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

Методические материалы по курсу

ПРИКЛАДНАЯ АЛГЕБРА

алгебраические основы кодирования, теории перечислений и шифрования

группы 320, 321, 323, 327, 328
осенний семестр 202X/202X уч. года

2023

Изложение теорий — задача сложная, и лучше всего идти по пути постепенного и последовательного рассмотрения объекта исследования.

Мацуо Команцу. Многообразие геометрии.

Предисловие

Данный конспект лекций подготовлен для бакалавров III-го «программистского» потока факультета ВМК МГУ, изучающих в 5-м семестре указанную дисциплину. В тексте рассматриваются приложения конечных алгебраических структур к задачам преобразования данных в целях защиты от случайных помех и несанкционированного доступа. Материал лекций как базируется на источниках, указанных в списке литературы (и, как правило, так или иначе переработан), так и подготовлен автором. При указанной переработке иногда приходилось идти, с учётом специфики аудитории и целей курса, на некоторое упрощение изложения.

Заметим, что стиль изложения в учебнике и непосредственно на лекциях различен. В учебнике все теоремы сопровождаются строгими доказательствами, а последовательное изложение обычно сопровождается различными пояснениями.

На лекциях же часто напоминают некоторые определения, формулы, важные при изложении материала

в данный момент. Этого избегают в учебниках, а повторение, как известно, — одно из главных условий запоминания и усвоения материала. По той же причине некоторые моменты рассуждений и доказательств излагаются часто подробнее (иногда — значительно), чем это принято в учебниках. То же относится и к примерам: на лекциях в начале рассмотрения той или иной темы, как правило, приводят очень простые примеры, ясно выявляющие те или иные моменты нового вводимого понятия. И наоборот, результаты, обозначения и др., считающиеся известными, не поясняются, чтобы не отвлекаться от хода рассуждений.

В данном конспекте неформальные «квазиопределения» выделяются *курсивом*, а моменты, на которые следует обратить внимание — *наклонным шрифтом*. Также опущены некоторые факультативные сведения, сообщаемые лектором при изложении той или иной темы (а неопущенные даны уменьшенным шрифтом). В связи со спецификой преподавания курса, в данный текст включены задачи с решениями.

Чтобы в дальнейшем не отвлекаться от порядка изложения, в первом разделе мы напоминаем уже, скорее всего, известные читателю, некоторые основные математические понятия и факты.

Глава 3 написана совместно с Д. А. Кропотовым. Его материалы также использованы при написании главы 2.

С. И. Гуров

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 называемое *носителем*, $e \in G$ — *нейтральный элемент*, а $\circ$ — бинарная операция на носителе, обеспечивающая выполнение следующих *законов* или *аксиом группы*:

$\Big[0)$ $\forall x, y\colon x \circ y \in G$ — *устойчивость* носителя;$\Big]$

1) $\forall x, y, z\colon (x \circ y) \circ z = x \circ (y \circ z)$ — *ассоциативность* групповой операции;

2) $\exists e\ \forall x : e \circ x = x \circ e = x$ — существование *нейтрального элемента* e;

3) $\forall x\ \exists y : y \circ x = x \circ y = e$ — *существование обратных элементов* ко всем $x \in G$.

Легко показываются единственность нейтрального элемента группы и единственность обратного элемента к данному. Действительно, пусть e_1 и e_2 — два нейтральных элемента группы G, а y_1 и y_2 — два обратных элемента к $x \in G$. Тогда по свойствам группы

$$e_1 = e_1 \circ e_2 = e_2\,,$$
$$y_1 = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_2 = y_2\,.$$

При отсутствии неясностей, группы обозначают $\langle G, \circ \rangle$ или, как и в случае всех *алгебраических систем* (АС) — просто символом носителя G.

Группы со свойством $x \circ y = y \circ x$ называются *абелевыми*[1]. Для них используют *аддитивную запись* $x+y$ групповой операции, нейтральный элемент называют *нулем (0)*, а обратный к элементу x — *противоположным* $(-x)$.

В общем случае используют мультипликативную запись групповой операции, вместо $\circ$ пишут $\cdot$ (или этот символ вообще опускают), обратный к x элемент обозначают x^{-1}, нейтральный — называют единицей, и когда группа имеет числовой характер, обозначают его символом 1.

Определим целую *степень элемента* при мультипликативной записи: положим $a^0 = e$, а для $n \in \mathbb{N}$ —

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ символов } a}\,, \quad a^{-n} = \left(a^{-1}\right)^n.$$

Легко показывается справедливость обычных свойств степени:

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

Аналогично определяется *кратное* na элемента a группы при аддитивной записи.

[1] В честь норвежского математика *Нильса Абеля* (Niels Henrik Abel, 1802–1829).

Если $|G| = n$, то G — *конечная группа порядка* n; в противном случае группа *бесконечная*.

Пример 1.2. 1. *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 $n \in \mathbb{N}$ — абелева группа по сложению.
- $\mathbb{Z}_n = \{ 0, 1, \dots, n-1 \}$, $n \geqslant 2$ — абелева группа по сложению, результат которого берётся по $\bmod n$.
- *Ненулевые* элементы множеств $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — абелевы группы относительно *умножения*.

2. *Симметрическая группа* S_n — группа всех подстановок n-элементного множества относительно операции их композиции. Нейтральный элемент S_n — единичная подстановка. Ясно, что $|S_n| = n!$, и легко показывается, что S_n *неабелева при* $n > 2$.

Прямой суммой $H \oplus G$ абелевых групп H и G называется группа, определённая на носителях H и G с заданной 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 абелевых групп — абелева группа.

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

$$a^n = e.$$

Тогда наименьшее такое n называют *порядком* этого элемента, символически $\operatorname{ord} a$; иначе данному элементу приписывают бесконечный порядок. Аналогично определяется порядок и для аддитивной записи группы. Например, в группе $\mathbb{Z}_6 = \{\,0, 1, 2, 3, 4, 5\,\}$ со сложением по $\bmod 6$ в качестве групповой операции, порядки элементов суть

$$\operatorname{ord} 1 = \operatorname{ord} 5 = 6, \quad \operatorname{ord} 2 = \operatorname{ord} 4 = 3, \quad \operatorname{ord} 3 = 2, \quad \operatorname{ord} 0 = 1. \quad (1.1)$$

Подгруппы, смежные классы, изоморфизмы. Если $\langle\, G, \cdot, e\,\rangle$ — группа, а H — подмножество G, само являющееся группой относительно операции $\cdot$, то $\langle\, H, \cdot, e\,\rangle$ — *подгруппа* G, символически $H \leqslant G$.

Чтобы проверить, является ли подмножество $H \subseteq G$ подгруппой группы $\langle\, G, \cdot, e\,\rangle$, достаточно установить справедливость

$$\forall\, a, b \in H\colon\ a \cdot b^{-1} \in H.$$

Ясно, что нейтральный элемент e входит в любую подгруппу. Одноэлементная *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 $\langle a\rangle$:

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

Теорема 1.3 (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.*

Для абелевых групп имеется усиление.

Лемма 1.4. *Пусть m — максимальный порядок элемента в конечной абелевой группе G. Тогда порядок любого элемента G делит m.*

Как пример — см. равенства 1.1.

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

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

Утверждение 1.5 (*о разложении группы на смежные классы*). *Левые смежные классы по данной подгруппе с разными представителями либо не пересекаются, либо совпадают, и в совокупности составляют всю группу. То же справедливо и для правых смежных классов.*

Все левые (как и все правые) смежные классы группы по данной подгруппе равномощны этой подгруппе.

Пример 1.6. Рассмотрим группу $G = \{0, 1, \ldots, 5\} \cong \mathbb{Z}_6$ и её подгруппу $H = \{0, 3\} \cong \mathbb{Z}_3$. Тогда $[\, G : H \,] = 6 : 2 = 3$, и смежные классы G по H суть

$$0 + H = \{0, 3\} = H, \quad 1 + H = \{1, 4\}, \quad 2 + H = \{2, 5\}.$$

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

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

Определение 1.7. 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* группы G по H, символически G/H.

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

Определение 1.8. Для групп $\langle\, G,\, \circ,\, e \,\rangle$ и $\langle\, G',\, \cdot,\, e' \,\rangle$ отображение $\varphi : G \to G'$ называется *изоморфизмом*, если оно биективно и

$$\varphi(a \circ b) \;=\; \varphi(a) \cdot \varphi(b).$$

Тогда эти группы называют *изоморфными*, символически $G \cong G'$.

Теорема 1.9 (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, гомоморфизмом является отображение $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$, сопоставляющее каждому целому числу его *вычет по* $\bmod n$ — остаток от деления на n (напомним, он всегда неотрицателен, а слово *вычет* (лат. residum) и означает *остаток*).

Символически, если G и G' — две группы и $\varphi : G \to G'$ — гомоморфизм, то

$$\operatorname{Im}(\varphi) \cong G/\operatorname{Ker}(\varphi),$$

где $\operatorname{Im}(\varphi) = \{\, \varphi(g) \mid g \in G \,\}$,
$\operatorname{Ker}(\varphi) = \{\, g \in G \mid \varphi(g) = e' \,\}$, e' — нейтральный элемент G'.

Циклические группы. Рассмотрим группы с записью групповой операции в мультипликативной форме. Если окажется, что *каждый* элемент группы C есть *целая* степень некоторого своего элемента a, то есть

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

то такая группа называется *циклической*, а сам элемент a — *порождающим* или *образующим*

При записи в аддитивной форме —

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

В циклической группе порождающий элемент обычно не единственен. Например, в группе $\langle\, \mathbb{Z},\, +,\, 0 \,\rangle$ имеется два порождающих элемента: -1 и $+1$.

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

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

с совпадением исходного и полученного положения — циклическая.

Для циклических групп возможны два случая.

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

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

Ясно, что она изоморфна группе $\langle\, \mathbb{Z},\ +,\ 0\,\rangle$.

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

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

Данная группа изоморфна аддитивной группе

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

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

Справедливость последнего соотношения вытекает из утверждения 1.26.

Итак, любая бесконечная 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*. Например, мультипликативная группа $\{\,1,\ -1,\ i,\ -i\,\}$ изморфна аддитивной $\mathbb{Z}_4$.

В $\mathbb{Z}_n$ все элементы порядка n являются порождающими. Поэтому их число совпадает с количеством натуральных чисел, взаимно простых с n.

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

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, $\varphi(n) \geqslant 2$.

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,

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 6.$$

1.2 Кольца

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*

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

Дистрибутивные законы обеспечивают тот факт, что нейтральный элемент ноль по сложению будет являться и нулём по умножению: $\forall x \in R: \ x \cdot 0 = 0$. Поэтому любую абелеву группу G можно формально превратить в кольцо, задав на ней *нулевое умножение*: $\forall x, y \in G: x \cdot y = 0$.

Отметим, что в кольце деление не постулируется.

Классическими примерами колец являются:

1) целые числа $\mathbb{Z}$ с обычными операциями сложения и умножения;

2) $\mathbb{Z}_n = \{ 0, 1, \ldots, n-1 \}$, $n \geqslant 2$ с обычными операциями сложения и умножения, результат которых берётся по $\bmod n$.

   Это кольцо его называют *кольцом классов вычетов*[2)], рассматривая его элементы как остатки от деления целых на n, а результаты обычных операций сложения и умножения берутся по $\bmod n$.

[2)] Интуитивно, это кольцо получается из отрезка $[\, 0, \ n-1 \,]$ соединением его концов, что дало название «кольцо» всей алгебраической структуре с аналогичными $\mathbb{Z}_n$ свойствами.

3) $\mathbb{Q}$ — кольцо рациональных чисел, являющееся полем. Это простейшее поле характеристики 0; оно является основным объектом исследования в теории чисел. Пополнение его по различным неэквивалентным нормам даёт поля *вещественных* чисел $\mathbb{R}$ и *p-адических* чисел $\mathbb{Q}_p$, где p — произвольное простое число.

Кольца специального вида.

- *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 оно называется *кольцом с единицей* или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$.
- *Тривиальное кольцо* — одноэлементное множество $\{0\}$; в нём и только в нём $0 = 1$.
- Кольцо R — *без делителей нуля*, если для любых ненулевых его элементов a и b невозможно, чтобы $a \cdot b = 0$.

  Например, *кольцо квадратных матриц* нетривиального порядка $n \geqslant 2$ 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* (*областью целостности*, ID, Integral Domain).

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

2. Множество чётных $2\mathbb{Z}$ с обычными операциями сложения и умножения есть нетривиальное ассоциативно-коммутативное кольцо без делителей нуля. Оно не является целостным, поскольку не унитально.
3. Кольцо $\mathbb{Z}_n$ при составном n имеет делители нуля ($3 \cdot 2 = 0$ в $\mathbb{Z}_6$) и поэтому не является областью целостности.

В унитальном коммутативном кольце элементы a и b называют *обратимыми*, если

$$a \cdot b = 1 \quad (\text{случай } a = b \text{ не исключается}).$$

Например, в кольце целых $\mathbb{Z}$ обратимы только 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 же p — простое число, то обратимы *все ненулевые* элементы кольца $\mathbb{Z}_p$, и $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ (то есть это кольцо является *полем*, см. далее).

Определение 1.13. Ненулевой 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 ± 1, простые числа и противоположные к ним.

Определение 1.14. Целостное кольцо, в котором каждый ненулевой элемент либо обратим, либо *однозначно* (с точностью до перестановки сомножителей и умножения на обратимые элементы) представляется в виде произведения неприводимых элементов называется *факториальным* (*кольцом с однозначным разложением на множители, гауссовым кольцом*).

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

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

Подмножество L кольца $\langle R, +, \cdot, 0 \rangle$ вновь окажется кольцом и будет называться его *подкольцом*, если L есть подгруппа *аддитивной группы* $\langle R, +, 0 \rangle$, устойчивая относительно операции умножения $\cdot$.

Например, при любом $n \in \mathbb{N}_0$ множество $n\mathbb{Z}$ является подкольцом кольца целых $\mathbb{Z}$. Легко видеть, что всякое подкольцо содержит 0 основного кольца и наследует свойства ассоциативности и коммутативности.

Подкольцо *собственное*, если оно не совпадает со всем кольцом[3)].

Идеалы колец и факторкóльца. Важнейшими подкольцами являются идеалы. Их роль в теории колец можно сравнить с ролью нормальных подгрупп в

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

теории групп.

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

$$\forall i \in I \ \forall r \in R\colon \ i \cdot r \in I.$$

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

Само кольцо и его нуль 0 — *тривиальные идеалы* кольца. Идеалы, не совпадающие со всем кольцом, называют *собственными*.

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

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

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

Например, $2\mathbb{Z} = (2)$ — главный идеал кольца $\mathbb{Z}$. Любое кольцо всегда имеет два *тривиальных* главных идеала: $(0) = \{0\}$ и $(1) = R$.

Целостные кольца, в которых все идеалы главные, называют *кольцами главных идеалов, КГИ* (PID, Principal Ideal Domain).

Примеры КГИ:

- Кольцо целых $\mathbb{Z}$ — все его идеалы имеют вид $(n) = n\mathbb{Z} = \{\, 0, \pm n, \pm 2n, \ldots \}$, $n \in \mathbb{N}$.

  Ясно, что для натуральных несовпадающих n и m если $m \mid n$, то $(n) \subset (m)$.

- Кольцо $\mathbb{Z}_n$ — любой ненулевой идеал содержит НОД своих ненулевых элементов и им порождается.
  Например, для $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}$: $\mathbb{Z}_6 = (1)$, $\{0, 2, 4\} = (2)$, $\{0, 3\} = (3)$ и $\{0\} = (0)$.

Все КГИ факториальны.

Пример правого неглавного идеала в кольце матриц порядка n: совокупность матриц, у которых все столбцы, кроме 1-го — нулевые.

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

Определение 1.17. *Максимальным идеалом* коммутативного кольца называется всякий его *собственный* идеал, строго не содержащийся ни в каком другом собственном идеале.

В нетривиальном коммутативном кольце всегда существует максимальный идеал.

Пример 1.18. В кольце целых чисел $\mathbb{Z}$

- 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.

Утверждение 1.19. *Максимальные идеалы в* $\mathbb{Z}$ *имеют вид* (p), *где* p — *простое число.*

Доказательство. Покажем сначала, что максимальные идеалы в $\mathbb{Z}$ имеют вид (p).

Пусть p — простое, но идеал (p) не максимальный. Тогда, поскольку $\mathbb{Z}$ — КГИ, найдётся такое число i, $0 < i < p$, что $(p) \subset (i)$. Это означает, что $i \mid p$, откуда либо $i = p$, либо $i = 1$. Первый случай невозможен, а второй означает, что идеал $(1) = \mathbb{Z}$ несобственный.

Обратно, если натуральное n имеет собственный делитель m. Тогда $(n) \subset (m)$ и идеал (n) — не максимальный. □

Определение 1.20. *Классом вычетов* $\overline{r}_I$ по модулю идеала I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ с представителем $r \in R$ называют множество

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

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.

Например, класс вычетов по модулю $(n) = n\mathbb{Z} \trianglelefteqslant \mathbb{Z}$ с представителем r есть

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

Здесь представитель r — остаток от деления некоторого целого на n, $0 \leqslant r < n$. Для $r = 3$ и $n = 5$ имеем: $\overline{3} = \{ 3, 3 \pm 5, 3 \pm 10, \dots \} = 3 + 5\mathbb{Z}$.

На классах вычетов определены операции сложения и умножения, индуцированные кольцевыми операциями над представителями, а результаты операций берутся по модулю идеала. При этом совокупность

всех классов вычетов кольца R по модулю идеала I образуют *факторкольцо*, символически R/I.

Понятно, что $\mathbb{Z}_n \cong \mathbb{Z}/(n)$. Например,

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

где $\overline{0}$ — все чётные числа, а $\overline{1}$ — все нечётные. Этот изоморфизм позволяет, переходя к соответствующему кольцу, опускать черту над символами представителей классов, как мы и будем обычно поступать.

Факторкольцо по максимальному идеалу является полем (см. 24). Поэтому кольцо $\mathbb{Z}_p$ при простом p есть поле.

Евклидовы кольца. В кольце целых $\mathbb{Z}$ возможно деление с остатком любого числа на любое ненулевое. При этом остаток, по определению неотрицательный, либо равен нулю, либо строго меньше модуля делителя. Желание описать кольца, в которых возможна аналогичная операция, приводит к следующему понятию.

Определение 1.21. 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

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

В большинстве пособий на норму накладывается ещё одно требование — выполнение неравенства $N(a) \leqslant N(ab)$. Однако оно носит технический характер: хотя для такой нормы легче доказываются некоторые свойства евклидовых колец, её легко

получить из вышеопределённой нормы. Основные же свойства евклидовых колец остаются в силе и без этого дополнительного свойства.

Именно наличие нормы даёт возможность определить деление элементов кольца друг на друга с остатком.

Пример 1.22.

