot (\underbrace{x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1}_{g(x)}).$$

Делим частное $g(x)$ на $x^2 + x + 1$:

$$g(x) = x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ = \left(x^2 + x + 1\right) \cdot \left(x^7 + x^4 + x^3 + x^2 + x + 1\right) + x$$

— 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 $x^3 + x + 1$:

$$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ = \left(x^3 + x + 1\right) (\underbrace{x^6 + x^5 + x^3 + x^2 + 1}_{h(x)}) \quad \text{— делится!}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

$$x^6 + x^5 + x^3 + x^2 + 1 = \\ = \left(x^3 + x + 1\right) \cdot \left(x^3 + x^2 + x + 1\right) + x^2,$$
$$x^6 + x^5 + x^3 + x^2 + 1 = \left(x^3 + x^2 + 1\right) \cdot x^3 + x^2 + 1.$$

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

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = \\ \left(x^2 + x + 1\right) \left(x^3 + x + 1\right) \left(x^6 + x^5 + x^3 + x^2 + 1\right).$$

2.28. 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.

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
  $f(x) = (x+1)\left(x^2 + 2x + 2\right).$
- Многочлен $g(x) = x^2 + 2x + 2$ не имеет корней в $\mathbb{F}_3$, его степень 2, т. е. он неприводим.
- Окончательно: $f(x) = (x+1)\left(x^2 + 2x + 2\right).$

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 —

$$g(x) \;=\; (x-\alpha)\cdot(x-\alpha^p)\cdot\left(x-\alpha^{p^2}\right)\cdot\ldots\cdot\left(x-\alpha^{p^{n-1}}\right),$$

  где α – произвольный корень $g(x)$ в F;
- не имеет корней ни в каком конечном поле, содержащим 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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right)$ 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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right)$ 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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right) = GF(3^2)$.

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

$$\beta \in \{\,0,\ 1,\ \alpha,\ \ldots,\ \alpha^{14}\,\} = F, \quad x^4 = x+1.$$

$\beta = 0$: $m_0(x) = x$.

$\beta = 1$: $m_1(x) = x+1$.

$\beta = \alpha$: сопряжённые с α элементы — α^2, α^4, α^8 и

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = \ldots$$
$$\ldots = x^4+x+1 = 0.$$

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 α^6, α^{12}, $\alpha^{24} = \alpha^9$, их м. м. —

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 +$$

$$+\left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2+$$
$$+\left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x+$$
$$+\left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right)=x^4+\big(\alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha)+$$
$$+(\alpha^3+\alpha^2+\alpha+1)\big)x^3+(\ldots)\,x^2+(\ldots)\,x+\alpha^{30}=$$
$$=x^4+x^3+x^2+x+1.$$

$\beta=\alpha^5$: 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 — α^{14}, $\alpha^{28}=\alpha^{13}$, $\alpha^{56}=\alpha^{11}$, их м. м. —

$$m_{\alpha^7}(x)=(x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14})=$$
$$=x^4+x^3+1.$$

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

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

1. Любой многочлен в поле характеристики 5 вместе с корнем α^3 имеет корнями и все сопряжённые с ним элементы $(\alpha^3)^5=\alpha^{15}$, $(\alpha^3)^{5^2}=\alpha^{75}$, $(\alpha^3)^{5^3}=\alpha^{375}$ 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 $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = \\
&= 4(4\alpha+3) + 3\alpha = 4\alpha + 2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = \\
&= 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\
&= 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3, \\
\alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\
&= 4(4\alpha+3) + 4\alpha + 1 = 3.
\end{aligned}$$

Ответ: $m(x) = x^2 + 3$.

2.31. Найти число I_2^6 неприводимых многочленов степени 6 среди $\mathbb{F}_2[x]$.