- 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.
  Пример — кольцо $\mathbb{R}[x]$ многочленов с действительными коэффициентами.

- Кольцо *целых гауссовых чисел* $\mathbb{Z}[i]$ (комплексные числа, которых вещественная и мнимая части целые) — евклидово с нормой $N(a+ib) = a^2 + b^2$.

- Можно показать неевклидовость КГИ

$$\left\{ m + n\frac{1+\sqrt{-19}}{2} \;\middle|\; m, n \in \mathbb{Z} \right\}.$$

Все евклидовы кольца — КГИ.

1.3 Поля

Определение 1.23. Целостное кольцо, в котором все ненулевые элементы обратимы, называется *полем*[4].

Поле также можно определить как пятёрку $\langle K, +, \cdot, 0, 1 \rangle$, в которой обе полученный из неё АС — $\langle K, +, 0 \rangle$ (*аддитивная*) и $\langle \{K \setminus \{0\}, \cdot, 1 \rangle = K^*$ (*мультипликативная*) являются *абелевыми группами*, связанными для всех $x, y, z \in K$ дистрибутивным законом $x \cdot (y + z) = x \cdot y + x \cdot z$.

Для нас важны следующие факты:

1) факторкольцо R/I является полем если и только если идеал I кольца R — *максимальный*;

2) ненулевые элементы поля K образуют абелеву группу K^* относительно *умножения*, её называют *мультипликативной группой* данного поля.

Ясно, что произвольное поле K
- можно рассматривать как евклидово кольцо с нормой, равной 1 для всех ненулевых элементов;
- имеет только два (*тривиальных*) идеала: $(0) = \{0\}$ и $(1) = K$, причём $K/(0) = K$ и $K/(1) = \{0\}$.

Подмножество K' поля K, само являющееся полем и устойчивое относительно сужения на него операций из K, называется *подполем*; при $K' \neq K$ это — *собственное* подполе. Примеры бесконечных полей и их подполей — числовые поля

[4] Первоначально у Р. Дедекинда — Körper, что означает *корпус* и подчёркивает замкнутость объекта

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C};$$

а конечных полей — $\mathbb{Z}_p \subset \mathbb{Z}_{p^n}$, p — простое число, n — натуральное.

Поле, не обладающее собственным подполем, называется *простым*. Поле рациональных чисел $\mathbb{Q}$ — простое.

Теорема 1.24 (Фробениус). *В каждом поле содержится только одно простое подполе, которое изморфно либо $\mathbb{Q}$, либо $\mathbb{Z}_p$, p — простое.*

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

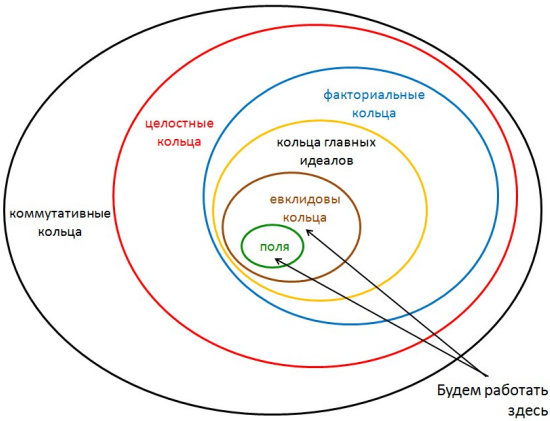


Рис. 1.1. От ассоциативных колец к полям

1.4 Векторные пространства, гомоморфизмы, сравнения

Абстрактные векторные пространства

Определение 1.25. *Абстрактным векторным пространством* над полем $K = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\langle V, K; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — множество *ве́кторов*, являющееся абелевой группой с нулём 0 по сложению $+$;
- $\cdot$ — бинарная операция *умножения элемента* («числа́») *из* K *на вектор из* V: $K \times V \dot{\to} V$,

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 элементов из V и их умножение на число из K определим покомпонентно. Получившаяся структура $V(K^n)$ 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 по $\bmod 2$, умножения $\&$ и нулевым элементом $\widetilde{0}$.

n-мерное координатное пространство V над полем K имеет n-элементный базис; при этом обычно рассматривают *естественный базис*

$$\boldsymbol{e}^1 = [\,1\,0\,\ldots\,0\,], \quad \ldots, \quad \boldsymbol{e}^n = [\,0\,0\,\ldots\,1\,].$$

Линейная оболочка базиса совпадает со всем пространством V, иными словами, любой вектор $x \in V$ есть (единственная) линейная комбинация базисных векторов:

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

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 систем различных типов.

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

Гомоморфизмами называют 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

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

Утверждение 1.26. *Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма.*

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 $(m \times n)$-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

$$a = b \pmod{m}, \quad \text{или} \quad a \equiv_m b, \tag{1.2}$$

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 (1.2) 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), (2) и (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:

$$\left\{ \begin{array}{l} ad \equiv_m bd, \\ \text{НОД}\,(d, m) = 1 \end{array} \right. \Rightarrow \ a \equiv_m b;$$

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

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

Глава 2

Конечные кольца и поля

Систематически конечные поля стали изучаться с начала XIX века. Простые поля были исследованы Ферма, Эйлером, Лагранжем, Лежандром и Гауссом. Современная теория конечных полей — раздел алгебры, актуальность которого чрезвычайно возросла в связи с разнообразными приложениями в комбинаторике, теории кодирования, криптографии, телекоммуникации.

2.1 Поля Галуа

Простые поля Галуа — поля классов вычетов по модулю простого числа. Нам известно, что для $n \in \mathbb{N}$ —

$(n) = \{\ 0,\ \pm n,\ \pm 2n,\ \pm 3n,\ \ldots,\ \}$ — идеал кольца $\mathbb{Z}$ и

$$\mathbb{Z}/(n) = \left\{\ \overline{0},\ \overline{1},\ \ldots,\ \overline{n-1}\ \right\}$$

— кольцо классов вычетов кольца целых $\mathbb{Z}$ по модулю идеала (n):

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

Черту над символами классов вычетов часто не ставят, обозначая класс его *представителем* — наимень-

шим по модулю положительным элементом. Так мы и будем поступать в дальнейшем.

Далее везде p *обозначает простое число*. Ясно, что идеал (p) — максимальный и $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ — *поле*. Его называют *простым полем Галуа* (prime field) и обозначают $\mathbb{F}_p$ или $GF(p)$[1]. Вообще *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...

---

[1] В честь *Эвари́ста Галуа́* (Evariste Galois, 1811–1832), основоположника современной высшей алгебры — теории абстрактных алгебраических структур. Первым обозначением обычно пользуются математики, а вторым — специалисты по информатике.

[2] То есть 2 — делитель 0, или, точнее 2 есть *нильпотент индекса* 2 *в кольце* $\mathbb{Z}/(4)$. Как тут не вспомнить высказывание *Ч. Пирса*: «*Абсолютная непогрешимость может быть присуща лишь Папе Римскому и экономическим советникам, но я совершенно уверен, что она не присуща таблице умножения*».

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

$$1 + \ldots + 1 = p1 = 0.$$

Наименьшее такое p есть порядок аддитивной группы поля K, его называют *характеристикой поля* и обозначают $\operatorname{char} K$.

Величина $\operatorname{char} K$ может быть только простым числом: иначе, если $\operatorname{char} K = u \cdot v$ при $u, v > 1$, получим $(u \cdot 1) \cdot v = 0$, то есть наличие в K делителей нуля.

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

По теореме 1.24 Фробениуса $\{0, 1, \ldots, p-1\} \cong \mathbb{Z}_p$ — минимальное подполе любого поля ненулевой характеристики p.

Существуют и *бесконечные* поля положительной характеристики. Например, такое поле может быть построено следующим образом.

Рассмотрим *поле $K(x)$ рациональных функций* над конечном полем K, элементами которого являются "дроби" $\frac{P}{Q}$, где P и $Q \not\equiv 0$ — *многочлены* от формальной переменной x с коэффициентами из K. На множестве данных "дробей" вводятся отношение эквивалентности, операции сложения, умножения и деления, аналогично тому, 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 ненулевой характеристики p.*

Будем рассматривать далее исключительно конечные поля. В них возможно сильное упрощение вычисления степеней сумм.

Лемма 2.1 (бином Ньютона по mod p). *В поле ненулевой характеристики p справедливо тождество*

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

Доказательство. В любом коммутативном кольце верна формула степени бинома

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

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

Данную формулу в шутку называют «*биномом двоечника*».

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. 17 обозначением, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ — мультипликативная группа (по умножению) q-элементного поля Галуа $\mathbb{F}_q$. Далее будет показано, что возможен только случай $q = p^n$, p — простое, n — натуральное.

Теорема 2.2. $\mathbb{F}_q^*$ — *циклическая группа.*

Доказательство. Пусть m — максимальный порядок элемента в мультипликативной группе поля.

По лемме 1.4 для абелевых групп имеем, что порядок каждого элемента $x \neq 0$ группы $\mathbb{F}_q$ делит m, то есть x является корнем $x^m = 1$.

У этого уравнения не более m корней, поэтому $m = q-1$, и все ненулевые элементы $\mathbb{F}_q$ — его корни. А это и означает, что группа $\mathbb{F}_q^*$ циклическая: существует такой элемент, что его порядок совпадает с порядком группы. □

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

Например, $\mathbb{F}_{11}^* = \langle \{1, 2 \ldots, 10\}, \cdot_{11}, 1 \rangle \cong$

$$\cong \mathbb{Z}_{10} = \langle \{0, \ldots, 9\}, +_{10}, 0 \rangle.$$

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

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

Представление элементов $\mathbb{F}_q$ степенями своего примитивного элемента α называют их представлением *в полярных координатах* (при этом формально полагают $0 = \alpha^{-\infty}$).

Найдём примитивные элементы поля $\mathbb{F}_{11}$; их всего 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 элемент 3 — *не является примитивным*.

Ещё примитивные элементы: 6, 7, и 8.

Как ускорить процесс нахождения примитивных элементов простого поля Галуа?

Если примарное разложение числа $p-1$

• *известно* — тогда 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. $p = 11$ (это наш случай), $p - 1 = 10 = 2 \cdot 5$. Поэтому проверяем степени $\frac{10}{5} = 2$ и $\frac{10}{2} = 5$ элементов 2 и 3 из $\mathbb{F}_{11}^*$:

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

$3^2 = 9 \neq 1,\ 3^5 = 243 \equiv_{11} 1 \ \Rightarrow\ 3$ — *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: $\alpha^{12} \equiv_{37} 1$ и $\alpha^{18} \equiv_{37} 1$.

Например, $3^{18} = 387\,420\,489 = 10\,470\,824 \cdot 37 + 1$, и поэтому элемент 3 — не примитивный в поле $GF(37)$.

• *неизвестно* — для этого случая эффективных алгоритмов не найдено.

Однако, если найден один примитивный элемент α поля $\mathbb{F}_p$, то остальные могут быть получены как его

степени α^k, где k — взаимно просто с $p-1=|\mathbb{F}_p^*|$. В нашем примере $p=11$, 2 — примитивный элемент $\mathbb{F}_{11}$, а взаимно простые с 10 значения суть 1, 3, 7 и 9. В результате получим все примитивные элементы $\mathbb{F}_{11}$:

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

Порождающие элементы простых полей Галуа. Порождающие элементы группы $\mathbb{F}_p^*$ называют также *первообразными корнями по модулю p*. Найдем наименьшие первообразные корни по модулям некоторых простых чисел.

$p=2$. Группа $\mathbb{F}_2^*$ состоит из одного элемента 1, он же является первообразным корнем.

$p=3$. Первообразный корень 2 — единственный неединичный элемент $\mathbb{F}_3^*$.

$p=5$. Поскольку $2^2=4\neq 1$, порядок 2 равен 4. Других вариантов нет, поскольку порядок элемента — делитель порядка мультипликативной группы. Значит, 2 — первообразный корень.

$p=7$. Снова $2^2=4\neq 1$, но $2^3=8\equiv_7 1$ и $\deg 2=3$.

Проверяем второй делитель 3 у $p-1=6$. Поскольку $3^2=9\not\equiv_7 1,\quad 3^3=27\not\equiv_7 1$, то 3 — первообразный корень.

Таблица наименьших первообразных корней π группы $\mathbb{F}_p^*$

p	3	5	7	11	13	17	19	23	29	31	37	41
π	2	2	3	2	2	3	2	2	2	3	3	7

Кольца многочленов: деление, корни. Легко видеть, что множество всех многочленов от формальной переменной с коэффициентами из некоторого поля K образует евклидово кольцо; его обозначают $K[x]$ и называют *кольцом многочленов над K (x — формальная переменная)*. Нетрудно видеть, что это кольцо евклидово.

Далее будем рассматривать кольца многочленов $\mathbb{F}_p[x]$ над простыми полями Галуа $\mathbb{F}_p$. На рис. 2.1 приведён пример деления «уголком» многочлена $x^7 + x^4 + x^2 + 1$ на $x^3 + x + 1$ в кольце $\mathbb{F}_2[x]$; здесь получилось частное $x^4 + x^2 + 1$ с остатком x.

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

Рис. 2.1. Пример деления многочленов над $\mathbb{F}_2$.

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

Из представления для многочленов

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

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

2.2 Неприводимые многочлены и расширение полей

Определение 2.3. Многочлен над некоторым полем называется *неприводимым* или *неразложимым*, если он не представим в виде произведения двух многочленов ненулевой степени.

Ясно, что все линейные многочлены неприводимы.

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

При этом ясно, что свойство многочлена «быть неприводимым» зависит от поля, над котором он задан. Например, многочлен $f(x) = x^2 + 1$ неприводим над $\mathbb{R}$, но приводим над $\mathbb{F}_2$: $x^2 + 1 = (x + 1)^2$.

В кольце многочленов над полем

$\mathbb{Q}$ — существуют неприводимые многочлены любой 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 над простыми полями Галуа, то есть вида

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, \;\; a_i \in \mathbb{F}_p, \; i = \overline{0, n-1}.$$

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

Вторая степень: $x^2 + ax + b$.

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$. Аналогично заключаем, что свободный член любого неприводимого многочлена над $\mathbb{F}_2$ равен 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 делимость $x + 1$, получаем условие

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

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 неприводимый многочлен 2-й степени, 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. 69).

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

Для дальнейшего будет важно, что поскольку кольца многочленов евклидовы, они являются КГИ.

Расширения простых полей

Определение 2.5. Поле K называется *расширением* поля F, если $F \subseteq K$.

С помощью идеалов неприводимых многочленов над простыми полями $\mathbb{F}_p$ можно строить новые конечные поля, являющиеся расширениями первых.

Для этого в кольце многочленов $\mathbb{F}_p[x]$ выберем некоторый неприводимый многочлен $a(x)$. В этом случае идеал $(a(x))$ — множество многочленов, кратных $a(x)$ — будет максимальным в $\mathbb{F}_p[x]$: доказательство проводится аналогично доказательству максимальности идеала (p) в $\mathbb{Z}$ при простом p (см. утверждение 1.19).

Рассмотрим теперь факторкольцо $\mathbb{F}_p[x]/(a(x))$. Оно будет состоять из классов $\overline{r(x)}$ вычетов (смежности) вида $\overline{r(x)} = r(x) + (a(x))$, где $r(x)$ — остаток от деления некоторого многочлена из $\mathbb{F}_p[x]$ на многочлен $a(x)$. Но мы договорились обозначать эти классы их *представителями* — в рассматриваемом кольце это многочлены $r(x)$. Ясно, что если $\deg a(x) = n$, то степени данных многочленов не выше $n-1$, то есть их и классов смежности всего p^n штук.

Построенное факторкольцо многочленов будет являться полем относительно сложения (коэффициентов по $\bmod p$) и умножения по модулю идеала $(a(x))$.

Построенное поле обозначают называют *расширением n-й степени* простого поля $\mathbb{F}_p$, символически $\mathbb{F}_p^n$, $GF(p^n)$ или $GF(q)$, $q = p^n$.

Аналогичным образом можно построить все конечные поля. Справедлива

Теорема 2.6. *Каждое конечное поле характеристики p изоморфно кольцу вычетов кольца многочленов $\mathbb{F}_p[x]$ по модулю идеала, порождённого неприводимым многочленом.*

Расширения простых полей впервые появились в работе *Э. Галуа* «Из теории чисел» (1830) и полями Галуа сначала

называли поля, построенные вышеуказанным способом. В докладе, прочитанном в 1893 г. на Международном математическом конгрессе в Чикаго, американский математик *Э. Г. Мур* (E. H. Moore) сообщил о доказательстве теоремы: «Любое конечное поле есть поле Галуа».

Пример 2.7. 1. Пусть $p = 2$ и $n = 2$. В кольце $\mathbb{F}_2[x]$ всех многочленов от x с коэффициентами из $\mathbb{F}_2 = \{0, 1\}$ имеется единственный неприводимый многочлен порядка 2: это $a(x) = x^2+x+1$. Его идеал $(a(x))$ является максимальным и состоит из многочленов, кратных порождающему $a(x)$: $(a(x)) = a(x) \cdot q(x)$, $q(x) \in \mathbb{F}_2[x]$.

Факторкольцо $\mathbb{F}_2[x]/(x^2+x+1)$ является полем $\mathbb{F}_2^2$ расширения 2-й степени исходного поля $\mathbb{F}_2$ и состоит из четырёх элементов: 0, 1, x и $x + 1$.

Не забудем, что, например, под x следует понимать все многочлены вида $x + q(x)(x^2 + x + 1)$, $q(x) \in \mathbb{F}_2[x]$.

2.1. Пусть $p = 3$ и $n = 2$. В кольце $\mathbb{F}_3[x]$ всех многочленов от x с коэффициентами из $\mathbb{F}_3 = \{0, 1, 2\}$ возьмём неприводимый многочлен $a(x) = x^2 + x + 2$.

Факторкольцо $\mathbb{F}_3[x]/(x^2+x+2)$ является полем $\mathbb{F}_3^2$ расширения 2-й степени исходного поля $\mathbb{F}_3$ и состоит из $3^2 = 9$-и элементов

$$0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2.$$

В этом поле $x^2 = -x-2 = 2x+1$, и поэтому, например,

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

2.2. Если в качестве порождающего расширенное поле взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен, например $b(x) = x^2 + 2x + 2$, то будет построено поле,

состоящее из тех же элементов. Отличие его от построенного ранее будет состоять в том, что теперь результат умножения многочленов нужно брать по модулю идеала $(b(x))$. В этом поле $x^2 = -2x - 2 = x + 1$, и, например,

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

Может возникнуть вопрос: *почему в обозначении расширения поля не используется многочлен $a(x)$, с помощью которого оно построено?* Ответ даёт

Теорема 2.8. *Любые два поля, содержащие одинаковое число элементов, изоморфны.*

Казалось бы данную теорему можно легко доказать: пусть F_1 и F_2 — два поля, полученные расширением какого-то простого поля Галуа двумя разными неприводимыми многочленами одной степени, и $\varphi : F_1 \to F_2$ — отображение некоторого порождающего элемента мультипликативной группы F_1^* в некоторый порождающей элемент мультипликативной группы F_2^*, а нуля F_1 — в нуль F_2. Тогда $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, поскольку все конечные циклические группы одного порядка изоморфны.

Однако не любой изоморфизм мультипликативных групп будет изоморфизмом самих полей: необходимо выполнение равенства $\varphi(a + b) = \varphi(a) + \varphi(b)$ для всех элементов a, b из F_1, а это обеспечивается не любым отображением указанного вида.

Доказательство теоремы 2.8 может быть найдено во многих пособиях, например, в [9] или [6].

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 2.9. Расширение Галуа может быть проведено и в поле нулевой характеристики. В кольце $\mathbb{R}[x]$ многочленов с действительными коэффициентами возьмём неприводимый многочлен x^2+1 и построим поле

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

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

Поля Галуа как векторные пространства. Итак, элементами поля $GF(p^n)$ являются многочлены над $GF(p)$ степени не выше n.

В то же время имеется очевидное взаимнооднозначное соответствие между многочленами из $GF(p^n)$ и векторами из координатного пространства над $GF(p)$:

$$b_0 + b_1x + \ldots + b_{n-1}x^{n-1} \ \leftrightarrow\ [\ b_0\ b_1\ \ldots\ b_{n-1}\ ].$$

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

Стандартный базис n-мерного координатного векторного пространства над простым полем Галуа $GF(p)$ составляют векторы

$$[1\,0\,0\ldots0],\quad [0\,1\,0\ldots0],\quad \ldots,\quad [0\,0\,0\ldots1],$$

или же, переходя к многочленам —

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

Представление элементов $GF(p^n)$ векторами в стандартном базисе или в виде многочленов называют представлением поля *в прямоугольных координатах*.

Приведём таблицу ненулевых элементов поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4+x+1\big)$, записанных многочленами от примитивного элемента $\alpha = x$. 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	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:

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

Заметим, что переход от степенного представления к векторному достаточно прост, а обратный переход — очень сложен.

Теорема 2.10. *Поле* $\mathbb{F}_p^n$ *содержит подполе (изоморфное)* $\mathbb{F}_p^m$, *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. □

2.3 Вычисления в конечных кольцах и полях

Алгоритм Евклида (ЕА) — в своём простейшем варианте применяют для нахождения НОД (a, b) *натуральных* чисел a и b.

Заметим, что общий делитель пары чисел (a, b), $a \geqslant b$, остаётся им и для пары $(a - kb, b)$, $k \in \mathbb{N}$, $a - kb \geqslant 0$. Поэтому вместо a в паре (a, b) можно взять остаток r от деления нацело a на b, и затем, переставив числа, повторить процедуру для (b, r). Процесс закончится, поскольку числа в паре уменьшаются, но остаются неотрицательными. В результате образуется пара $(r, 0)$, и ясно, что НОД $(a, b) = r$.

Алгоритм Евклида[3)]
нахождения НОД (a, b), $a \geqslant b$, $a, b \in \mathbb{N}$

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

Пример 2.11. Найдём НОД $(252, 105)$ по алгоритму Евклида.

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

Теорема 2.12 (соотношение Безу[4)]). *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 $r = u + (-q)v$, $q \in \mathbb{N}$. Это справедливо для каждого шага алгоритма Евклида, откуда следует указанное представление. □

Замечание. Коэффициенты Безу могут быть выбраны неоднозначно, например

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

[3)] Этот алгоритм дважды описал в «Началах» Евклид, но не был им открыт: он упоминается в «Топике» Аристотеля, появившейся на 50 лет ранее «Начал».

[4)] Для взаимно простых чисел открыто *Клодом 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. 51).

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 $r = b$.
1. Перевычислим r как остаток от деления a на 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 2.13. 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 $(105, 42)$ 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 Gen-EA-I нахождения элемента c^{-1} в кольце $\mathbb{Z}_m$ при условии $\text{НОД}(c, m) = 1$ (что гарантирует существование решения).

1. Запишем исходные данные в виде двухстрочной таблицы

$$\begin{matrix} m & 0 \\ c & 1 \end{matrix}$$

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

3. Домножим последнюю строку на q, вычтем результат из предпоследней и запишем полученное в качестве новой 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 2.14. Решим в кольце (поле) $\mathbb{Z}/(101)$ сравнение

$$4y = 1.$$

Применим алгоритм Gen-EA-I, для удобства нумеруя строки и записывая значения частных и вычитаемые строки:

1	101	0	
2	4	1	$q = 25$ (100 25)
3	1	-25	$q = 4$
4	0		

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

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

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

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 решим в кольце $\mathbb{F}_p[x]$ соотношение Безу

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

а затем, при необходимости, выразим $y(x)$ 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 $\chi_i(x)$, так как нас интересует только значения $y_i(x)$, $i = 0, 1, \ldots$.

Удобна следующая форма алгоритма.

Обобщённый алгоритм Евклида Gen-EA-I 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 $r_{-1}(x)$, находя 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 $r_{n-1}(x) = c$ — 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 2.15. 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: $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
$q_1(x) = 4x$,
$r_1(x) = 3, \quad \deg r_1(x) = 0$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) =$
$= 1 + 4x\left(x^2 + 5\right) = 4x^3 + 6x + 1.$

Шаг 3: Остаток $r_1(x) = 3$ отличается от 1 на множитель-константу. Для получения решения вычисляем элемент $3^{-1} \equiv_7 5$ и домножаем на него y_1:
$5y_1(x) = y(x) = 6x^3 + 2x + 5.$

Ответ: в поле $\mathbb{F}_7[x]/\left(x^4 + x^3 + x^2 + 3\right)$ имеем
$$(x^2 + x + 3)^{-1} = 6x^3 + 2x + 5.$$

2.4 Минимальные многочлены элементов расширенных полей

Минимальные многочлены: определение. Пусть дано простое поле $\mathbb{F}_p$, кольцо $\mathbb{F}_p[x]$ многочленов над ним и расширенное поле $\mathbb{F}_p^n$.

Рассмотрим элемент β расширенного поля $\mathbb{F}_p^n$ и будем интересоваться многочленами из $\mathbb{F}_p[x]$, для которых он является корнем.

Определение 2.16. *Минимальным многочленом (м. м.)* или *минимальной функцией* элемента β поля $\mathbb{F}_p^n$ называется нормированный многочлен $m_\beta(x)$ наименьшей степени кольца $\mathbb{F}_p[x]$, для которого β является корнем.

Пример 2.17. Ниже приведены м. м. из кольца многочленов $\mathbb{F}_2[x]$ для некоторых элементов β поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/\left(x^4+x+1\right)$ с порождающем элементом $\alpha = x$.

$\beta \in \mathbb{F}_2[x]/\left(x^4+x+1\right)$	$m_\beta(x) \in \mathbb{F}_2[x]$
$\beta = 0$	x
$\beta = 1$	$x+1$
$\beta = \alpha = x$	x^4+x+1
$\beta = \alpha^5 = x^2+x$	x^2+x+1

Составим линейный многочлен $f(x) = x-\beta$. Он нормирован и имеет β своим корнем. Однако, поскольку $\beta \in \mathbb{F}_p^n$, то $f(x) \in \mathbb{F}_{p^n}[x] \neq \mathbb{F}_p[x]$, и поэтому $f(x)$ не является м. м. элемента β. и поэтому он не является м. м. элемента β.

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 $x \in F$.

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 m первыми элементами базиса $\left\{\, 1,\, x,\, \ldots,\, x^{n-1} \,\right\}$ поля F, что невозможно.

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

Теорема 2.18. *Для каждого элемента β поля $\mathbb{F}_p^n$ существует м. м., и его степень не превосходит n.*

Доказательство. Рассмотрим элементы 1, β, β^2, …, β^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, …, c_n, что

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

Поэтому β — корень многочлена

$$c(x) = c_0 + c_1x + \ldots + c_nx^n.$$

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

Теорема 2.19. *Минимальные многочлены неразложимы.*

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

$$m_\beta(x) = m_1(x) \cdot m_2(x),$$
$$1 < \deg m_1(x), \deg m_2(x) < \deg m.$$

Тогда из $m_\beta(\beta) = 0$ следует, что $m_1(\beta) = 0$ и/или $m_2(\beta) = 0$, т. е. β является корнем какого-то многочлена степени меньшей, чем степень $m_\beta(x)$, что невозможно. □

Теорема 2.20. *Пусть $m_\beta(x)$ — м. м. для элемента β некоторого поля Галуа характеристики p, а $f(x)$ — многочлен из $\mathbb{F}_p[x]$, 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 более одного, то они должны взаимно делить друг друга, а значит, различаться на обратимый множитель-константу. Поскольку м. м. нормирован, эти многочлены совпадают.

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 не окажется, что

1) $\beta^{p^d} = \beta$, и тогда

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

Раскрыв скобки, получим явный вид $m_\beta(x)$.
Ясно, что коэффициентами в $m_\beta(x)$ могут оказаться только элементы поля $\mathbb{F}_p$, иначе — ошибка в вычислениях.

2) $\beta^{p^d} = x$, и тогда $m_\beta(x)$ есть многочлен $a(x)$ после нормировки, как и для случая $\beta = x$.
Ясно, что в бинарном случае нормировка не требуется.

Пример 2.21. Найдём минимальные многочлены элементов $\beta_1 = x^2+x$ и $\beta_1 = x+1$ поля $\mathbb{F}_2[x]/\big(x^4+x+1\big)$.

В этом поле $x^4 = x+1$.

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

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

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

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

Найдём его коэффициенты:

$$\beta^2+\beta = \big(x^2+x+1\big)+\big(x^2+x\big) = 1,$$
$$\beta^3 = \big(x^2+x+1\big)\cdot\big(x^2+x\big) = \ldots = 1.$$

Окончательно имеем $m_\beta(x) = x^2+x+1$[5].

[5] Заметим, что в данном случае вычислений коэффициентов можно было и не проводить: единственный неприводимый над $\mathbb{F}_2$ многочлен 2-й степени есть x^2+x+1.

2. $\beta = \beta_2 = x + 1$. Элементы, сопряжённые с β:

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

поэтому $m_\beta(x) = a(x) = x^4 + x + 1$.

2.5 Поле разложения многочлена

Свойства многочленов над конечным полем. В общем случае в разложении многочлена $f(x)$ над $\mathbb{F}_p$ на неприводимые множители встречаются многочлены степени выше 1. Это связано с недостаточным количеством элементов в поле $\mathbb{F}_p$.

Определение 2.22. *Полем разложения многочлена* $f(x) \in \mathbb{F}_p[x]$ называют наименьшее по n расширение $\mathbb{F}_p^n$ поля $\mathbb{F}_p$, в котором $f(x)$ разлагается в *произведение линейных над* $\mathbb{F}_p^n$ *многочленов.*

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

Поле комплексных чисел $\mathbb{C}$ является расширением поля действительных чисел $\mathbb{R}$. Квадратный многочлен $x^2 + 1$ неприводим в $\mathbb{R}[x]$ (не имеет действительных корней), но разлагается на линейные множители в $\mathbb{C}[x]$:

$$x^2 + 1 = (x + i)(x - i).$$

Пример 2.23. Многочлен $x^5 + 1 \in \mathbb{F}_2[x]$ приводим:

$$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Но второй сомножитель в этом разложении уже неприводим (см. с. 39).

Рассмотрим расширение $\mathbb{F}_2 \subset \mathbb{F}_2[x]/(x^4+x^3+x^2+x+1) = F$. В этом поле многочлен x^5+1 уже раскладывается на линейные множители.

Действительно, мультипликативная группа поля F — циклическая группа из 15 элементов. Поэтому в ней есть подгруппа из 5 элементов. Каждый элемент этой подгруппы является корнем многочлена x^5+1 (в поле $\operatorname{char} 2$ выполняется $1 = -1$). Получаем разложение x^5+1 на линейные множители.

Этот пример можно обобщить.

Теорема 2.24. *Для любого многочлена $f(x) \in k[x]$ существует поле его разложения $K \supseteq k$.*

Иными словами, в кольце $K[x]$ многочлен $f(x)$ разлагается на линейные множители.

Доказательство. Построим цепочку расширений полей

$$F = F_0 \subset F_1 \subset \dots$$

по следующему правилу. Разложим $f(x)$ на неприводимые множители в поле F_i. Если все эти множители имеют степень 1, то $K = F_i$.

Если в разложении есть неприводимый множитель $g(x)$, степени больше 1, то следующее поле в цепочке определим как

$$F_{i+1} = F_i[x]/(g(x)).$$

Итак, цепочка расширений заканчивается на поле разложения.

Осталось доказать, что процесс построения цепочки расширений всегда останавливается. Для этого заметим, что указанный многочлен $g(x)$ в поле F_{i+1} обязательно имеет корень — это x.

Поэтому количество сомножителей степени 1 в разложении многочлена $f(x)$ на неприводимые увеличивается при переходе от поля F_i к полю F_{i+1} хотя бы на один. Поэтому процесс построения расширений рано или поздно остановится. □

Пример 2.25. Найдём поле разложения многочлена $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$. Убеждаемся в начале, что ни один из элементов $\mathbb{F}_7 = \{0, 1, \ldots, 6\}$ не является корнем $f(x)$, поэтому данный многочлен 2-й степени неприводим в $\mathbb{F}_7[x]$.

Образуем поле $\mathbb{F}_7[x]/(x^2+1)$. Это и есть $7^2 = 49$-элементное поле разложения многочлена $f(x) = x^2+1$ над $\mathbb{F}_7$. В нём многочлен $f(x)$ имеет два корня: x и $-x = 6x$.

Теорема 2.26. *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 $x\left(x^{q-1} - 1\right) = x^q - x = 0$. □

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 мультипликативной группы поля $\mathbb{F}_p^n$.

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

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

Из теоремы 2.26 следует ещё один способ нахождения обратных элементов в поле $\mathbb{F}_p^n$, удобный при небольших p и n:

$$x^{p^n} = x \;\Rightarrow\; x^{-1} = x^{p^n-2}.$$

Найдём, например, элемент, обратный к $\alpha = x + 1$ в поле $F = \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2^3$. Здесь $p^n - 2 = 6$, $x^3 = x + 1$ и

$$\begin{aligned}\alpha^{-1} = \alpha^6 = (x+1)^6 = (x+1)^{2^2} \cdot (x+1)^2 = \\ = (x^4+1)(x^2+1) = (x^2+x+1)(x^2+1) = \\ = x^4 + x^3 + \cancel{x^2} + \cancel{x^2} + x + 1 = x^4 = x^2 + x.\end{aligned}$$

Теорема 2.27 (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
$$x^m - 1 = x^r y^k - 1 = x^r \underbrace{(y^k - 1)} + \underbrace{x^r - 1}.$$

□

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

Пример 2.28. 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 2.29. *Все неприводимые многочлены n-й степени над $\mathbb{F}_p$ делят бином $x^{p^n} - x$.*

Доказательство. $n = 1$. 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 $\mathbb{F}_p[x]$ и строим поле $\mathbb{F}_p[x]/\big(f(x)\big) \cong \mathbb{F}_p^n$.

В нём x — корень корень $f(x)$, и, по теореме 2.26, бинома $x^{p^n-1} - 1$. По свойствам м. м. (теорема 2.20) бином $x^{p^n-1} - 1$ делится на $f(x) = m_x(x)$. □

Пример 2.30. 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 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 2.31. *Любой неприводимый многочлен, делящий бином $x^{p^n}-x$, имеет степень, не превосходящую 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 $1, x, \ldots, x^{k-1}$.

Поскольку бином $x^{p^n}-x$ делится на f, то в поле F имеем

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

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. По формуле бинома в конечном поле (см. лемму 2.1 на с. 33) и $\alpha^{p^n} = \alpha$ для любого $\alpha \in F$ получим

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

или

$$\beta^{p^n} - \beta = 0,$$

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

Резюмируем: в кольце $\mathbb{F}_p[x]$ делителями бинома $x^{p^n} - x$ могут быть неприводимые многочлены только степени $\leqslant n$, при этом степени n — *все* из них.

Корни неприводимого многочлена. Следующая теорема позволяет находить все корни неприводимого многочлена из $\mathbb{F}_p[x]$, если известен хотя бы один корень: достаточно возводить его последовательно в степени p.

Теорема 2.32 (о корнях неприводимого многочлена). *Пусть $\beta \in \mathbb{F}_p^n$ — корень неприводимого многочлена*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}_p[x].$$

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 $n > 1$.

Используя бином Ньютона по $\bmod p$ (см. лемму 2.1) устанавливаем, что

$$\begin{aligned} f(\beta) = 0 &\Leftrightarrow (f(\beta))^p = 0 \\ &\Leftrightarrow (a_0 + a_1\beta + \ldots + a_n\beta^n)^p = 0 \\ &\Leftrightarrow a_0 + a_1\beta^p + \ldots + a_n(\beta^p)^n = 0 \\ &\Leftrightarrow f(\beta^p) = 0. \end{aligned}$$

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 $f(x)$.

Пусть $\beta^{p^\ell} = \beta^{p^k}$, $\ell \leqslant k$. Мы знаем, что $\beta^{p^n} = \beta$. С другой стороны, поскольку

$$\beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^\ell}\right)^{p^{n-k}} = \beta^{p^{n-k+\ell}},$$

то β — корень уравнения $x^{p^{n-k+\ell}-1} - 1 = 0$.

Из следствия 2) теоремы 2.26 (в поле $\mathbb{F}_p^n$ справедливо представление $x^{p^n-1}-1 = (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1})$) получаем $n - k + \ell \geqslant n$, так что $\ell \geqslant k$. Поэтому $\ell = k$, и все выписанные выше корни различны. □

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

Корни $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$ 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 только что доказанную теорему.

Для нахождения корней приводимого многочлена можно предварительно разложить его на неприводимые множители.

Пример 2.33. 1. Найдём корни неприводимого над $\mathbb{F}_2$ многочлена

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

Эти корни будут элементами поля $\mathbb{F}_2[x]/(f(x))$ разложения многочлена $f(x)$ над $\mathbb{F}_2$. Один из корней получаем немедленно — это x, а остальные три — суть x^2, $x^4 = x^3 + 1$ и, наконец,

$$x^8 = x^6 + 1 = \big(x^3 + 1\big)\, x^2 + 1 = x^5 + x^2 + 1 =$$
$$= \big(x^4 + x\big) + x^2 + 1 = x^3 + 1 + x + x^2 + 1 = x^3 + x^2 + x.$$

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

Покажем, что, например, x^2 — действительно корень $f(x)$: поскольку

$$f(x^2) = x^8 + x^6 + 1$$

и $x^8 = x^6 + 1$, то $f(x^2) = 0$.

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; находим, что

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

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 нём $\varphi(x)$ имеет корни x и x^3.