1. По одной формуле

$$\sum_{d|6} d \cdot I_2^d = 1 \cdot I_2^1 + 2 \cdot I_2^2 + 3 \cdot I_2^3 + 3 \cdot I_2^6 = 2^6 = 64.$$

Поскольку $I_2^1 = I_2^3 = 2$ и $I_2^2 = 1$, то

$$(64 - (2 + 2 + 6)/6) = 54/6 = 9.$$

2. По другой формуле

$$\begin{aligned}
I_2^6 &= \frac{1}{6} \sum_{d|6} \mu(d) \cdot 2^{\frac{6}{d}} = \\
&= \frac{1}{6} \left[\mu(1) \cdot 2^6 + \mu(2) \cdot 2^3 + \mu(3) \cdot 2^2 + \mu(6) \cdot 2^1 \right] = \\
&= \frac{1}{6} \left[64 - 8 - 4 + 2 \right] = 54/6 = 9.
\end{aligned}$$

2.32. Примитивен ли элемент x в полях

1) $\mathbb{F}_2[x]/(x^3+x+1) = F_1$?
2) $\mathbb{F}_2[x]/(x^4+x^3+x^2+x+1) = F_2$?

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 $\operatorname{ord} x$ нужно проверить на равенства $x^3 = 1$ и $x^5 = 1$.

   Первое равенство явно не имеет места, поэтому вычисляем с учётом $x^4 = x^3+x^2+x+1$:

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

   Это означает, что $\operatorname{ord} x = 5 \neq 15$, x — *не есть примитивный элемент* F, а м.м. $a(x)$ не примитивен.

2.33. Найти корни многочлена

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

Вычисление значений $f(x)$ для $x = 0, 1, \ldots, 4$, показывает, что $f(3) = 0$, т. е. $x = 3$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x-3 = x+2$, получим $x^3+3x^2+4x+4 = (x-3)\cdot\big(x^2+x+2\big)$.

Перебором элементов $x \in GF(5)$ убеждаемся, что $f_2(x) = x^2+x+2$ — неприводимый многочлен.

В поле $\mathbb{F}_5[x]/\big(x^2+x+2\big)$ корни многочлена $f_2(x)$ суть $\{\, x,\, x^5 \,\}$ и $x^2 = -x-2 = 4x+3$.

Вычисляем:

$$x^5 \;=\; \big(x^2\big)^2 x \;=\; x(4x+3)^2 \;=\; x\,\big(x^2+4x+4\big) \;=$$
$$=\; x(4x+3+4x+4) \;=\; x(3x+2) \;=\; 3x^2+2x \;=$$
$$=\; 2x+4+2x \;=\; 4x+4.$$

Ответ: $\{\, 3,\, x,\, 4x+4 \,\}$.

2.34. Является ли многочлен

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

примитивным?

Подстановкой в $f(x)$ всех элементов $0, \ldots, 4$ 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 $d = 24/2 = 12$, $24/3 = 8$. Вычисляем:

$$x^4 \;=\big(x^2\big)^2 \;=\; (4x+3)^2 \;=\; x^2+4x+4 \;=\; \ldots$$
$$\ldots \;=\; 3x+2 \;\neq\; 1,$$
$$x^8 \;=\big(x^4\big)^2 \;=\; (3x+2)^2 \;=\; -x^2+2x+4 \;=\; \ldots$$
$$\ldots \;=\; 3x+1 \neq\; 1.$$
$$x^{12} \;=x^8x^4 \;=\; (3x+1)(3x+2) \;=\; -x^2+4x+2 \;=\; \ldots$$
$$\ldots \;=\; 4 \neq\; 1.$$

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\big(x^2+x+2\big)$.

2.35. Для бинома $x^{40}-1 \in \mathbb{F}_5[x]$ определить количество и степени неприводимых сомножителей.

В каком минимальном поле расширения $\mathbb{F}_5[x]$ данный бином раскладывается на линейные множители?

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 $\{\,\overline{0}, \overline{1}, \ldots, \overline{7}\,\}$ разбиваются на орбиты:

$$\{\,\overline{0}\,\}, \{\,\overline{1}, \overline{5}\,\}, \{\,\overline{2}\,\}, \{\,\overline{3}, \overline{7}\,\}, \{\,\overline{4}\,\}, \{\,\overline{6}\,\}.$$

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 $x^{40} - 1 = \left(x^8 - 1\right)^5$ 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):

$$
\begin{aligned}
x^8-1 &= \left(x^4-1\right)\left(x^4+1\right),\\
x^4-1 &= \left(x^2-1\right)\left(x^2+1\right),\\
x^2-1 &= (x-1)(x+1),\\
x^2+1 &\equiv_5 x^2-4 = (x-2)(x+2),\\
x^4+1 &\equiv_5 x^4-4 = \left(x^2-2\right)\left(x^2+2\right).
\end{aligned}
$$