В этом поле $x^2 = -2x - 2 = x + 1$, поэтому

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

Ответ: поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right) = \mathbb{F}_3^2$ является полем разложения многочлена $f(x) = x^4 + 2x^3 + x^2 + x + 1 \in \mathbb{F}_3[x]$ — минимальном полем характеристики 3, в котором многочлен $f(x)$ имеет корни; они суть 1, 2, x и $2x + 1$.

3. Найдём минимальное поле характеристики 3, в котором многочлен $f(x) = x^4 + 2x^2 + 2x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители, а в данном поле — все корни этого многочлена.

Перебором элементов $\mathbb{F}_3 = \{0, 1, 2\}$ находим, что $f(x) = 0 \pmod 3$ лишь при $x = 2$, что даёт разложение

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

Далее устанавливаем, что многочлен $x^3 + 2x^2 + 2$ имеет в $\mathbb{F}_3$ единственный корень 2, справедливо представление

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

и последний сомножитель неразложим. Поэтому заключаем, что образованное им поле $\mathbb{F}_3[x]/(x^2+x+2)$ является полем разложения исходного многочлена $f(x) = x^4 + 2x^2 + 2x + 2 \in \mathbb{F}_3[x]$.

В этом поле $x^2 = -x - 2 = 2x + 1$ и многочлен $f(x)$ имеет корни: 2 (2-й степени), а также x и

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

2.6 О существовании неприводимых многочленов и полей. Примитивные многочлены

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

Теорема 2.34 (Гаусс). $\displaystyle\sum_{d|n} d \cdot I_p^d = p^n.$

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 $I_2^1 = 2$, так как имеется два неприводимых над $\mathbb{F}_2$ многочлена: x и $x+1$ (все линейные многочлены неприводимы). Отсюда $I_2^7 = (128-2)/7 = 18$.

Из формулы Гаусса имеются важные

Следствия.

1. Простая оценка ($n \geqslant 2$)

$$n \cdot I_p^n = p^n - \sum_{d|n,\, k<n} d \cdot I_p^d \geqslant$$

$$\geqslant p^n - p^{n-1} - \ldots - p - 1 = p^n - \frac{p^n - 1}{p - 1} > 0$$

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

2. Отсюда, в свою очередь, следует 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 натуральных n: $\mu(1) = 1$, и для $n > 1$ —

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

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

Основное свойство функции Мёбиуса: сумма её значений по всем делителям целого числа n, не равного единице, равна нулю

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}.$$

Теорема 2.35 (формула Гаусса).

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

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

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

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

Примитивные многочлены

Определение 2.36. Минимальный многочлен примитивного элемента поля называется *примитивным многочленом*.

Иными словами, нормированный неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$ примитивен, если x — примитивный элемент мультипликативной группы поля $\mathbb{F}_p[x]/(f(x))$.

Пример 2.37. 1) Неприводимый многочлен

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

примитивен: элемент x поля $\mathbb{F}_2[x]/\big(x^4+x+1\big)$ является порождающим его мультипликативной группы.

Действительно, данная мультипликативная группа состоит из $2^4 - 1 = 15 = 3\cdot 5$ элементов, при этом $x^3 \neq 1$ и

$$x^5 = x\cdot x^4 = x\cdot(x+1) = x^2 + x \neq 1.$$

2) Неприводимый многочлен

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

не примитивен: мультипликативная группа поля $\mathbb{F}_2[x]/(g(x))$ состоит из 15-и элементов, а порядок элемента x есть 5:

$$x^5 = x \cdot x^4 = x^4 + x^3 + x^2 + x = \\ = (x^3 + x^2 + x + 1) + x^3 + x^2 + x = 1.$$

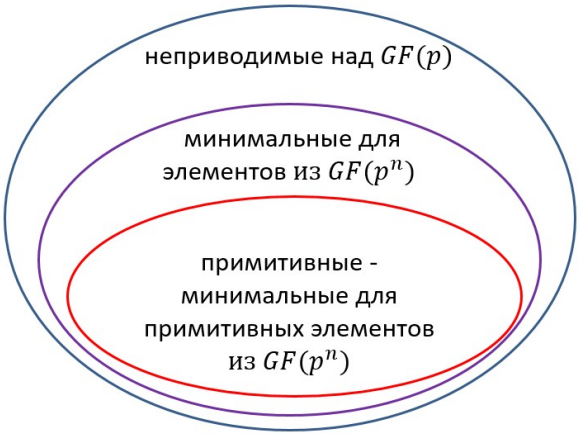


Рис. 2.2. Соотношение множеств неприводимых, минимальных и примитивных многочленов

2.7 Циклические подпространства колец вычетов

Идеалы в кольцах классов вычетов. Рассмотрим факторкольцо 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 2.38. *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. 19).

2. Пусть $g = u\varphi \pmod f$. Тогда из $\deg g = \deg \varphi$ следует, что u — константа, и при $u = 1$ получим $g = \varphi$, а 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 $\deg u = n - k$, то есть требуемое. □

Циклическое пространство

Определение 2.39. Подпространство координатного линейного пространства F^n над полем F называется *циклическим*, если вместе с вектором $[\,a_0\,\ldots\,a_{n-1}\,]$ оно содержит вектор $[\,a_{n-1}\,a_0\,\ldots\,a_{n-2}\,]$.

Рассмотрим кольцо $R = \mathbb{F}_p[x]/(x^n-1)$. Его элементами будут многочлены из $\mathbb{F}_p[x]$ степени $< n$.

В этом кольце, рассматриваемом как векторное пространство, имеется естественный базис $1,\ x,\ \ldots,\ x^{n-1}$. Циклический сдвиг координат в этом базисе равносилен умножению на x:

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

Поэтому R называют *циклическим полиномиальным кольцом.*

Следующая теорема указывает, когда и подпространство циклического полиномиального кольца оказывается циклическим.

Теорема 2.40. *В кольце классов вычетов по модулю бинома x^n-1 подпространство является циклическим если и только если оно идеал.*

Доказательство. Если подпространство I — идеал циклического полиномиального кольца R, то оно замкнуто относительно умножения на x, а это умножение и есть циклический сдвиг. Следовательно подпространство I — циклическое.

Обратно, пусть I — циклическое подпространство кольца R. 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 R. □

Пример 2.41. Рассмотрим два многочлена над $\mathbb{F}_2$: приводимый бином $f(x) = x^4 - 1 = x^4 + 1$ и его неприводимый делитель $\varphi(x) = x + 1$.

В кольце $R_4 = \mathbb{F}_2[x]/\big(x^4 - 1\big)$ все кратные φ многочлены имеют вид

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

$a, b, c \in \{\, 0,\ 1 \,\}$ 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	$x^3 + 1$

Убеждаемся, что если $g \in (\varphi)$, то и $g \cdot x \in (\varphi)$.

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

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

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

Пусть эти многочлены имеют степени $s_1, \ldots, s_k$ соответственно и $s_1 + \ldots + s_k = n$.

Все 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 s, то β^p, β^{p^2}, $\ldots$ $\beta^{p^{s-1}}$ — также его корни. Отсюда следует, что величины k и $s_1, \ldots, s_k$ можно найти, разбив элементы $\mathbb{Z}_n$ на *орбиты* отображения $\ell \mapsto p\ell \pmod{n}$.

Пример 2.42. 1. Вернёмся к примеру с разложением бинома $x^{15} + 1 \in \mathbb{F}_2[x]$. Относительно умножения на 2 элементы $\mathbb{Z}_{15}$ 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.

В данном случае эти многочлены легко определяются: линейный неприводимый многочлен есть, очевидно, $x+1$, квадратный неприводимый многочлен над $\mathbb{F}_2$ единственен (это x^2+x+1), также в $\mathbb{F}_2$ имеются только три неприводимых многочлена 4-й степени. И полученное разложение совпадает с найденным ранее в на с. 63.

2. Найдём структуру разложения бинома x^9-1 над $\mathbb{F}_2$. Относительно умножения на 2 элементы $\mathbb{Z}_9$ на три орбиты:

$$\{0\},\ \{1,2,4,8,7,5\},\ \{3,6\}.$$

Поэтому данный бином разлагается в произведение одного линейного многочлена $(x+1)$, одного квадратного (x^2+x+1) и некоторого неприводимого многочлена 6-й степени.

3. Найдём структуру разложения 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 бином $x^{23}-1$ разлагается в произведение линейного многочлена $x+1$ и двух неприводимых многочленов 11-й степени.

Глава 3

Коды, исправляющие ошибки

Теория корректирующих кодов начала развиваться после опубликования в 1948 г. теоретической статьи *Клода Шеннона* (Claude Elwood Shannon, 1916–2001) «Математическая теория связи», и особенно после работ М. Голея (1949) и Р. Хэмминга (1950).

В свой основополагающей статье Шеннон установил i. a., что по каналу связи информация может передаваться безошибочно, если скорость передачи не превышает пропускной способности канала. Однако это утверждение является теоремой чистого существования, которое не даёт конкретных способов создания кодов.

Метод построения кодов, исправляющих одну ошибку опубликован Р. Хэммингом позднее статьи К. Шеннона, но был переоткрыт им ранее (см. ниже): Хэмминг ждал получения патента, закрепляющего именно его авторство.

3.1 Блоковое кодирование

Задача помехоустойчивого кодирования. Рассматривается поток *битов*, проходящий по каналу с шумом, вследствие чего возникают ошибки. Канал может быть пространственным (линия связи) или же временны́м (хранение данных).

Примем модель возникновения ошибок, согласно которой под воздействием шума некоторые биты слу-

чайно, независимо и с равными вероятностями могут оказаться инвертированными, но вставок, выпадений или стираний (замен на некоторой символ, отличный от 0 и 1) битов нет (*двоичный симметричный канал*).

Задача: обеспечить возможность автоматического исправления максимального числа ошибок, построив *помехозащищённый код*, и имеющий, по возможности, простые алгоритмы кодирования и декодирования.

Одним из возможных естественных подходов к решению данной проблемы состоит в разбиении всего потока информации на *сообщения* — последовательные непересекающиеся блоки битов фиксированной длины k. После этого каждый блок можно кодировать (модифицировать):

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

б) в зависимости от предыдущих, реализуя *свёрточное* или *потоковое кодирование*.

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

- $S = \{0,1\}^k$ — пространство всех возможных *сообщений* (*информационных слов*) длины k каждое; k называют *рангом кода*.
- Для обеспечения помехозащищённости вместо сообщений передают *кодовые слова* (*кодослова*)

большей длины $n = k + m$, $m > 0$, и поэтому такое кодирование называют *избыточным*.
При $m = 0$ или $k = 0$ говорят о *тривиальных кодах*.

- *Кодом* будем называть совокупность C всех кодовых слов, $|C| = Q = 2^k$ — *мощность кода*;
- *Кодированием* называют взаимнооднозначное преобразование сообщения в кодовое слово.

  Кодирование, при котором биты сообщения переходят в заранее фиксированные позиции кодового слова, называют *разделимым* (сообщение вложено в кодослово). Тогда соответствующие k бит кодового слова называют *информационными*, а остальные m — *проверочными*.
- *Декодирование* — восстановление сообщения по принятому, возможно искажённому слову.
- $R = k/n$ — *скорость* кода, основная его характеристика; m/n — *избыточность* кода.

Впервые (1942) конструктивный метод построения кодов, способных корректировать одиночные ошибки и с простым декодированием предложил выдающийся английский статистик, биолог-эволюционист и генетик *Рональд А. Фишер* (Sir Ronald Aylmer Fisher, 1890–1962). Однако широко известным он стал только после опубликования в 1950 г. статьи американского математика *Ричарда Хэмминга* (Richard Wesley Hamming, 1915–1998).

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

Кодовое расстояние

Определение 3.1. Минимальное хэммингово расстояние между словами кода C называется его *кодовым расстоянием* или *минимальным расстоянием кода*, символически $d(C)$ или просто d.

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

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

Ясно, что код может исправить до r ошибок, если в B^n шары радиусов r с центрами в кодовых словах не имеют общих точек. 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, что практически невозможно уже начиная с $k = 50$.

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

Простейшие коды. Блоковое кодирование и декодирование

1. В простейшим случае блоки сообщений содержат по $k = 1$ биту, то есть пространство сообщений есть $S = \{0, 1\}$.

Код с повторением каждого символа $2r + 1$ раз, очевидно, исправит до $r \geqslant 1$ ошибок. Простейший его вариант — *утраивание*: $0 \mapsto 000$, $1 \mapsto 111$.

Этот код содержит $m = 2r$ проверочных символов и имеет крайне низкую скорость.

2. *Код с одной проверкой на чётность* содержит только один проверочный символ, являющийся суммой по $\bmod 2$ информационных символов. Поэтому общее число единиц в кодовом слове кода всегда чётно. Если принятое слово содержит чётное число единиц, то оно декодируется отбрасыванием проверочного символа, в противном случае происходит отказ от декодирования. Понятно, что такой код обнаружит ошибки только нечётной кратности, а остальные — пропустит.

Данный код применяется, в частности, в com-портах настольных ПК, обеспечивающих передачу данных от клавиатуры к системному блоку.

Рассмотренные простейшие коды представляют собой в некотором смысле «предельные случаи» двоичного кодирования. Код с повторением может иметь произвольную корректирующую способность, но он имеет минимальную скорость. Код с одной проверкой на чётность обладает максимальной скоростью, но способен только обнаруживать и только нечётное число ошибок.

3. *Матричный код* прост, но способен в удачных случаях справить несколько ошибок. Он предполагает представление исходного сообщения в виде квадратной таблицы и формирование двух векторов проверки одной проверкой на чётность — см. рис. 3.1.

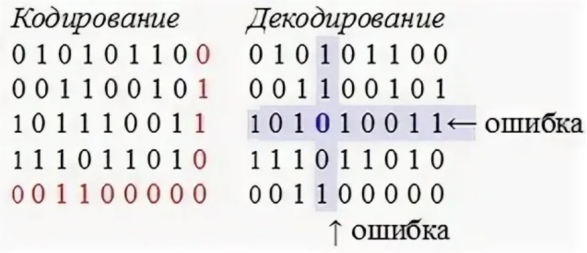


Рис. 3.1. Матричный код

Кодирование. Все векторы далее мы будем, как принято в теории кодирования, считать *вектор-строками*. Обозначения:

- сообщение — двоичный k-вектор

$$\boldsymbol{u} = [\, u_0 \ldots u_{k-1} \,];$$

- кодовое слово — двоичный n-вектор

$$\boldsymbol{v} = [\, v_0 \ldots v_{n-1} \,].$$

- совокупность C всех кодовых слов — $[n, k]$-*код*, или, с кодовым расстоянием — $[n, k, d]$-*код*.

  В общем случае не все векторы длины k включаются во множество возможных сообщений S, и код тогда имеет мощность $Q < 2^k$. Для таких кодов используют обозначение (n, Q, d). Соответствующие обозначения для q-ичных кодов — $[n, k, d]_q$ и $(n, Q, d)_q$.

Пример 3.2. Избыточный код $[5, 2]$-код:

$C = \{\boldsymbol{v}_1 = [00000], \boldsymbol{v}_2 = [10101], \boldsymbol{v}_3 = [01110], \boldsymbol{v}_4 = [11011]\}$.

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 позициях ошибочных (инвертированных) битов и 0 — в остальных.

Декодирование принятого слова $\boldsymbol{w}$ *обычно значительно сложнее* кодирования, и проводится оно в два этапа.

I этап. Определение кодового слова $\boldsymbol{c}$ как *ближайшего* в метрике Хэмминга слову к $\boldsymbol{w}$ — *декодирование по максимуму правдоподобия* (MLD, Maximum Likelihood Decoding, задача NCP, Nearest Code Problem).
Если d — кодовое расстояние и произошло не более $\lfloor (d-1)/2 \rfloor$ ошибок, то $\boldsymbol{c} = \boldsymbol{v}$.

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

I-й этап может быть выполнен по *таблице декодирования*. В ней кодовые слова образуют первую строку. Под каждым кодовым словом задан перечень возможных принятых слов, которые могут декодироваться в

это кодовое слово, и каждое такое слово появляется в таблице только один раз.

Таблица декодирования имеет размер $2^{n-k} \times 2^k$. 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. На практике же значения n и k могут достигать *сотен тысяч* бит.

Приняв некоторые ограничения на множество кодовых слов, можно сократить трудоёмкость кодирования/декодирования. Эти ограничения приводят к использованию кодов специального вида: *линейных*, а из линейных — *циклических*.

Плотная упаковка шаров в единичный куб

Теорема 3.3. *Максимальная мощность $Q = 2^k$ двоичного кода длины n, исправляющего не более $r = \lfloor n/2 \rfloor$ ошибок находится в пределах*

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

Доказательство известно читателю из курса Дискретной математики. □

Границы для мощности Q называют: нижнюю — *границей Гильберта*, верхнюю — *границей Хэмминга*.

Верхняя граница для Q впервые была приведена в работе 1947 г. индийского математика и статистика *Калъямпуди Р. Рао* (Calyampudi Radhakrishna Rao, 1920), и через три года — в работе *Р. Хэмминга*. Нижнюю границу установил в 1952 г. американский математик *Эдгар Гильберт* (Edgar Nelson Gilbert,

1923–2013, не путать со знаменитым немецким математиком *Давидом Гильбертом* (David Hilbert, 1862–1943)).

Из неравенства границы Хэмминга следует, что параметры блокового $[n, k, d]$-кода связаны соотношением

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

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

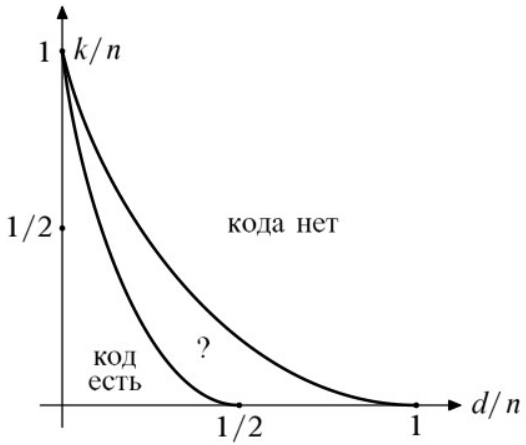


Рис. 3.2. Границы Гильберта (левая) и Хэмминга (правая) для двоичных кодов при $n \gg 1$.

Чтобы построить блоковый $[n, k]$-код, исправляющий данное количество r ошибок и имеющий максимальную мощность, нужно вложить в единичный куб B^n максимально возможное число k не пересекающихся шаров радиуса r. Это *задача плотной упаковки*:

правое неравенство, приведённое в теореме 3.3 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, рассматривая только нетривиальные двоичные коды, такое удаётся только в следующих случаях:

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. 99), у него $k = 12$ и $m = 11$;

3) $[n, n-1, 2]$ — коды с одной проверкой на чётность.

Эти коды называют *совершенными* или *экстремальными*. *Расширенные*, т. е. дополненные общей проверкой на чётность, коды Хэмминга и Голея также совершенны.

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

Покажем метод построения кода Хэмминга и удостоверимся, что для него граница Хэмминга достигается.

Выберем значение $m > 1$ и образуем 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

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

$$\underbrace{\qquad\qquad}_{k=2^m-1-m} \quad \underbrace{\qquad\qquad}_{m}$$

из $k = 2^m - 1 - m$ строк длины $n = 2^m - 1$. Просуммировав по $\mathrm{mod}\,2$ всевозможные совокупности строк таблицы и добавив нулевую строку, получим $[\,n, k\,]$-код Хэмминга. Его мощность

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

Найдём кодовое расстояние построенного кода. Для этого надо оценить вес сумм по $\mathrm{mod}\,2$ всех непустых совокупностей строк полученной таблицы.

Замечаем, что в каждой строке таблицы имеется не менее трёх единиц. Если же сложить по $\mathrm{mod}\,2$ две строки, то в левой части будет находится две единицы, а в правой — хотя бы одна. Если сложить не менее трёх строк, то левая часть кодового слова будет содержать не менее трёх единиц. Отсюда следует, что расстояние между кодовыми словами всегда не менее $3 = d$, т. е. он способен исправить одиночную ошибку.

Код Хэмминга с $m = 6$ применяется в памяти ECC-памяти (error-correcting code memory, память с коррекцией ошибок) современных компьютеров.

Пример 3.5. Положим $m = 3$, тогда $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$. 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

Задаваемый этой таблицей $[7, 4]$-код Хэмминга содержит $Q = 2^4 = 16$ кодовых слов.

Построенный код содержит по одному слову весов 0 и 7, по семь слов весов 3 и 4. Он исправляет 1 ошибку, обнаруживает все 2-, 5-, 6-кратные ошибки и 80% 3- и 4-кратных ошибок.

Первой ЭВМ, в которой использовался код Хэмминга, была IBM 7030, построенная в 1960 г., через 10 лет после опубликования кода.

3.2 Линейные коды

Линейные коды: определение, свойства. Практически вся теория блокового кодирования относится к линейным кодам, позволяющим в ряде случаев получать алгоритмы кодирования/декодирования, приемлемые по эффективности.

Общую теорию линейных кодов построил в 1956 г. американский математик *Давид Слепян* (David S. Slepian, 1923–2007).

Определение 3.6. Блоковый $[n, k]$-код C называют *линейным*, если он образует линейное векторное подпространство размерности k координатного пространства W всех n-слов: $C \leqslant \{0,1\}^n = W$.

Линейный код обладает следующими свойствами.

1. В рассматриваемом двоичном случае множество кодовых слов C линейного кода образует абелеву группу относительно операции «сумма по $\bmod 2$» $(+)$. Действительно, легко удостовериться, что операция $+$ на подпространстве $C \leqslant W$ обеспечивает выполнение теоретико-групповых аксиом. Поэтому линейные двоичные коды называют *групповыми*.

Пример 3.7. Нетрудно убедиться, что код из примера 3.2 — групповой. Коды Хэмминга, очевидно, являются линейными.

Разделимые линейные коды называют *систематическими*. В них проверочные символы являются линейными комбинациями информационных, и поэтому суммирование по $\bmod 2$ двух разрешенных кодовых слов дает также кодовое слово.

2. Кодовое расстояние d линейного кода C есть число единиц в ненулевом кодовом слове минимального веса. Действительно, для $\boldsymbol{x}, \boldsymbol{y} \in C$, $\boldsymbol{x} \neq \boldsymbol{y}$, положим $\boldsymbol{z} = \boldsymbol{x}+\boldsymbol{y} \neq \mathbf{0}$. Поскольку C — группа, то $\boldsymbol{z} \in C$. Тогда

$$d(C) = \min\{\rho(\boldsymbol{x}, \boldsymbol{y})\} = \min\{wt(\boldsymbol{x}+\boldsymbol{y})\} = \min\{wt(\boldsymbol{z})\}.$$

Пример 3.8. В примере 3.2 вес ненулевых наборов $\boldsymbol{c}_2$ и $\boldsymbol{c}_3$ минимален и равен 3, таким образом $d(C) = 3$.

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

Для разделимых линейных $[n, k, d]$-кодов легко

получить оценку Синглтона[1]: $d \leqslant n - k + 1$. 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.

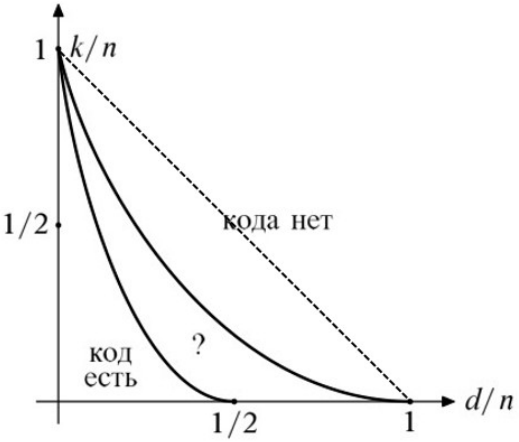


Рис. 3.3. Граница Синглтона (пунктир) для двоичных кодов при $n \gg 1$.

3. Существует базис $\{\, \boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1} \,\}$ линейного кода C как подпространства W, состоящий из векторов $\boldsymbol{g}_i \in \{0,1\}^n$, $i = 0, \ldots, k-1$. Поэтому любое кодовое слово $\boldsymbol{v} \in C$ может быть представлено в виде

[1] *Рихард Синглтон* (Richard Collom Singleton, 1928–2007), американский математик.

линейной комбинации базисных векторов:

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

Порождающая матрица. Составим матрицу из векторов некоторого базиса линейного кода C:

$$G_{k\times n} = \begin{bmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \\ \dots \\ \boldsymbol{g}_{k-1} \end{bmatrix}.$$

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

$$\boldsymbol{v} = \boldsymbol{u}G \subset B^n = W. \tag{3.1}$$

Пример 3.9. Линейный код из примера 3.2 порождается матрицей

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

Из (3.1) следует, что кодирование линейного $[\,n,\,k\,]$-кода может быть осуществлено за время $O(n^2)$.

Очевидно перестановка строк порождающей матрицы и сложение любой линейной комбинации некоторых строк с произвольной строкой не изменяют подпространства кодовых слов

$$C = \left\{ \boldsymbol{v} = \boldsymbol{u}G \mid \boldsymbol{u} \in B^k \right\}.$$

Эти операции называют *элементарными*, и они соответствуют переходу к *новому базису* данного кода.

Порождающую матрицу, задающую линейный $[n, k]$-код с помощью элементарных преобразований столбцов можно преобразовать к виду

$$G_{k\times n} = [\, I_k \; P_{k\times m} \,],$$

где I_k — единичная матрица порядка k. Такую форму порождающей матрицы называют *канонической* или *приведённо-ступенчатой*. При кодировании такой матрицей всё k-битное сообщение составит *начало* кодового слова, обеспечивая разделимое кодирование.

Если к элементарным операциям добавить возможность *перестановки столбцов* G, то это, конечно, изменит порождаемый код. Однако новое подпространство кодовых слов будет обладать теми же метрическими свойствами, что и исходное, поскольку все попарные расстояния между его векторами останутся прежними.

Коды, полученные преобразованиями последнего вида, называют *эквивалентными*. Формально, два линейных $[n, k]$-кода с порождающими матрицами G и G_1 эквивалентны, если найдётся такая квадратная невырожденная матрица A порядка k, что $G_1 = AG$.

Ясно также, что линейный код можно преобразовать в эквивалентный ему систематический не только с исходным сообщением в первых битах, но и с произвольно заданными позициями информационных бит.

Пример 3.10. В примере 3.5 была получена таблица, сложением различных совокупностей строк которой получаются все кодовые слова кода Хэмминга. Она и является порождающей канонической (4×7)-матрицей данного кода.

Для того, чтобы узнать кодовое расстояние линейного кода, в общем случае необходимо получить все кодовые слова, для чего можно умножить все, кроме нулевого, векторы сообщений $\boldsymbol{u}$ на порождающую матрицу G и определить минимальный вес полученных кодовых слов.

Ортогональное дополнение к коду. Проверочная матрица. Элементы пространства W, ортогональные всем кодовым словам линейного $[n, k]$-кода C образуют *ортогональное линейное (нулевое) подпространство* $C^\perp$ пространства W:

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

Элементы $C^\perp$ называют *двойственным к C кодом.* Всегда будем иметь $\dim C = k$ и $\dim C^\perp = n - k = m$.

Хотя и C, и $C^\perp$ — подпространства W, но в общем случае W не есть их прямая сумма: произвольный вектор из W может либо не разлагаться, либо разлагаться неоднозначно в сумму векторов из C и $C^\perp$.

Пример 3.11. Рассмотрим в B^3 подпространства

C	$C^\perp$
$[000]$	$[000]$
$[110]$	$[110]$
	$[001]$
	$[111]$

размерности 1 и 2 соответственно. Тогда вектор $[110]$ представляется в виде суммы векторов из C и $C^\perp$ неоднозначно, а вектор $[100]$ вообще не имеет такого представления.

Причиной этих «старанностей» является то, что из ортогональности системы векторов над конечным полем не следует

их линейной независимости, как это имеет место в евклидовом пространстве.

Пусть $\{ \boldsymbol{h}_0, \ldots, \boldsymbol{h}_{m-1} \}$ — некоторый базис $C^\perp$. Тогда матрица

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

называется *проверочной матрицей (parity-check matrix)* кода C. Она осуществляет сюръективное отображение $H : W \to \{0,1\}^{n-k} = C^\perp$.

Ясно, что проверочная матрица H, как и порождающая G, определена с точностью до элементарных преобразований *строк* — базисных векторов $C^\perp$.

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

$$0 \to \{0,1\}^k \xrightarrow{G} \{0,1\}^n \xrightarrow{H} \{0,1\}^{n-k} \to 0.$$

Здесь и на рис. 3.4 символы матриц обозначают соответствующие линейные преобразования пространств: G — мономорфизм, H — эпиморфизм и ядро H совпадает с образом C преобразования G —

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

Иными словами, для всех $\boldsymbol{u} \in S$ справедливо

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

Это означает, что $GH^T = O$ — *нулевая матрица*.

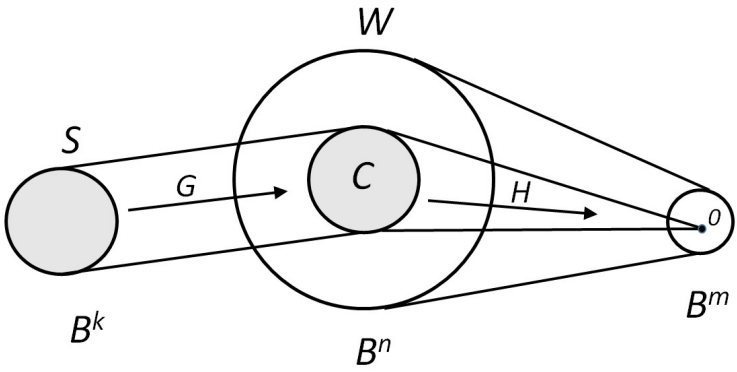


Рис. 3.4. Преобразования: G — сообщений в линейный код C и H — принятых слов в $C^{\perp}$.

Пример 3.12. Для примера 3.11:

$$GH^T = [\,1\ 1\ 0\,] \times \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = [\,0\ 0\,] = O.$$

Если порождающая матрица линейного $[\,n, k\,]$-кода имеет каноническую форму $G_{k\times n} = [\ I_k\ P_{k\times m}\ ]$, то его проверочной матрицей будет

$$H_{m\times n} \ = \ \left[\ P^T_{m\times k}\ I_m\ \right],$$

где I_m — единичная матрицы порядка m.

Действительно, в этом случае

$$GH^T \ = \ [\ I\ P\ ] \times \begin{bmatrix} P \\ I \end{bmatrix} \ = \ P + P \ = \ O.$$

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

$$G \ = \ [\ P\ I\ ], \quad H \ = \ \left[\ I\ P^T\ \right].$$

Очень важное замечание: для кодов в поле характеристики отличной от 2, очевидно,

$$H = \left[\; -P^T \; I \; \right] \; (!)$$

Но мы рассматриваемом двоичные коды, где $-P = P$.

Пример 3.13. Для построенной в примере 3.5 порождающей матрицы $G_{4\times 7}$ 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* $m = 3$.

Итак, линейный $[n, k]$-код задаётся либо порождающей матрицей $G_{k\times n}$, либо проверочной матрицей $H_{m\times n}$. Эти матрицы определены с точностью до элементарных преобразований строк, что отвечает выбору различных базисов в пространствах C и $C^{\perp}$. Однако фиксирование позиций информационных бит при систематическом кодировании задаёт G и H однозначно.

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

Пример 3.14. Пусть линейный $[6, 3]$-код C задан порождающей матрицей

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

Требуется:

1. Кодом C осуществить несистематическое и систематическое кодирование векторов

$$\boldsymbol{u}_1 = [\,0\,1\,1\,] \text{ и } \boldsymbol{u}_2 = [\,1\,0\,1\,].$$

2. Построить проверочную матрицу H' для систематического кодирования.
3. Определить кодовое расстояние d кода C.

Решение.

1. *Несистематическое кодирование* находим непосредственно:

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

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

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

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

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

$$\begin{aligned} \boldsymbol{v}_{/1} &= \boldsymbol{u}_1 G' = [\,1\,1\,0\,0\,1\,0\,], \\ \boldsymbol{v}_{/2} &= \boldsymbol{u}_2 G' = [\,1\,0\,1\,1\,0\,0\,]. \end{aligned}$$

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

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

и найдём

$$P^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

(случайно получилось $P^T = P$).

Далее нужно

1) последовательно разместить *столбцы* P^T 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

$$H'_{3\times 6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

3. Найдем кодовое расстояние d. Для этого закодируем все ненулевые сообщения $\boldsymbol{u}_1$, ..., $\boldsymbol{u}_7$ и найдем минимальный хэммингов вес полученных кодовых кодовых слов:

$$\begin{bmatrix} \boldsymbol{v}_1 \\ \dots \\ \boldsymbol{v}_7 \end{bmatrix} = \begin{bmatrix} \boldsymbol{u}_1 \\ \dots \\ \boldsymbol{u}_7 \end{bmatrix} \times G' = $$

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

В итоге определим, что $d(C) = 3$.

Код Голея. М. Голей[2] в 1949 г. обнаружил, что

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

Это позволило предположить, что существует совершенный $[\,23,\, 12,\, 7\,]$-код исправляющий до 3-х ошибок, который и был Голеем указан. Код оказался линейным, и более того — циклическим (см. далее).

Доказано, что условие «$2^n / \left(C_n^0 + \ldots + C_n^r\right)$ — целое, $0 < r < n$» выполняется только для кодов Хэмминга, Голея и тривиальных.

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

3.3 Декодирование линейных кодов

Списочное декодирование. Декодирование линейных кодов по максимуму правдоподобия является NP-полной задачей. Поэтому в большинстве случаев для их декодирования приходится строить приближенные алгоритмы.

Одним из часто используемых приемов является *списочное декодирование*, которое состоит в поиске кодовых слов ближайших в некотором смысле к принятому слову. Далее из полученного списка может быть выбрано наиболее вероятное кодовое слово или кодовое слово, удовлетворяющее некоторым дополнительным проверочным соотношениям, которые не были учтены при построении этого списка. Сложность такого подхода определяется максимально возможным размером списка.

Известны более эффективные методы декодирования линейных кодов, основанные на вычислении исправляющего вектора, который принято называть *синдромом*[3)].

Синдром ошибки. Цель I-го, наиболее сложного этапа декодирования — узнать, какое кодовое слово передавалось. Однако оказывается легче сначала определить, каков вектор $\boldsymbol{e}$ ошибок, произошедших в канале.

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

[3)] Синдром в общем смысле — совокупность явлений, вызванных отклонением от нормы.

$$\boldsymbol{v}H^T = H\boldsymbol{v}^T = \mathbf{0}. \tag{3.2}$$

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

$$\boldsymbol{w}H^T = \boldsymbol{v}H^T + \boldsymbol{e}H^T = \mathbf{0} + \boldsymbol{e}H^T \stackrel{\text{def}}{=} \boldsymbol{s}. \tag{3.3}$$

Определение 3.15. *Синдром слова* $\boldsymbol{w}$, принятого при передаче сообщения, закодированного линейным кодом с проверочной матрицей H и, возможно, содержащего ошибки, называют вектор $\boldsymbol{s} = \boldsymbol{w}H^T$.

Ясно, что если $\boldsymbol{s} = \mathbf{0}$, 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 типов кодов.

Если же ошибки произошли, то для их исправления воспользуемся фактом, что синдромы принятого вектора $\boldsymbol{w}$ и вектора ошибки $\boldsymbol{e}$ совпадают (3.3). Отсюда следует, что вектор ошибок $\boldsymbol{e}$ удовлетворяет неоднородной недоопределённой СЛАУ

$$\boldsymbol{e}H^T = \boldsymbol{s}, \tag{3.4}$$

а кодовые слова являются решениями соответствующей однородной системы (3.2)

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

Определение ошибок по словарю синдромов. Можно попытаться восстановить неизвестный вектор $\boldsymbol{e}$, используя тот факт, что он является решением системы (3.4).

Для этого нужно составить *словарь синдромов* — таблицу, строки которой соответствуют всем 2^m возможным синдромам. Очевидно множество всех векторов, имеющих одинаковые с $\boldsymbol{w}$ синдромы есть смежный класс по подгруппе C.

Каждая строка таблицы будет содержать и *наиболее вероятный вектор ошибок*, данному синдрому соответствующий. Этот вектор должен иметь наименьший вес среди возможных решений системы (3.4) 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.

Пример 3.16. Пусть C есть бинарный линейный $[4, 2]$-код с порождающей матрицей G и проверочной матрицей H:

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Строим следующую *стандартную таблицу*.

Сообщения	00	10	01	11	
Кодовые слова	0000	1010	0111	1101	$[00]$
Другие смежные классы	1000	0010	1111	0101	$[10]^T$
	0100	1110	0011	1001	$[11]^T$
	0001	1011	0110	1100	$[01]^T$
	лидеры				*синдромы*

Первый столбец содержит лидеры смежных классов, последний — синдромы.

Пусть исходное сообщение есть $\boldsymbol{u} = [10]$. Тогда соответствующее ему кодовое слово есть $\boldsymbol{v} = [1010]$. Если ошибка произошла во 2-м разряде, то будет получено слово $\boldsymbol{w} = [1110]$. Его синдром: $\boldsymbol{s} = \boldsymbol{w}H^T = [11]$.

Вектор ошибки $\boldsymbol{e} = [0100]$ есть лидер смежного класса, имеющий тот же синдром. Тогда передаваемое кодовое слово, скорее всего, было словом

$$\boldsymbol{c} = \boldsymbol{w} + \boldsymbol{e} = [1110] + [0100] = [1010] = \boldsymbol{v},$$

а сообщение, которое передавали, было $\boldsymbol{u} = [10]$ (информационная часть кода). Таким образом, ошибка передачи успешно исправлена.