Итого в $\mathbb{F}_5[x]$:

$$
x^8-1 = (x+1)(x-1)(x+2)(x-2)\cdot \left(x^2+2\right)\left(x^2-2\right).
$$

И далее

$$
x^{40}-1 = (x+1)^5(x-1)^5(x+2)^5(x-2)^5\cdot \left(x^2+2\right)^5\left(x^2-2\right)^5.
$$

2.36. 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) $f(x)\in\mathbb{F}_5[x]$.

$\deg f(x)=2$ 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.

2.37. Найти корни многочлена

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

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, таким образом, $x = 2$ — 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 корней многочлена $2x^3 + 4x + 3$ будем искать корни

$$f_2(x) = 3 \cdot (2x^3 + 4x + 3) = x^3 + 2x + 4.$$

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 многочлен[9)].

В поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$ корнями многочлена $f_2(x) = 0$ будут x, x^5, x^{25}.

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 &= x^2(3x+1) = 3x^3 + x^2 = 4x + 3 + x^2 = \\ &= x^2 + 4x + 3; \\ x^{25} &= \big(x^5\big)^5 = \big(x^2 + 4x + 3\big)^5 = x^{10} + 4^5 x^5 + 3^5 = \\ &= x^{10} + 4\big(x^2 + 4x + 3\big) + 3 = x^{10} + 4x^2 + x. \end{aligned}$$

(поскольку $4^5 = 2^{10} = 102\underline{4}$ и $3^5 = 81 \cdot 3 = 24\underline{3}$).

Найдём отдельно x^{10}:

$$x^{10} = \big(x^5\big)^2 = \big(x^2 + 4x + 3\big)^2 =$$

[9)] а если бы это был многочлен 4-й степени?

$$= x^4 + x^2 + 3^2 + 3x^3 + 4x + x^2 =$$
$$= x^4 + 3x^3 + 2x^2 + 4x + 4 =$$
$$= \cancel{3}x^2 + \cancel{x} + \cancel{4}x + 3 + \cancel{2}x^2 + 4x + 4 = 4x + 2.$$

Продолжаем:

$$x^{25} = x^{10} + 4x^2 + x = \cancel{4}x + 2 + 4x^2 + \cancel{x} = 4x^2 + 2.$$

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

2.38. Найти корни многочлена

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

В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{\big(x^4 + x^3 + 1\big)}_{f_1(x)}\underbrace{\big(x^4 + x^3 + x^2 + x + 1\big)}_{f_2(x)}.$$

Уравнения $f_1(x) = 0$ и $f_2(x) = 0$ ранее были решены: их корни соответственно суть

$$x,\ x^2,\ x^3 + 1,\ x^3 + x^2 + x$$
$$\text{в поле } F_1 = \mathbb{F}_2[x]/\big(x^4 + x^3 + 1\big)$$

и $x,\ x^2,\ x^3,\ x^3 + x^2 + x + 1$

$$\text{в поле } F_2 = \mathbb{F}_2[x]/\left(x^4+x^3+x^2+x+1\right).$$

Степени обоих расширений поля $GF(2)$ совпадают 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:

$$\begin{gathered} x \mapsto x+1, \\ x^2 \mapsto (x+1)^2 = x^2+1, \\ x^3 \mapsto (x+1)^3 = x^3+x^2+x+1, \\ x^3+x^2+x+1 \mapsto \left(x^3+x^2+x+1\right)+\left(x^2+1\right)+ \\ +(x+1)+1 = x^3. \end{gathered}$$

Проверим, что, например, x^2+1 — корень $f(x)$:

$$\begin{aligned} f\left(x^2+1\right) &= \left(x^2+1\right)^8+\left(x^2+1\right)^4+\left(x^2+1\right)^2+ \\ &\quad +\left(x^2+1\right)+1 = \\ &= \left(x^{16}+1\right)+\left(x^8+1\right)+\left(x^4+1\right)+x^2. \end{aligned}$$

Очевидно $x^{16} = x$, $x^4 = x^3 + 1$ и
$x^8 = \left(x^3 + 1\right)^2 = x^6 + 1$.
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 $f\left(x^2+1\right)$ полученные полиномиальные представления степеней x, получим

$$f(x^2+1) = (x+1) + \left(x^3 + x^2 + x + 1\right) + x^3 + x^2 = 0.$$

Ответ: многочлен $f(x) = x^8 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$ имеет в поле $\mathbb{F}_2[x]/\left(x^4 + x^3 + 1\right)$ 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.