Заметим, что рассматриваемый код имеет кодовое расстояние 2, однако он исправил одиночную ошибку! Объясняется это тем, что условие $r = \lfloor (d-1)/2 \rfloor$ утверждает возможность правильного исправления *всевозможных* ошибок числом не более r. В то же время рассматриваемый код исправит только три из возможных четырёх одиночных ошибок.

Например, если в том же кодовом слове ошибка произошла в 3-м разряде, то будет принято слово $\boldsymbol{w} = [1000]$. Соответствующий ему синдром есть $\boldsymbol{s} = [10]$, лидер соответствующего класса — $[1000]$ и передаваемое кодовое слово будет восстановлено неверно. Это произошло потому, что у смежного класса элементов, имеющих синдром $[10]$ имеется два вектора ошибок минимального веса: $[1000]$ и $[0010]$, а в качестве лидера выбран первый из них.

Приведённый в данном примере код оказывается простейшим примером линейного кода с *неравной защитой от ошибок* (*Linear Unequal Error Protection,*

LUEP). Данному коду соответствует *разделяющий вектор* $(3, 2)$, который показывает, что минимальное кодовое расстояние равно 3, если различаются информационные (первые) биты сообщения, и равно 2 для проверочной части кода. Это является одним из аргументов применения систематического кодирования.

В случае линейных кодов с больши́ми параметрами становится практически невозможным найти лидеров смежных классов. Так, например, линейный $[\,50, 20\,]$-код имеет около 10^9 смежных классов. Чтобы преодолеть подобные затруднения, необходимо строить специальные коды.

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 3.13 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 есть двоичный код номера позиции ошибки.

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

Пример 3.17. 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

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

При кодировании матрицей G биты сообщения помещаются последовательно в 3, 5, 6 и 7-ю позиции кодового слова, а остальные три (1, 2 и 4 — степени 2) бита являются проверочными.

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

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

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

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

Тогда синдром

$$\boldsymbol{s} = \boldsymbol{w}(H')^T = [\ 1\ 0\ 1\ ] \leftrightarrow 5_{10}.$$

указывает позицию ошибки.

Дуальные коды. Поскольку $GH^T = O = HG^T$, то можно использовать H как порождающую, а G — 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*. Возможен случай, когда $H = G$. Такие коды называют *самодуальными*.

Все самодуальные коды — чётной длины.

Например расширенный $[8, 4, 4]$-код Хэмминга, задаваемый матрицей

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

самодуален.

3.4 Циклические коды

Циклические коды — наиболее изученные среди линейных. При их изучении используется теория конечных полей, которая в этой области оказывается особенно результативной.

Англ. CRC, *Cyclic Redundancy Code* — избыточный циклический код. Впервые их в 1957–58 годах построил американский учёный *Юджин Прейндж* (Eugene August Prange, 1917–2006).

Не путать с имеющим ту же аббревиатуру *Cyclic Redundancy Check* — применением циклического кодирования в качестве хэш-функции с целью обнаружения ошибок, но не их исправления.

Заметим, что циклические коды не обязательно линейные, но мы будем рассматривать исключительно линейные циклические коды.

Полиномиальное представление слов. Установим изоморфное соответствие векторов сообщения $\boldsymbol{u} \in \{0,1\}^k$ и кодового слова $\boldsymbol{v} \in \{0,1\}^n$ с их полиномиальными представлениями $u(x), v(x) \in \mathbb{F}_2[x]$:

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

Код, представляемый порождающим полиномом называется *полиномиальным*. Чтобы полиномиальный код был циклическим, порождающий полиномом должен быть делителем $x^n - 1$, n — длина кодового слова.

Определение и построение циклических кодов

Определение 3.18. Блоковый код называется *циклическим*, если он инвариантен относительно циклических сдвигов своих кодовых слов.

Теория циклических кодов основана на изоморфизме пространства двоичных n-последовательностей пространству полиномов степени не выше $n-1$, позволяя применять более простые, чем в общем случае, алгоритмы кодирования и декодирования.

Например, двоичный код

$$C = \{\, 000,\ 011,\ 101,\ 110 \,\}$$

может быть записан в виде

$$C = \{\, 0,\ 1+x,\ 1+x^2,\ x+x^2 \,\} \subset \mathbb{F}_2[x]/(x^3-1).$$

По теореме 2.40 циклическое пространство образуют элементы идеала I в кольце $R_n = \mathbb{F}_p[x]/(x^n-1)$ классов вычетов по модулю идеала x^n-1. Такой идеал в кольце R_n задаётся каким-либо делителем $g(x)$ бинома x^n-1: элементы I суть многочлены из $\mathbb{F}_p[x]$, кратные $g(x)$ по $\bmod\,(x^n-1)$.

Поэтому построить двоичный циклический $[\,n,k\,]$-код можно следующим образом.

1. Задаются значениями $0 < m < n$ и выбирают *любой* делитель $g(x)$ степени $m = n-k$ бинома x^n-1. *Многочлен $g(x)$ полностью задаёт циклический код*, его называют *порождающим* данный код или его *генератором*.

2. Идеал $(g(x))$ кольца $R_n = \mathbb{F}_2[x]/(x^n-1)$ состоит из всех многочленов вида
$$f(x)\cdot g(x), \quad 0 \leqslant \deg f(x) < k = n-m.$$
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. В то же время справедлива оценка $d \geqslant m = \deg g(x)$: такое число единиц будет иметь кодовое слово сообщения $[\,1,\,0,\,\ldots,\,0\,]$.

Пример 3.19. Построим циклический код длины $n = 23$. В п. 2 примера 2.42 найдены число и степени неприводимых многочленов, факторизующих бином $x^{23} - 1$. Конкретно это разложение таково:

$$x^{23} - 1 = (x+1)(\underbrace{x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1}_{g_1(x)}) \times \\ \times (\underbrace{x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1}_{g_2(x)})$$

(делители $g_1(x)$ и $g_2(x)$ пришлось искать подбором). 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. Мы построили код Голея.

Заметим, что эффективного способа нахождения неприводимых делителей биномов вида $x^n - 1$ нет.

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

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 (эквивалентный исходному).

Кодирование циклическими кодами. Пусть циклический $[\,n, k\,]$-код C задаётся порождающим поли-

номом $g(x)$, делящим бином $x^n - 1$ и $\deg g(x) = m = n - k$.

Несистематическое кодирование выполняется умножением кодируемого полинома на порождающий:

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

Систематическое кодирование выполняется помещением в старшие (правые) разряды кодового слова сообщения $g(x)$, а в младшие (левые) его 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 3.20. 1. Построим циклический код длины 7.

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени его неприводимых многочленов-делителей, для чего применим способ разбиения $\mathbb{Z}_7$ на орбиты относительно умножения на 2 по $\bmod 7$ (см. с. 74):

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

Таким образом, бином $x^7 - 1$ имеет один линейный делитель и два неприводимых делителя 3-й степени. Поскольку эти многочлены однозначно определяются, получаем разложение

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

В качестве порождающего полинома выберем многочлен

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

Тогда $m = \deg g(x) = 3$, $k = 4$, и будет построен циклический $[\,7, 4\,]$-код Хэмминга.

Заметим, что получаем при выборе

- $g(x) = x + 1$ — код с проверкой на чётность;
- $g(x) = (x+1)\left(x^3+x+1\right)$ — расширенный код Хэмминга;
- $g(x) = \left(x^3+x+1\right)\left(x^3+x^2+1\right)$ — код 7-кратного повторения;
- $g(x) = x^7 - 1$ или $g(x) \equiv 1$ — тривиальные коды.

2. Закодируем построенным кодом сообщение

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

Несистематическое кодирование:

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

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

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

то есть $r(x) = x$, и поэтому

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

Декодирование циклических кодов

Определение 3.21. *Синдромом* $s(x)$ *слова* $w(x)$, принятого при передаче сообщения, закодированного циклическим кодом, и, возможно, содержащего ошибки, называют остаток от деления $w(x)$ на многочлен $g(x)$, порождающий код.

Ясно, что если $s(x) \equiv 0$, 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 по k трудоёмкость.

3.5 Коды БЧХ. Кодирование

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

Коды предложили *Радж Чандра Боуз* (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)[4].

Циклотомические классы

Определение 3.22. Ненулевые элементы поля $\mathbb{F}_p^t$, имеющие общий минимальный многочлен, называют *сопряженными*, и они составляют *циклотомический класс*.

Ясно, что циклотомические классы

$$C_0 = \{1\},\ C_1,\ \ldots$$

либо совпадают, либо не пересекаются, и в совокупности образуют *разбиение* мультипликативной группы поля $\mathbb{F}_p^t$, или её *разложение на классы над* $\mathbb{F}_p$.

В поле характеристики p если α — корень некоторого полинома, то и α^p — его корень. Поэтому циклотомические классы можно получать возведением в степень p какого-то одного его элемента. Это совпадает с построением орбиты отображения (см. с. 75)

$$\ell \mapsto p\ell \pmod{(p^t - 1)}.$$

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

$$C_1 = \left\{ \alpha = \alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \ldots, \alpha^{2^{t-1}} \right\}.$$

[4] Заметим, что Hocquenghem является галицинизированной формой германской или фламандской фамилии, и правильное её чтение — *Óкенгем*.

Пример 3.23. Пусть $t = 4$ и α — примитивный элемент поля $\mathbb{F}_2^4$. Тогда мультипликативная его группа

$$\{\, \alpha,\, \alpha^2,\, \ldots,\, \alpha^{14},\, \alpha^{15} = \alpha^0 = 1 \,\}$$

разлагается над $\mathbb{F}_2$ на циклотомические классы

$$C_0 = \{\, \alpha^0 = 1 \,\},\ C_1 = \{\, \alpha,\, \alpha^2,\, \alpha^4,\, \alpha^8 \,\},$$
$$C_2 = \{\, \alpha^3,\, \alpha^6,\, \alpha^{12},\, \alpha^9 \,\},\ C_3 = \{\, \alpha^5,\, \alpha^{10} \,\},$$
$$C_4 = \{\, \alpha^7,\, \alpha^{14},\, \alpha^{13},\, \alpha^{11} \,\}.$$

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*

$$\delta \;=\; 2r + 1 < n.$$

Последовательные степени $\alpha,\, \alpha^2,\, \alpha^3,\, \ldots,\, \alpha^{2r}$ 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 $\deg g(x) = m = n - k$, 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 — корни любого многочлена, соответствующего кодовому слову.

Определение 3.24. *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: $s_i = w(\alpha^i)$, $i = 1, \ldots, 2r = \delta - 1$.

Поскольку $w(x) = v(x) + e(x)$, то для всех $i = 1, \ldots, \delta - 1$ 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 $x^n - 1$, $k = n - \deg g(x)$, $n = 2^t - 1$.

Алгоритм построения двоичного кода БЧХ, исправляющего не менее r ошибок

1. Выбрать величину t, определяющую длину кода $n = 2^t - 1 > 2r + 1 = \delta$.
2. Выбрать неприводимый полином $a(x)$ степени t, определив тем самым 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 все $2r$ нулей $\alpha, \alpha^2, \ldots, \alpha^{2r}$ кода; пусть таких классов h.
4. Найти минимальные многочлены
$$g_1(x),\ g_2(x),\ \ldots,\ g_h(x)$$
каждого циклотомического класса.
5. Вычислить порождающий полином кода
$$g(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_h(x).$$

Пример 3.25. Выберем $t = 3$ и построим некоторые БЧХ-коды длины $n = 2^3 - 1 = 7$.

Рассмотрим поле $\mathbb{F}_2^t = \mathbb{F}_2^3$. Его мультипликативная группа относительно любого своего примитивного элемента α разобьётся на 3 циклотомических класса над $\mathbb{F}_2$ (см. пример 3.20):

$$C_0 = \left\{ \alpha^0 = 1 = \alpha^7 \right\},$$
$$C_1 = \left\{ \alpha, \alpha^2, \alpha^4 \right\}, \; C_2 = \left\{ \alpha^3, \alpha^6, \alpha^5 \right\}.$$

Образуем $\mathbb{F}_2^3$ как факторкольцо $\mathbb{F}_2[x]/(a(x))$ по идеалу примитивного многочлена $a(x) = x^3 + x + 1$ степени $t = 3$. Получим реализацию рассматриваемого поля, в которой $\alpha^3 = \alpha + 1$ и $a(x)$ является м. м. $g_1(x)$ для примитивного элемента $\alpha = x$ и всего класса C_1. Данное конкретное поле будем обозначать F.

Поскольку $a(x)$ является примитивным многочленом, то полагаем $\alpha = x$.

Далее необходимо в зависимости от требуемого числа исправляемых ошибок указать полином, порождающий код.

1. *Код БЧХ длины $n = 7$, исправляющий $r = 1$ ошибку.* В этом случае $2r = 2 = \delta - 1$ и нули кода α, α^2 попадают в один циклотомический класс C_1. Минимальный многочлен элементов этого класса — $g_1(x) = a(x)$, поэтому порождающий полином $g(x) = a(x)$, $m = 3$, и в результате получаем уже известный $[7, 4, 3]$-код Хэмминга с $d = \delta$ (см. пример 3.20).

2. *Код БЧХ длины $n = 7$, исправляющий не менее $r = 2$-х ошибок.* Теперь $2r = 4 = \delta - 1$. Нули α, α^2,

α^3, α^4 строящегося кода попадают 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 перед степенями x в $g_2(x)$:

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

$$\alpha^8 + \alpha^9 + \alpha^{11} = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \alpha(\alpha + 1) = 0,$$

$$\alpha^{14} = (\alpha^7)^2 = 1^2 = 1.$$

Таким образом $g_2(x) = x^3 + x^2 + 1$[5] 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 код с 7-кратным повторением, содержащий всего два кодовых слова: $[\,0 \ldots 0\,]$ и $[\,1 \ldots 1\,]$, и исправляющий 3 ошибки, т. е. получаем $d = 7 > \delta = 5$.

Пример 3.26. Попытаемся построить лучшие коды, взяв бóльшие их длины: выберем $t = 4$, и тогда длина кода будет $n = 2^4 - 1 = 15$.

[5] Можно было догадаться сразу: это второй из двух неприводимых многочленов степени 3 из $\mathbb{F}_2[x]$.

Рассмотрим поле $\mathbb{F}_2^t = \mathbb{F}_2^4$. Как показано в примере 3.23, его мультипликативная группа относительно любого своего примитивного элемента α разобьётся на 5 циклотомических классов над $\mathbb{F}_2$:

$$C_0 = \{\, \alpha^0 = 1 = \alpha^{15} \,\},\ C_1 = \{\, \alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8 \,\},$$
$$C_2 = \{\, \alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^9 \,\},\ C_3 = \{\, \alpha^5,\ \alpha^{10} \,\},$$
$$C_4 = \{\, \alpha^7,\ \alpha^{14},\ \alpha^{13},\ \alpha^{11} \,\}.$$

Образуем $\mathbb{F}_2^4$ как факторкольцо по идеалу примитивного многочлена $a(x) = x^4 + x + 1$ степени $t = 4$. Получим реализацию рассматриваемого поля, в которой $\alpha^4 = \alpha + 1$, и $a(x)$ является м. м. $g_1(x)$ для примитивного элемента $\alpha = x$ и всего класса C_1. Данное конкретное поле будем обозначать далее F.

1. *Код БЧХ длины $n = 15$, исправляющий не менее 2-х ошибок.* В этом случае $2r = 4 = \delta - 1$, 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 $R = 7/15$.

2. *Код БЧХ длины $n = 15$, исправляющий не менее 3-х 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 α, α^2, ..., α^6 кода.

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 3.27. Рассматриваем $[7, 4]$-код Хэмминга, построенный в примере 3.20 для циклических кодов, где был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [\,0\,0\,1\,1\,]$:

$$v(x) = x^3 u(x) + x \;\leftrightarrow\; [\,0\,1\,0\,0\,0\,1\,1\,].$$

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

$$[\,0\,1\,0\,0\,0\,\overline{0}\,1\,] \leftrightarrow w(x) = x^6 + x.$$

Для декодирования $w(x)$ найдем синдром:

$$s = w(\alpha) = \alpha^6 + \alpha = \ldots = \alpha^2 + 1 + \alpha \neq 0.$$

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 $n = 2^t - 1$ исправляющий до $r = \lfloor (d-1)/2 \rfloor$ ошибок, при построении которого для определения порождающего полинома использовалось поле

$$\mathbb{F}_2^t \cong \mathbb{F}_2[x]/(a(x)) = F, \quad \deg a(x) = t$$

с примитивным элементом α.

Пусть при передаче кодового слова произошло $\nu \leqslant r$ 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 синдром принятого полинома $w(x)$:

$$s_i = w(\alpha^i) = e(\alpha^i), \quad i = \overline{1, 2r}.$$

Если все они равны 0, то считаем, что ошибок не произошло. Иначе $1 \leqslant \nu$, и с учётом $(\alpha^i)^j = (\alpha^j)^i$ запишем значения синдромов через степени α:

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

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

Введём обозначения $\beta_k = \alpha^{j_k}$, $k = \overline{1, \nu}$; эти величины называют *локаторами ошибок*. Перепишем полученную систему как зависимости с введёнными переменными:

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

Прямые методы решения подобных систем нелинейных уравнений неизвестны. Решение данной системы отыскивают, выполняя переход к СЛАУ линейных уравнений относительно коэффициентов вводимого полинома $\sigma(x)$.

Определим *полином локаторов ошибок*:

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

считая формально $\sigma_0 = 1$ и $\sigma_k = 0$ при $k > \nu$. Корнями его, очевидно, будут величины $\beta_k^{-1} = \alpha^{-j_k}$, $k = \overline{1, \nu}$.

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

$$\left\{ \begin{array}{l} \sigma_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \ldots + \beta_{\nu-1}\beta_\nu, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_\nu = \beta_1\beta_2 \ldots \beta_\nu. \end{array} \right. \qquad (\Sigma)$$

Системы (S) и (Σ) 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*[6)], которые в поле характеристики 2 за-

[6)] Эти тождества были найдены Исааком Ньютоном около 1666 г. Тому же вопросу была посвящена более ранняя работа (1629) Альбера Жирара о которой И. Ньютон, по всей видимости, не знал. Тождества находят применение во многих областях математики і. а. в теории Галуа, теории групп, комбинаторике и др.

писываются как

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

Данные равенства представляют собой квадратную СЛАУ порядка ν относительно неизвестных $\sigma_1, \ldots, \sigma_\nu$. Её можно переписать в виде

$$\begin{bmatrix} s_1 & s_2 & \ldots & s_\nu \\ s_2 & s_3 & \ldots & s_{\nu+1} \\ \ldots & \ldots & \ldots & \ldots \\ s_\nu & s_{\nu+1} & \ldots & s_{2\nu-1} \end{bmatrix} \times \begin{bmatrix} \sigma_\nu \\ \sigma_{\nu-1} \\ \ldots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} s_{\nu+1} \\ s_{\nu+2} \\ \ldots \\ s_{2\nu} \end{bmatrix} \qquad (*)$$

Матрица этой СЛАУ является *ганкелевой*: на её диагоналях, перпендикулярных главной, стоят равные элементы.

Стандартными методами эта система не может быть решена, поскольку значение ν неизвестно. Алгоритмы решения системы $(*)$ называют *декодерами*.

Например, декодер Питерсона (*W. Peterson*) состоит в последовательных попытках решения данных соотношений для $\nu = r, r-1, \ldots$ до тех пор, пока матрица очередной СЛАУ не окажется невырожденной. Метод прост и хорош при малом r, поскольку сложность обращения матрицы растёт примерно как куб её размера.

В литературе часто используют термин *PGZ-декодер* (*Питерсона-Горенштейна-Цирлера*). Это связано с использованием данного алгоритма Горенштейном (*D. Gorenstein*) и Цирлером (*N. Zierler*) для декодирования недвоичных кодов БЧХ и Рида – Соломона.

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

После нахождения полинома локаторов ошибок нужно отыскать все ν его корней. Это можно выполнить перебором элементов α, $\alpha^2, \ldots$ мультипликативной группы F^*.

По найденным корням $\sigma(x)$ легко определяются определить позиции ошибок: если α^ℓ — корень $\sigma(x)$, то позиция ошибки j есть

$$j = -\ell \pmod{n}.$$

Алгоритм I-го этапа декодирования
$[n, k, d]$-кода БЧХ
с нулём кода α из поля $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^t$,
$\deg a(x) = t$ и принятого слова $w(x) \in \mathbb{F}_2[x]$,
$\deg w(x) = n = 2^t - 1 > d$.

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 всех элементов F^*; пусть эти корни суть $\alpha^{\ell_1}, \ldots, \alpha^{\ell_\nu}$.
4. Найти позиции ошибок $j_i \equiv_n -\ell_i$, $i = \overline{1, \nu}$.
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 сообщение $u(x)$.

Декодер Сугиямы. Данный декодер, разработанный в 1975 г. *Ясуо Сугиямой* (Yasuo Sugiyama), базируется на обобщённом алгоритме Евклида[7)] и его часто выбирают при аппаратной реализации декодеров.

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* (над F):

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

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 Ньютона–Жирара (NG), то есть все они равны 0. Значит полином значений ошибок $\Lambda(x)$ имеет нулевую «среднюю часть».

Обозначим его начальную часть $\lambda(x)$, а из заключительной вынесем за скобку x^{2r+1}:

$$s(x)\sigma(x) = \underbrace{1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_\nu x^\nu}_{\lambda(x)} +$$

[7)] Данный декодер создавался для декодирования кодов Рида–Соломона, но БЧХ-коды являются их подклассом.

$$+\ x^{2r+1}\underbrace{\left(\lambda_{2r+1}+\ldots+\lambda_{2r+\nu}x^{\nu-1}\right)}_{b(x)},\quad 1\leqslant\nu\leqslant r.$$

Это означает, что справедливо сравнение

$$s(x)\sigma(x)\ =\ \lambda(x)\pmod{x^{2r+1}}. \tag{3.6}$$

Данное соотношение называют *ключевым уравнением Падэ*[8]. Его решение $\sigma(x)$ при $\nu\leqslant r$ единственно.

Уравнение (3.6) имеет вид (2.1), что 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 $\mathbb{F}_2[x]/(x^{2r+1})$ с условием останова «*степень очередного остатка не более* r» и опусканием заключительного шага нормировки (см. с. 51).

Пример 3.28. Рассматриваем $[\,15,5,7\,]$-код БЧХ с полем разложения $\mathbb{F}_2[x]/\left(x^4+x+1\right)=F$, построенный в п. 2 примера 3.26. При вычислениях удобно пользоваться таблицей со с. 45.

Пусть передаётся сообщение

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

При систематическом кодировании (опустим этот этап) порождающим полиномом (3.5) кодовым словом, как можно показать, будет

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

[8] *Анри Эжен Паде*, Henri Eugene Pade, 1863–1953 —французский математик.

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

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

или в виде полинома —

$$w(x) = x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1.$$

1. Найдём все $d-1=6$ компонент синдрома:

$$s_1 = w(\alpha) = (\underbrace{\alpha^3+1}_{\alpha^{14}}) + (\underbrace{\alpha^3+\alpha^2+\alpha}_{\alpha^{11}}) + (\underbrace{\alpha^2+1}_{\alpha^8}) +$$
$$+ (\underbrace{\alpha^3+\alpha^2}_{\alpha^6}) + (\underbrace{\alpha+1}_{\alpha^4}) + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha,$$
$$s_2 = w(\alpha^2) = (w(\alpha))^2 = s_1^2 = \alpha^2,$$
$$s_3 = w(\alpha^3) = \ldots = \alpha^8,$$
$$s_4 = w(\alpha^4) = s_1^4 = \alpha^4,$$
$$s_5 = w(\alpha^5) = \ldots = 1,$$
$$s_6 = w(\alpha^6) = s_3^2 = \alpha^{16} = \alpha.$$

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 Сугиямы, решим относительно $\sigma(x)$ соотношение Безу

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

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

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

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

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

Это последний шаг декодера, так как степень остатка $r_2(x)$ не превосходит $r = 3$. Таким образом, найден полином локаторов ошибок

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

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

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

$\sigma(\alpha) = \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2 \neq 0$;
$\sigma(\alpha^2) = \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha \neq 0$;
$\sigma(\alpha^3) = \alpha^{10} + \alpha^{11} + \alpha^{17} + \alpha^{13} =$

$$= \left(\alpha^2+\alpha+1\right) + \left(\alpha^3+\alpha^2+\alpha\right) + \alpha^2 + \\ + \left(\alpha^3+\alpha^2+1\right) = 0.$$

Первый корень α^3 полинома $\sigma(x)$ найден. Далее перебирая α^4, α^5, …, α^{15}, находим ещё два корня:

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

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

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

Поскольку применялось систематическое кодирование, II-й этап декодирования элементарен: исходное сообщение есть $\boldsymbol{u} = [\,0\,1\,1\,0\,1\,]$.

Коды БЧХ: резюме. Коды БЧХ используются довольно широко, что обусловлено следующими основными причинами.

1. Для выбора примитивных многочленов при построении БЧХ-кодов составлены специальные таблицы.

   Хорошие коды БЧХ небольшой длины существуют, но, как правило, не лучшие из известных.

2. Разработаны достаточно эффективные методы декодирования БЧХ-кодов (Форни, Берлекэмпа – Мэсси, Питерсона – Горенстейна – Цирлера, Сугиямы, ...).

   При этом никаких более эффективных способов вычисления позиций ошибок, кроме полного перебора корней и нахождения элементов, обратных к найденным локаторам (т. н. *процедура Ченя*) до сих пор не открыто.

3. В методическом плане коды БЧХ обладают относительно простой и ясной конструкцией, что облегчает понимание многих других видов циклических кодов.

Указанные достоинства кодов БЧХ, казалось бы, закрывают проблему выбора помехоустойчивых кодов для различных задач. Однако коды БЧХ являются *асимптотически плохими*: с увеличением длины n кодового слова как скорость кода k/n, так и отношение d/n стремятся к нулю.

Известный американский учёный в области кодирования *Элвин Берлекемп* (*Elwyn Berlekamp*, 1940–2019) в своей классической монографии *Алгебраическая теория кодирования* пишет: «*Истинное достоинство конструкции Боуза – Чоудхури – Хоквингема состоит не в теореме о том, что для любого данного t можно построить коды с исправлением t ошибок. ... Важнейшее свойство БЧХ-кодов состоит в том, что они позволяют исправить t ошибок (и многие ошибки более высокой кратности) с помощью легко реализуе-*

мого алгоритма».

Крупнейшему специалисту в области теории информации *Питеру Элаису* (*Peter Elias*, 1923–2001), открывшему в 1955 г. свёрточные коды, принадлежит фраза: «*Я могу предложить систему кодирования со сколь угодно малой вероятностью пропуска ошибки, но я не уверен, что мой правнук дождётся её декодирования*».

Для исправления ошибок сейчас, как правило, применяют *коды Рида – Соломона*, способные исправлять *пакеты ошибок* (burst error) замещения. Это принципиально недвоичные коды, являющиеся подклассом недвоичных кодов БЧХ.

Коды Рида – Соломона могут быть использованы для восстановления потерянных символов в компьютерных сетях передачи информации. Однако для этих целей в последнее время разработаны специальные *фонтанные коды*, использующие не алгебраическое, *стохастическое кодирование* пакетов данных.

Глава 4

Теория перечислений Пойа

4.1 Действие группы на множестве

Пусть даны:

- группа $\langle\, G, \circ, e \,\rangle$, $|G| = n$;
- множество T, $|T| = N > 0$.
- $Bij(T)$ — множество всех перестановок элементов T (биекций на T).
- S_T — симметрическая группа множества T:

$$S_T \;=\; \langle\, Bij(T), *, 1_T \,\rangle.$$

Дадим два эквивалентных определения действия α группы G на множестве T; символически $G \underset{\alpha}{:} T$.

Обозначим через $\mathrm{Hom}\,(\,G_1, G_2\,)$ множество гомоморфизмов из группы G_1 в группу G_2 (о гомоморфизмах групп см. с. 12).

Определение 4.1 (I). $\alpha \in \mathrm{Hom}\,(\,G, S_T\,)$.

Определение 4.2 (II). $\alpha = \langle\, G, T; \circ, \triangleright, e, 1_T \,\rangle$ — двухосновная алгебра с носителями G и T, где

$G \times G \overset{\circ}{\to} G$ — групповая операция;

$G \times T \overset{\triangleright}{\to} T$ — новая некоммутативная операция.

Аксиомы для операций:

$$1.\ e \triangleright t = t; \qquad 2.\ (g \circ h) \triangleright t = h \triangleright (g \triangleright t).$$

Запись операции $\triangleright$: $g(t) = t'$.
Тогда аксиомы: $e(t) = t$ и $(g \circ h)(t) = h(g(t))$.

Элементы g группы G порождают перестановки на T, обладающие указанными свойствами.

Действие α группы G на множестве T называют *эффективным*, если для любых двух перестановок $g, h \in G$, $g \neq h$ существует элемент $t \in T$ такой, что $g(t) \neq h(t)$. *Тривиальное действие* $\forall\, g \in G : \alpha(g) = 1_T$ неэффективно.

Для данной перестановки g:

Введём отношение эквивалентности $\sim_g$ на T —

$$t \sim_g t' \Leftrightarrow \exists\, k \in \mathbb{Z} : g^k(t) = t'$$

Рефлексивность (R), *симметричность* (S) и *транзитивность* (T) отношения $\sim_g$ легко показываются.

Смежные классы эквивалентности $\sim_g$ называются *g-циклами*: элементы этих классов образуют циклы:

$$t \overset{g}{\to} t' \overset{g}{\to} \ldots \overset{g}{\to} t, \qquad \textit{и у каждого элемента —}$$

по единственной входящей и исходящей стрелке.

Обозначения:

- $\nu_1, \nu_2, \ldots, \nu_N$ — количества циклов длины $1, 2, \ldots, N$;
- $\langle\, \nu_1, \nu_2, \ldots, \nu_N \,\rangle = Type(g)$ — *тип перестановки* g — упорядоченная совокупность числа циклов длины $1, 2, \ldots, N$ соответственно;

- $C(g)$ — число всех g-циклов (классов эквивалентности $\sim_g$).

Понятно, что $\sum\limits_{k=1}^{N} \nu_k(g) = C(g)$ и $\sum\limits_{k=1}^{N} k \cdot \nu_k(g) = N$.

Пример 4.3. Пусть $T = \{1, \ldots, 10\}$ и

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} =$$
$$= (1,9,3)(2,6)(4,8,10)(5)(7) = (2,6)(1,9,3)(4,8,10).$$

Тогда $Type(g) = \langle 2, 1, 2, 0, \ldots, 0 \rangle$ и

$$C(g) = 2 + 1 + 2 = 5, \quad \big|T\big| = 2 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 = 10.$$

По всей группе G:

Отношение эквивалентности $\sim_G$ на T —

$$t \sim_G t' \Leftrightarrow \exists\, g \in G : g(t) = t'.$$

Свойства (R), (S) и (T) отношения $\sim_G$ очевидны.

- Классы этой эквивалентности называют *орбитами*; они образуют разбиение множества T.
- Класс эквивалентности, в которую попадает элемент t обозначаем $\mathrm{Orb}\,(t)$.
- Число получившихся орбит — $C(G)$.

Если $C(G) = 1$ (любой элемент T может быть переведён в любой), то действие $G \underset{\alpha}{:} T$ называют *транзитивным*.

Фиксатор перестановки и стабилизатор элемента множества. Выясним, когда выполняется равенство

$$g(t) \;=\; t.$$

Для этого рассмотрим два случая, в которых полагаем заданным либо t, либо g.

1. Фиксируем g, т. е. находим все элементы множества T, которые данная перестановка оставляет на месте — это *фиксатор перестановки* $g \in G$:

$$\left\{\, t \in T \mid g(t) = t \,\right\} \;=\; \mathrm{Fix}\,(g) \;\subseteq\; T.$$

2. Считаем данным t, т. е. находим все перестановки g, которые оставляют этот элемент неподвижным — это *стабилизатор элемента* $t \in T$:

$$\left\{\, g \in G \mid g(t) = t \,\right\} \;=\; \mathrm{Stab}\,(t) \;\subseteq\; G.$$

Очевидно $\forall\, t \in T : \; e \in \mathrm{Stab}\,(t)$, т. е. $\mathrm{Stab}\,(t) \neq \varnothing$. И более того, стабилизатор есть подгруппа группы G:

Утверждение 4.4. $\qquad \mathrm{Stab}\,(t) \leqslant G.$

Доказательство. Для $t \in T$ рассмотрим $g,\, h \in \mathrm{Stab}\,(t)$. Тогда $g(t) = h(t) = t$ и $h^{-1}(t) = t$. Следовательно

$$(g \circ h^{-1}) \triangleright t \;=\; t \;\Rightarrow\; g \circ h^{-1} \in \mathrm{Stab}\,(t)\,.$$

□

Поэтому стабилизатор $\mathrm{Stab}\,(t)$ называют ещё *стационарной подгруппой*[1] *элемента* t и обозначают иногда G_t.

[1] или *изотопической подгруппой*

Утверждение 4.5. *При действии группы G на множество T между множеством левых смежных классов G по стационарной подгруппе G_t элемента $t \in T$ и его орбитой $\mathrm{Orb}\,(t)$ существует взаимно однозначное соответствие.*

Доказательство. Левые смежные классы G по G_t обозначаем gG_t, $g \in G$, считая при этом, что на элементы T сначала действует некоторая перестановка из G_t, а затем — фиксированная перестановка g.

Но тогда любая перестановка $h \in gG_t$ одинаково подействует на $t \in T$: $h(t) = g(t) = t' \in \mathrm{Orb}\,(t)$ (т. к. все элементы G_t оставляют t на месте). С учётом того, что смежные классы либо совпадают, либо не пересекаются, утверждение доказано. □

Из этого утверждения вытекает важное

Следствие. *Длина орбиты $\mathrm{Orb}\,(t)$ равна индексу стационарной подгруппы $\mathrm{Stab}\,(t)$ в группе G:*

$$\big|\,\mathrm{Orb}\,(t)\big| \;=\; \frac{\big|G\big|}{\big|\,\mathrm{Stab}\,(t)\big|} \;=\; [\,G : \mathrm{Stab}\,(t)\,]\,.$$

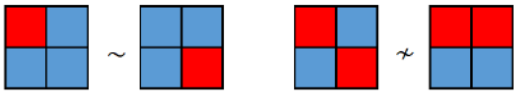
Доказательство. По теореме Лагранжа

$$H \leqslant G \;\Rightarrow\; \big|\,G\,\big| = \big|\,H\,\big| \cdot [\,G : H\,]$$

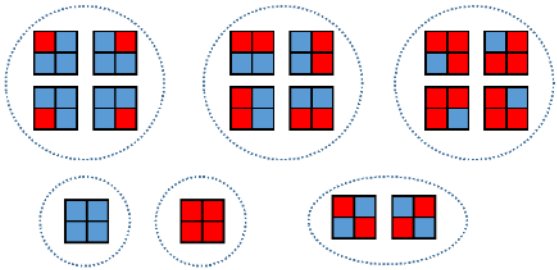
число смежных классов группы G по её подгруппе $H \leqslant G$ равно индексу $[\,G : H\,]$. □

4.2 Постановка задачи. Лемма Бёрнсайда

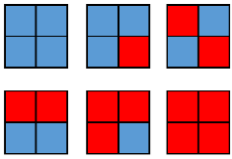
Рассмотрим такую задачу: каким количеством способов можно раскрасить клетки доски 2×2 в красный и синий цвета? Раскраски считаются различными, если одну из другой нельзя получить поворотами доски:



Множество всевозможных раскрасок разбивается на классы эквивалентности, и нам нужно найти число этих классов.



Итак, раскрасить клетчатую доску 2×2 в красный и синий цвета можно шестью различными способами:



Множество всевозможных раскрасок разбивается на классы эквивалентности, и нам нужно найти число этих классов.

Нижеприведённую лемму обычно связывают с именем английского алгебраиста Уильяма Бёрнсайда (1852–1927), который сформулировал и доказал её в 1897 г. Однако О. Коши в 1845 г. и Ф. Фробениусу в 1887 г. уже была известна доказываемая в ней формула. Поэтому данную лемму иногда иронически называют *леммой не Бёрнсайда*.

Лемма 4.6 (Бёрнсайд). *Если группа G действует на множестве T, то*

$$C(G) = \frac{1}{|G|}\sum_{g\in G}\Big|\operatorname{Fix}(g)\Big| = \frac{1}{|G|}\sum_{t\in T}\Big|\operatorname{Stab}(t)\Big|;$$

при этом первое равенство называется леммой Бёрнсайда.

Доказательство. Пусть $|G| = n$, $|T| = N$ и действие $G \overset{\alpha}{:} T$ задаётся $n \times N$ матрицей $A = \|g_i(t_j)\|$, $i = \overline{1,n}$, $j = \overline{1,N}$.