2.39. Найти корень многочлена

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

Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных:

$$f(x) = x^4 + 2x + 2 = \left(x^2 + ax + b\right)\left(x^2 + cx + d\right) =$$
$$= x^4 + cx^3 + dx^2 x + ax^3 + acx^2 + adx + bx^2 + bcx + bd =$$
$$= x^4 + (a+c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd.$$

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 $\mathbb{F}_3[x]/\left(x^4+2x+2\right)$.

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}:

$$\begin{aligned} x^9 &= \left(x^4\right)^2 x = (x+1)^2 x = x^3+2x^2+x; \\ x^{27} &= \left(x^9\right)^3 = \left(x^3+2x^2+x\right)^3 = x^9+2x^6+x^3 = \\ &= \ldots = x^3+x^2+x. \end{aligned}$$

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 $\mathbb{F}_3[x]/(f)$.

2.40. Найти корни многочлена $f(x)=x^5+x^2+1\in\mathbb{F}_2[x]$.

Поскольку $f(0)=f(1)=1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

$$x^5+x^2+1 = \left(x^2+x+1\right)\left(x^3+x^2\right)+1,$$

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\left(x^5+x^2+1\right)$.
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}:

$$\begin{aligned} x^8 &= x^5x^3 = \left(x^2+1\right)x^3 = x^5+x^3 = x^3+x^2+1; \\ x^{16} &= \left(x^8\right)^2 = \left(x^3+x^2+1\right)^2 = x^6+x^4+1 = \\ &= x^5x+x^4+1 = (x^3+x)+x^4+1 = \\ &= x^4+x^3+x+1. \end{aligned}$$

Ответ: в поле $\mathbb{F}_2[x]/\left(x^5+x^2+1\right)$ 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. Построить порождающую G и проверочную H матрицы для

1. тривиального кода утраивания;
2. кода проверки на чётность.

1. Код утраивания является линейным $(3, 1)$-кодом, у которого

$$G_{3,1} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \; I_1 = \begin{bmatrix} 1 \end{bmatrix}, \; P_{2,1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; H_{2,3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

2. Код проверки задаётся порождающей матрицей

$$G = \begin{bmatrix} I \\ 1 \ldots 1 \end{bmatrix} = \begin{bmatrix} 10 \ldots 0 \\ 01 \ldots 0 \\ 00 \ldots 1 \\ 11 \ldots 1 \end{bmatrix}$$

или проверочной матрицей

$$H = \begin{bmatrix} 1 \ldots 1 \; I \end{bmatrix} = \begin{bmatrix} 11 \ldots 1 \end{bmatrix}.$$

3.2. Для кода Хемминга, 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
$$\boldsymbol{u}_1 = [\,1\;1\;0\;1\,]^T,\ \boldsymbol{u}_2 = [\,1\;0\;0\;1\,]^T.$$

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 $\begin{bmatrix} I_3 & P \end{bmatrix}$, преобразуя *строки*:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{(1)\leftrightarrow(3)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow$$
$$\xrightarrow{(1)+(3)\mapsto(1)} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование.

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

3.3. 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

$$u(x) = x^2 + x \leftrightarrow [\,0\;1\;1\,]^T.$$

Для определения кодового расстояния найдём все кодовые слова:

$$\begin{aligned} v(x) &= g(x)(ax^2 + bx + c) = \\ &= \left(x^6 + x^3 + 1\right)\left(ax^2 + bx + c\right) = \\ &= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c. \end{aligned}$$

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 $u(x)$:

$$u(x) \;\mapsto\; v(x) = x^6 u(x) + r(x).$$

1) Вычисляем $x^6 u(x) = x^6\left(x^2 + x\right) = x^8 + x^7$.

2) Находим остаток $r(x)$ от деления $x^6 u(x)$ на $g(x)$:

$$\begin{array}{l|l} x^8 + x^7 & x^6 + x^3 + 1 \\ \cline{2-2} x^8 \quad + x^5 \quad + x^2 & x^2 + x \\ \cline{1-1} \quad x^7 + x^5 \quad + x^2 & \\ \quad x^7 \quad + x^4 \quad + x & \\ \cline{1-1} \quad x^5 + x^4 + x^2 + x & \end{array}$$

Т. о. $r(x) = x^5 + x^4 + x^2 + x$ и

$$v(x) = x^8 + x^7 + x^5 + x^4 + x^2 + x \leftrightarrow [0\,1\,1\,0\,1\,1\,\underline{0\,1\,1}]^T.$$

3.4. Рассмотрим код Хэмминга систематического кодирования с порождающим примитивным полиномом $a(x) = x^3 + x + 1$.

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,
3) $w_3(x) = x^6 + x^3 + x^2 + x$.

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. 126):

Находим позицию j ошибки.

1. $x^6 + x^2 + x = \left(x^3 + x + 1\right)^2 + \underline{x + 1}$, $j = 3$.

   Действительно,

$$w(\alpha) = \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1.$$

2. $x^6 + x^5 + x^3 + x^2 + x = \\ = \left(x^3 + x^2 + x + 1\right)\left(x^3 + x + 1\right) + \\ + \underline{x^2 + x + 1}$, $j = 5$;

   Действительно,

$$w(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^5 + \alpha + 1 + \alpha^2 + \alpha = \alpha^5.$$

3. $x^6 + x^3 + x^2 + x = \left(x^3 + x\right)\left(x^3 + x + 1\right) + \underline{0}$, т. е. ошибки не произошло.

3.5. Имеем $\alpha^{31} = 1$ и разложение F^* над $\mathbb{F}_2$ есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8\, \alpha^{16}\},$$
$$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}, \{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\},$$
$$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}, \{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\},$$
$$\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}.$$

3.6. Пусть $n = 5$ и α — примитивный элемент поля $\mathbb{F}_2^5 = F$. Найти разложение F^* над $\mathbb{F}_2$.

Будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов данного поля со с. 46.

С её помощью вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\
&= (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\
&= \alpha^3 + \alpha + 1 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \big(w(\alpha^2)\big)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1.$$

Решим соотношение Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \quad \deg\lambda(x) \leqslant 2.$$

с помощью обобщённого алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^5,$
$r_{-1}(x) = s(x),$
$\sigma_{-2}(x) = 0,$
$\sigma_{-1}(x) = 1.$

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$
$q_0(x) = \alpha^2 x,$
$r_0(x) = s(x),$
$\sigma_0(x) = -q_0(x) = \alpha^2 x.$

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x),$
$q_1(x) = \alpha^{12}x + \alpha^5,$
$r_1(x) = \alpha^{14}x^2 + 1,$
$\deg r_1(x) = 2 \leqslant r,$
$\sigma_1(x) = \sigma_{-1}(x) - \sigma_0(x)q_1(x) =$
$= 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) =$
$= \underbrace{\alpha^{14}x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} = \sigma(x).$

3.7. 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 $w(x)$.

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:

$$\text{-}5 \equiv_{15} 10, \qquad \text{-}8 \equiv_{15} 7.$$

3.8. Построить 31-разрядный БЧХ-код для исправления не менее $r = 3$ ошибок.

Имеем $n = 31 = 2^5 - 1$, $t = 5$, $\delta - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни α, α^2, α^3, α^4, α^5, α^6, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $C_1 = \{\, \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16} \,\}$.

При решении задачи 3.5 на с. 157 о разложение F^* на классы было установлено, что эти классы также будут пятиэлементными:

$$\begin{aligned}
C_2 &= \{\, \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17} \,\};\\
C_3 &= \{\, \alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18} \,\}.
\end{aligned}$$

На с. 35 были приведены неприводимые многочлены 5-й степени над $\mathbb{F}_2$: их шесть —

1) x^5+x^2+1,
2) x^5+x^3+1,
3) $x^5+x^3+x^2+x+1$,
4) $x^5+x^4+x^2+x+1$,
5) $x^5+x^4+x^3+x+1$,
6) $x^5+x^4+x^3+x^2+1$.

Во многих монографиях[10)] есть таблицы неприводимых многочленов. В них 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:

для многочлена № 3 —

$$\left(x^5+x^3+x^2+x+1\right)\Big|_{x=\alpha^3} = \alpha^{15}+\alpha^9+\alpha^6+\alpha^3+1 = \\ = (\alpha^3+1)^3+\alpha^4(\alpha^3+1)+\alpha(\alpha^3+1)+\alpha^3+1 = \ldots = 0,$$

для многочлена № 5 —

$$\left(x^5+x^4+x^3+x+1\right)\Big|_{x=\alpha^5} = \alpha^{25}+\alpha^{20}+\alpha^{15}+\alpha^5+1 = \\ = (\alpha^3+1)^5+(\alpha^3+1)^4+(\alpha^3+1)^3+\alpha^5+1 = \ldots = 0.$$

Таким образом,

$$g_2(x)=x^5+x^3+x^2+x+1,\ g_{\alpha^5}(x)=x^5+x^4+x^3+x+1$$

[10)] например, [8], Том 1, Таблица С.

и порождающий многочлен для $(31, 16, 7)$-кода БЧХ есть

$$g(x) = g_1(x) \cdot g_2(x) \cdot g_3(x) =$$
$$= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1,$$
$$\deg g(x) = m = 15,\ k = n - m = 16.$$

3.9. 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.

Для вычислений в поле F нам понадобится таблица, уже построенная на с. 46.

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = (\alpha^3 + \alpha^2)\, x + 1 :$$
$$\sigma(\alpha) = \alpha^4 + \alpha^3 + 1 = \alpha + 1 + \alpha^3 \neq 0;$$
$$\sigma(\alpha^2) = \alpha^5 + \alpha^4 + 1 = \alpha^2 + \alpha + \alpha + 1 + 1 = \alpha^2 \neq 0;$$
$$\ldots\ldots$$
$$\sigma(\alpha^9) = \alpha^{12} + \alpha^{11} + 1 =$$
$$= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 = \mathbf{0}.$$

Линейный полином $\sigma(x)$ имеет один корень α^9, и поэтому позиция единственной ошибки есть $-9 \equiv_{15} 6$.

4. Алгебраические основы криптографии

4.1. 1. Решить комбинаторную задачу.

Пусть p — простое число, большее 2. Сколько существует способов C раскрасить вершины правильного p-угольника в a цветов, если раскраски, получающиеся совмещением при вращении многоугольника вокруг своего центра, считать одинаковыми?

2. На основе полученного решения доказать малую теорему Ферма.

Теорема 4.27 (Ферма, малая). *Если целое a не делится на простое число p, то* $a^{p-1} \equiv_p 1$.

1. Если не отождествлять раскраски указанного типа, то всех раскрасок a^p.

Исключим одноцветные раскраски, остальных — $a^p - a$. Вращение раскрашенного более, чем в один цвет p-угольника вокруг своего центра на p углов $\frac{2\pi}{p}$, $2\frac{2\pi}{p}$, …, 2π даст неразличимые раскраски.

Итого, число различных раскрасок в более, чем один цвет равно $\frac{a^p-a}{p}$, и тогда всех раскрасок —

$$C = \frac{a^p - a}{p} + a = \frac{a\left(a^{p-1} - 1\right)}{p} + a.$$

2. Если $p = 2$, то a нечётно и утверждение теоремы тривиально.

Иначе показано, что C — целое число, откуда при $a \not\vdots p$ должно выполняться $(a^{p-1} - 1) \vdots p$, т. е. $a^{p-1} \equiv_p 1$.

4.2. Докажите справедливость сравнения $x^{(p-1)(q-1)} \equiv_n 1$ без использования теоремы Эйлера.

По малой теореме Ферма имеем

$$x^{p-1} \equiv_p 1.$$

Возводя обе части этого соотношения в степень $q-1$, получим

$$x^{(p-1)(q-1)} \equiv_p 1, \quad \text{и аналогично —} \quad x^{(p-1)(q-1)} \equiv_q 1.$$

Поэтому существуют такие целые u и v, что

$$x^{(p-1)(q-1)} = u \cdot p + 1 = v \cdot q + 1, \quad \text{откуда} \quad u \cdot p = v \cdot q.$$

Поскольку p и q — простые, найдутся и целые u' и v' такие, что u делится на q, v — на p:

$$u = u' \cdot q, \qquad v = v' \cdot p.$$

Но так как $n = pq$, это означает, что

$$x^{(p-1)(q-1)} = u' \cdot pq + 1, \quad \text{или} \quad x^{(p-1)(q-1)} \equiv_n 1.$$

4.3. В системе шифрования RSA по данным модулю $n = 91$ и экспоненте $e = 29$ найти ключ расшифрования d.

Заметим сначала, что значения $n = 91$ и $e = 29$ взаимно просты.

Найдём разложение $n = pq$ и значение функции Эйлера модуля:

$$91 = 7 \cdot 13; \quad \varphi(91) = 6 \cdot 12 = 72.$$

Число $e = 29$ не имеет общих делителей ни с $n = 91$, ни с $\varphi(n) = 72$, и значит годится в качестве ключа зашифрования.

Найдём d из условия $d \cdot 29 \equiv_{72} 1$ по алгоритму GE-InvZm:

1	72	0		
2	29	1	$q = 2$	(58 2)
3	14	-2	$q = 2$	(28 -4)
4	1	**5**	$q = 14$	
5	0			

Откуда $d = 5$.

4.4. Пусть в шифрсистеме RSA организатор (получатель сообщений) опубликовал открытый ключ ($n = 21, e = 11$). На стороне отправителя используя стандартную кодировку кириллического алфавита (А=01, Б=02, ...) зашифровать сообщение АБВ и расшифровать полученную криптограмму на стороне получателя.

Организатор выбрал $n = 21 = 3 \cdot 7$, поэтому $\varphi(21) = 2 \cdot 6 = 12$. Для определения d по алгоритму GE-InvZm решается сравнение

$$d \cdot 11 \equiv 1 \pmod{12}:$$

1	12	0	
2	11	1	$q = 1$
3	1	**-1**	$q = 11$
4	0		

Таким образом $d = -1 \equiv_{12} 11$ (к сожалению, оказалось $d = e$).

Отправитель кодирует сообщение $x_1 = $ А, $x_2 = $ Б, $x_3 = $ В словом 010203 и зашифровывает его:

$$\begin{aligned} y_1 &= 01^{11} = 1 \equiv_{21} 01, \\ y_2 &= 02^{11} = 2048 \equiv_{21} 11, \\ y_3 &= 03^{11} = 177147 \equiv_{21} 12. \end{aligned}$$

Получив криптограмму 011112, организатор расшифровывает его:

$$\begin{aligned} x_1 &= 01^{11} = 1 \equiv_{21} 1, \\ x_2 &= 11^{11} = 285311670611 \equiv_{21} 2, \\ x_3 &= 12^{11} = 743008370688 \equiv_{21} 3. \end{aligned}$$

4.5. Решить сравнения

а) $6^x \equiv_{11} 2$; б) $8^x \equiv_{11} 3$; в) $2^x \equiv_{13} 3$.

Используем алгоритм согласования (см. с. **??**).

(а) $\underline{6^x \equiv_{11} 2}$. Имеем $p = 11$, $a = 6$, $b = 2$.

1. $H = \lceil \sqrt{11} \rceil = 4$.
2. $6^4 = 1\,296 \equiv_{11} 9 = c$ $(1296 = 117 \cdot 11 + 9)$.
3. $u = 1, 2, 3, 4$

u	1	2	3	4
9^u	9	$9 \cdot 9 = 81$	$4 \cdot 9 = 36$	$3 \cdot 9 = 27$
$9^u \pmod{11}$	9	4	3	5

4. $v = 0, \ldots, 4$

v	0	1	2	3	4
6^v	1	6	36	216	1296
$2 \cdot 6^v$	2	12	72	432	2592
$2 \cdot 6^v \pmod{11}$	9	1	6	3	7

5. Совпал элемент 3 таблиц при $u = 3$ и $v = 3$. Отсюда $Hu - v = 4 \cdot 3 - 3 \equiv_{10} 9$.

Ответ: $x = 9$.

(б) $\underline{8^x \equiv_{11} 3}$. Имеем $p = 11$, $a = 8$, $b = 3$.

1. $H = 4$.

2. $8^4 = 4\,096 \equiv_{11} 4 = c$.

u	1	2	3	4
3. 4^u	4	$4 \cdot 4 = 16$	$5 \cdot 4 = 20$	$9 \cdot 4 = 36$
$4^u \pmod{11}$	4	5	9	3

4.

v	0	1	2	3	4
8^v	1	8	64	512	4096
$3 \cdot 8^v$	3				
$3 \cdot 8^v \pmod{11}$	3				

5. Совпал элемент 4 таблиц при $u = 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 4 = 16 \equiv_{10} 6$.

Ответ: $x = 6$.

(в) $\underline{2^x \equiv_{13} 3}$. Имеем $p = 13$, $a = 2$, $b = 3$.

1. $H = 4$.

2. $2^4 = 16 \equiv_{13} 3 = c$.

3.

u	1	2	3	4
c^u	3	9	27	3
$c^u \pmod{13}$	**3**	9	1	3

4.

v	0	1	2	3	4
2^v	1				
$3 \cdot 2^v$	3				
$3 \cdot 2^v \pmod{11}$	**3**				

5. Совпал элемент 3 таблиц при $u = 1, 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 1 = 4$, или $4 \cdot 4 \equiv_{12} 4$.

Ответ: $x = 4$.

4.6. Алиса A, Боб B и Кирилл C ведут секретную переписку, используя протокол DH, в качестве параметров которого они выбрали значения $p = 23$ и $\alpha = 2$. Секретные ключи Алисы, Боба и Кирилла суть

$$x_A = 5,\ x_B = 17;\ \text{и}\ \ x_C = 12 \text{ соответственно.}$$

Определить их открытые X_A, X_B и X_C и общие секретные ключи K_{AB}, K_{AC} и K_{BC}.

$$X_A = 2^5 = 32 \equiv_{23} 9;$$
$$X_B = 2^{17} = 131\,072 \equiv_{23} 18;$$
$$X_C = 2^{12} = 4\,096 \equiv_{23} 2;$$
$$K_{AB} = X_A^{17} = 9^{17} = 16\,677\,181\,699\,666\,569 \equiv_{23} 3;$$
$$K_{AC} = X_A^{12} = 9^{12} = 282\,429\,536\,481 \equiv_{23} 9;$$
$$K_{BC} = X_B^{12} = 18^{12} = 1\,156\,831\,381\,426\,176 \equiv_{23} 18.$$

4.7. В системе RSA выбраны простое числа $p = 11$ и $q = 17$ и экспонента $e = 13$. Определить открытый и секретный ключи и расшифровать шифртексты $y_1 = 02$ и $y_2 = 03$.

Определим модуль $n = pq = 11 \cdot 17 = 187$. При этом экспонента $e = 13$ взаимно проста с $p - 1 = 10$ и $q - 1 = 16$. Открытый ключ есть пара $(187, 13)$.

Определим ключ расшифрования d. Вычислив $\varphi(n) = (p-1)(q-1) = 160$, решим сравнение

$$d \cdot 13 \equiv_{160} 1.$$

1	160	0	
2	13	1	$q = 12$ (156 12)
3	4	-12	$q = 3$ (12 -36)
4	1	**37**	$q = 4$
5	0		

Получаем $d = 37$.

Расшифровываем криптограммы 02 и 03:

$$x_1 = 2^{37} = 137\,438\,953\,472 \equiv_{187} 117,$$
$$x_2 = 3^{37} = 450\,283\,905\,890\,997\,363 \equiv_{187} 141.$$

Список литературы

1. *Авдошин С. М., Набебин А. А.* Дискретная математика. Модулярная алгебра, криптография, кодирование. — М.: ДМК Пресс, 2017.
2. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. — М.: КомКнига, 2006.
3. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. — М.: КомКнига, 2006.
4. *Введение* в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.
5. *Вернер М.* Основы кодирования. Учебник для ВУЗов. — М: Техносфера, 2004.
6. *Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н.* Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.
7. *Касами Т., Токура Н., Ивадари Ё., Инагаки Я.* Теория кодирования. — М.: Мир, 1978.
8. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. — М.: Мир, 1988.

9. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.

10. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

11. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.

12. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.