Подсчитаем двумя различными способами мощность множества $M = \big\{(g,t) \in G \times T \mid g(t) = t\big\}$: по столбцам и по строкам матрицы A. Получим

$$\sum_{g\in G}\Big|\operatorname{Fix}(g)\Big| = \big|M\big| = \sum_{t\in T}\Big|\operatorname{Stab}(t)\Big|.$$

Если x и y принадлежат одному классу эквивалентности по $\sim_G$, то $\operatorname{Orb}(x) = \operatorname{Orb}(y)$ и их стационарные подгруппы имеют одинаковую мощность:

$$|G_x| = \frac{|G|}{|\operatorname{Orb}(x)|} = \frac{|G|}{|\operatorname{Orb}(y)|} = |G_y|.$$

Выберем по представителю $t_1, \ldots, t_{C_G}$ из всех $C(G)$ орбит. Тогда

$$|M| = \sum_{t \in T} |G_t| = \sum_{i=1}^{C(G)} |G_{t_i}| \cdot \left| \operatorname{Orb}(t_i) \right| =$$

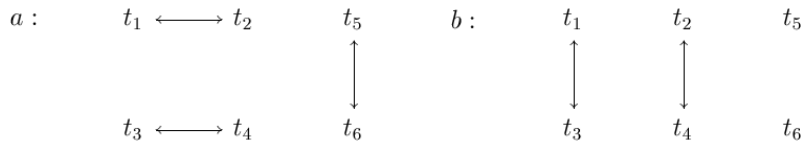
$$= \sum_{i=1}^{C(G)} \frac{|G|}{\left| \operatorname{Orb}(t_i) \right|} \cdot \left| \operatorname{Orb}(t_i) \right| = |G| \cdot C(G).$$

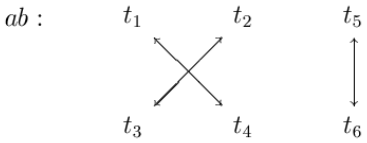
□

Пример 4.7. Действие четверной группы Клейна V_4 на множестве $T = \{ t_1, \ldots, t_6 \}$:

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$\triangleright$	t_1	t_2	t_3	t_4	t_5	t_6
e	t_1	t_2	t_3	t_4	t_5	t_6
a	t_2	t_1	t_4	t_3	t_6	t_5
b	t_3	t_4	t_1	t_2	t_5	t_6
ab	t_4	t_3	t_2	t_1	t_6	t_5





$$Type(e) = \langle 6, 0, 0, 0, 0, 0 \rangle, \quad Type(a) = \langle 0, 3, 0, 0, 0, 0 \rangle,$$

$$Type(b) = \langle 2,2,0,0,0,0\rangle, \quad Type(ab) = \langle 0,3,0,0,0,0\rangle.$$
$$C(e) = 6,\ C(a) = C(ab) = 3,\ C(b) = 4.$$
$$\mathrm{Stab}\,(t_1) = \mathrm{Stab}\,(t_2) = \mathrm{Stab}\,(t_3) = \mathrm{Stab}\,(t_4) = e \leqslant V_4,$$
$$\mathrm{Stab}\,(t_5) = \mathrm{Stab}\,(t_6) = \langle e, b\rangle \leqslant V_4.$$
$$\mathrm{Fix}\,(a) = \mathrm{Fix}\,(ab) = \varnothing,\ \mathrm{Fix}\,(b) = \{t_5, t_6\},\ \mathrm{Fix}\,(e) = T.$$
$$\big|\,\mathrm{Orb}\,(t_1)\big| = \frac{4}{1} = 4, \quad \big|\,\mathrm{Orb}\,(t_5)\big| = \frac{4}{2} = 2.$$
$$\frac{1}{4}\sum_{g\in G}\big|\,\mathrm{Fix}\,(g)\big| = \frac{6+2}{4} = 2,$$
$$\frac{1}{4}\sum_{t\in T}\big|\,\mathrm{Stab}\,(t)\big| = \frac{4\cdot 1 + 2\cdot 2}{4} = 2.$$

Как применять лемму Бёрнсайда? Для определения числа классов эквивалентности надо представить *отождествляемые элементы множества* T *как классы эквивалентности* действия некоторой группы G на T и по лемме Бёрнсайда определить $C(G)$.

Задача 4.1 (про слова). Составляются слова длины $l \geqslant 2$ из алфавита $A = \{\, a_1, \ldots, a_q \,\}$. Слова считаются эквивалентными, если они получаются одно из другого перестановкой крайних букв. Определить число S неэквивалентных слов.

Решение (прямым использованием леммы Бёрнсайда). Пусть T — множество слов длины l в алфавите A, $|T| = N = q^l$.

Надо представить эквивалентности как орбиты некоторого действия подходящей группы G на T.

Очевидно, двукратная перестановка не меняет ничего, и поэтому подходит $G \cong \mathbb{Z}_2 = \{ e, f \}$. Действие f: переставляет в слове крайние буквы.

Число неэквивалентных слов = число классов эквивалентности действия $\mathbb{Z}_2 \underset{\alpha}{:} T$ —

$$\big|\operatorname{Fix}(e)\big| = \big|T\big| = q^l, \qquad \big|\operatorname{Fix}(f)\big| = q^{l-2} \cdot q = q^{l-1}.$$

$$W = C(\mathbb{Z}_2) = \frac{1}{2} \sum_{g \in G} \big|\operatorname{Fix}(g)\big| = \frac{q^l + q^{l-1}}{2} = \frac{q^{l-1}(q+1)}{2}.$$

Для $l = 3$, $q = 2$ имеем $|T| = 8$ и $W = \frac{4 \cdot 3}{2} = 6$. Пусть $A = \{a, b\}$, тогда слова и классы —

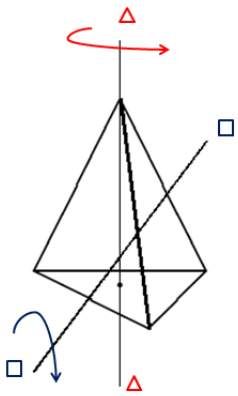
	aaa		(1)
aab		baa	(2)
	aba		(3)
abb		bba	(4)
	bab		(5)
	bbb		(6)

Платоновы тела — правильные 3-мерные многогранники. Рассматриваем их группы *вращений* (самосовмещений в 3-хмерном пространстве).

Платоновы тела	*Группа* вращения	*Порядок* группы
тетраэдр	T (тетраэдра)	$4 \cdot 3 = 12$
куб и октаэдр	O (октаэдра)	$8 \cdot 3 = 24$
икосаэдр и додекаэдр	Y (икосаэдра)	$12 \cdot 5 = 60$

Икосаэдр имеет 20 граней, 30 рёбер и 12 вершин.

T — группа вращения тетраэдра



$T = \langle t,\ f \rangle,\ t^3 = f^2 = e$, где:

t — вращение на $120°$ вокруг оси, проходящей через вершину и центр тетраэдра (△—△); таких осей 4.

f — вращение на $180°$ вокруг оси, проходящей через центры двух противоположных рёбер (□—□); таких осей 3.

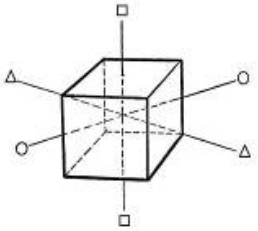
$|T| = (3-1)\cdot 4 + (2-1)\cdot 3 + 1 = 12.$

Действие T на грани (или вершины) тетраэдра: типы перестановок

$$\square:\ Type(t) = Type(t^2) = \langle 1,0,1,0\rangle;$$
$$\triangle:\ Type(f) = \langle 0,2,0,0\rangle.$$

Тетраэдр двойственен самому себе $\Rightarrow$ действие на грани = действие на вершины.

O — группа вращения октаэдра (= куба)



$O = \langle t, f, r\rangle, t^4 = f^2 = r^3 = e$, где:
t — вращение на $90°$ вокруг оси, проходящей через середины двух противоположных граней (□—□), таких осей 3;
f — вращение на $180°$ вокруг оси, проходящей через середины двух противоположных рёбер (○—○), таких осей 6;

r — вращение на 120° вокруг оси, проходящей через две противоположные вершины ($\triangle$—$\triangle$) таких осей 4.

$$|O| = 3 \cdot 3 + 1 \cdot 6 + 2 \cdot 4 + 1 = 24.$$

Пример 4.8 (Действие O на вершины куба: типы перестановок).

$$\begin{aligned}
\square: \ Type(t) &= Type(t^3) = \langle 0,0,0,2,0,\ldots\rangle;\\
Type(t^2) &= \langle\, 0,4,0,\ldots\,\rangle;\\
\circ: \ Type(f) &= \langle\, 0,4,0,\ldots\,\rangle;\\
\triangle: \ Type(r) &= Type(r^2) = \langle\, 2,0,2,0,\ldots\,\rangle.
\end{aligned}$$

Поскольку $|G| = |G_x| \cdot [G : G_x]$, то число элементов в группе вращения правильного многогранника есть $\big|E_0\big| \cdot \big|V\big|$, где $\big|E_0\big|$ — число рёбер, выходящих из одной вершины и $\big|V\big|$ — число вершин многогранника.

4.3 Цикловой индекс

Определение. Существует универсальный способ вычисления числа $C(G)$ — количества классов эквивалентности (= орбит).

Сопоставим каждой перестановке $g \in G$ вес $w(g)$ по правилу:

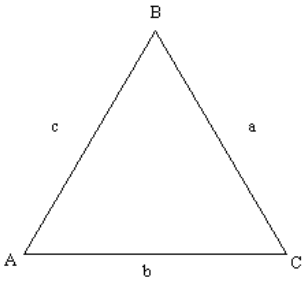
$$Type(g) = \langle \nu_1, \ldots, \nu_N \rangle \ \Rightarrow \ w(g) = \underbrace{x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}}_{\text{моном}}.$$

Определение 4.9. *Цикловым индексом* $Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N)$ действия группы G на множестве T называют средний вес подстановок в группе:

$$Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N) = \frac{1}{|G|} \sum_{g \in G} w(g) = \\ = \frac{1}{|G|} \sum_{g \in G} x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

Пример 4.10. Вычислим цикловой индекс действия группы всех преобразований правильного треугольника в себя (т. е. оставляющих его неподвижным), на его стороны.

T — стороны треугольника, $N = 3$.
$G \cong S_3 = \langle t, f \rangle$ — все перестановки сторон,
$n = 3! = 6$.



$G \underset{\alpha}{:} T$ — самодействие группы S_3
Треугольник — самодвойственная фигура $\Rightarrow$
$\Rightarrow$ действие на стороны $=$
$=$ действие на вершины

$$Im(G \underset{\alpha}{:} T) = \\ = \{ e, \underbrace{(abc)}_{t}, \underbrace{(acb)}_{t^2}, \underbrace{((a)(bc))}_{f}, \underbrace{((b)(ac))}_{tf}, \underbrace{((c)(ab))}_{t^2 f} \}.$$

$g \in S_3$	$Type(g)$	$w(g)$	# мономов
$e = (a)(b)(c)$	$\langle\, 3,\, 0,\, 0 \,\rangle$	x_1^3	1
$t,\, t^2$	$\langle\, 0,\, 0,\, 1 \,\rangle$	x_3^1	2
$f,\, tf,\, t^2 f$	$\langle\, 1,\, 1,\, 0 \,\rangle$	$x_1^1 x_2^1$	3
Всего			6

$$Z(S_3) = \frac{1}{6}\big[\, x_1^3 + 2x_3^1 + 3x_1^1 x_2^1 \,\big] \; -$$

— цикловой индекс *самодействия группы* S_3, или, что то же, *группы симметрии треугольника*.

Определение числа классов эквивалентности. *Зачем нужен цикловой индекс?*
Пусть заданы множество T, группа G и действие $G \underset{\alpha}{:} T$.

1. Припишем каждому элементу T одно из r значений (неформально: покрасим в один из r цветов). Всего, очевидно, имеется r^N раскрасок.

2. *Не будем различать раскраски*, если элементы t и $t' = g(t)$ раскрашены одинаково.

Вопрос: сколько существует *неэквивалентных раскрасок = классов эквивалентности*?
Ответ: это значение вычисляется через цикловой индекс. Имеем —

1. Каждый класс эквивалентности — это g-цикл; их $C(g) = \nu_1 + \ldots + \nu_N$ штук.

2. Каждая перестановка $g \in G$ с типом $\langle \nu_1, \ldots, \nu_N \rangle$ будет иметь $|\operatorname{Fix}(g)| = r^{C(g)}$ неподвижных точек: каждый класс эквивалентности это g-цикл, их $C(g)$ и

$$\big|\operatorname{Fix}(g)\big| \;=\; x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}\Big|_{x_1=\ldots=x_N=r} \;=\; r^{C(g)}.$$

Отсюда, по лемме Бёрнсайда, число полученных классов эквивалентности = неэквивалентных раскрасок:

Теорема 4.11 (Пойа).

$$C(G \underset{\alpha}{:} T) \;=\; Z(G \underset{\alpha}{:} T,\, x_1,\, \ldots,\, x_N)\Big|_{x_1=\ldots=x_N=r}.$$

Например, $Z_G(1, \ldots, 1) = 1$: если все элементы покрасить в один цвет, то таких раскрасок одна.

4.4 Задачи на применение циклового индекса

Задача 4.1 (про слова). Определить число S неэквивалентных слов длины $\ell \geqslant 2$ в q-буквенном алфавите, если эквивалентными считаются слова, получающиеся друг из друга перестановкой крайних букв.

Было решение: $\quad S = \dfrac{q^\ell + q^{\ell-1}}{2}.$

Решение (новое, использующее цикловой индекс):

$G = \{\, e,\, g \,\} \;\cong\; \mathbb{Z}_2; \quad T\colon \underbrace{\bigcirc\overbrace{\bigcirc\ldots\bigcirc}^{\ell-2}\bigcirc}_{\ell}.$

$g \in G$	$Type(g)$	$w(g)$	# мономов
e	$\langle \ell, 0, \ldots, 0 \rangle$	x_1^ℓ	1
g	$\langle \ell-2, 1, 0, \ldots, 0 \rangle$	$x_1^{\ell-2}x_2^1$	1
Всего			$\lvert G\rvert = 2$

Цикловой индекс: $Z(x_1, \ldots, x_\ell) = \dfrac{1}{2}\left[x_1^\ell + x_1^{\ell-2}x_2\right]$.

$$S = Z(q, \ldots, q) = \frac{q^\ell + q^{\ell-1}}{2}.$$

Задача 4.2 (самая первая). Сколькими способами можно раскрасить доску 2×2 в r цветов, если раскраски, переходящие друг в друга при вращении квадрата, считаются одинаковыми?

Решение. Группа вращения квадрата — Z_4.

$g \in Z_4$	$Type(g)$	$w(g)$	#
e	$\langle 4,0,0,0\rangle$	x_1^4	1
$t,\ t^3$	$\langle 0,0,0,1\rangle$	x_4^1	2
t^2	$\langle 0,2,0,0\rangle$	x_2^2	1
Всего			4

Цикловой индекс:

$$P_{Z_4}(x_1, \ldots, x_4) = \frac{1}{4}\left[\, x_1^4 + 2x_4 + x_2^2 \,\right].$$

$$\#\text{раскрасок} = P(r, \ldots, r) = \frac{r^4 + 2r + r^2}{4};$$

$$\text{для 2-х цветов: } P(2, \ldots, 2) = \frac{16 + 4 + 4}{4} = 6,$$

— как и было найдено при прямом подсчёте.

Классическая комбинаторная задача об ожерельях

- *Ожерелье* — окружность, на которой на равных расстояниях по дуге располагаются точки, которым приписан символ конечного алфавита — «окрашенные бусины».
- *Задача об ожерельях*: сколько различных ожерелий можно составить из N бусин r цветов?
- Какие ожерелья считать неразличимыми? *Варианты*: если одно ожерелье получается из другого *самосовмещением* —
  1) только *поворотом* в плоскости вокруг центра ожерелья[2)] — самодействие группы $\mathbb{Z}_N$;
  2) и *поворотом*, и *переворотом в пространстве* — самодействие *группы диэдра*[3)] D_N.

Задача 4.3 (об ожерельях $N = 5$, $r = 3$; 1-й вариант). Сколько разных ожерелий можно составить из 5 бусин 3 цветов?

1. Ожерелья одинаковы, если одно получается из другого *поворотом*.

Решение $G \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

Элемент $\mathbb{Z}_5$	$Type(g)$	$w(g)$	# мономов
e	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
t, t^2, t^3, t^4	$\langle 0, 0, 0, 0, 1 \rangle$	x_5	4

[2)] т. н. *карусель*

[3)] двойной пирамиды

Цикловой индекс: $Z(x_1, \ldots, x_5) = \frac{1}{5}\left[x_1^5 + 4x_5\right]$.

$$\#Col(3) = Z(3, \ldots, 3) = \frac{1}{5}\left(3^5 + 4 \cdot 3\right) = 51.$$

Задача 4.4 (Олимпиады «*Покори Воробьёвы горы – 2009*»). Для 50 детей детского сада закуплены 50 одинаковых тарелок. По краю каждой тарелки равномерно расположено 5 белых кружочков. Воспитатели хотят закрасить какие-либо из этих кружочков в другие цвета так, чтобы все тарелки стали различными.

Какое наименьшее число дополнительных цветов потребуется им для этого?

Как должны были решать школьники. Пусть требуется r цветов.

Отбросим r вариантов раскраски в один цвет. Число остальных вариантов —

без учёта возможности поворота тарелки: $r^5 - r$;

с учётом поворота: $\frac{r^5 - r}{5}$, т. к. каждый вариант повторяется 5 раз.

Итого: $\#Col(r) = \frac{r^5 - r}{5} + r = \frac{r^5 + 4r}{5}$, и при 2-х дополнительных цветах — $\#Col(3) = 51$.

Решая эту задачу, мы доказали малую теорему Ферма:

Теорема 4.12 (Ферма, малая). *Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.*

Доказательство. Число различных раскрасок непомеченных вершин правильного p-угольника более, чем в один из a цветов при простом p равно $\frac{a\cdot\left(a^{p-1}-1\right)}{p}$ (целое число).

Отсюда, если a не делится на p, то на p делится $(a^{p-1}-1)$, то есть $a^{p-1} \equiv_p 1$. □

Задача 4.4 (об ожерельях $N = 5$, $r = 3$; 2-й вариант).

2. Ожерелья одинаковы, если одно получается из другого *поворотом и/или переворотом.*

Решение G — *группа диэдра* $D_5 = \langle t, f\rangle$, $t^5 = f^2 = e$, $n = |D_5| = 10$.

Элемент D_5	$Type(g)$	$w(g)$	# мономов
e	$\langle\, 5,\, 0,\, 0,\, 0,\, 0\,\rangle$	x_1^5	1
$t,\, t^2,\, t^3,\, t^4$	$\langle\, 0,\, 0,\, 0,\, 0,\, 1\,\rangle$	x_5	4
$f,\, tf,\, \ldots,\, t^4f$	$\langle\, 1,\, 2,\, 0,\, 0,\, 0\,\rangle$	$x_1x_2^2$	5
Всего			10

Цикловой индекс: $P = \dfrac{1}{10}\left[\, x_1^5 + 4x_5 + 5x_1x_2^2\,\right]$.

$$\#Col(3) \;=\; Z(x_1,\ldots,x_5)\Big|_{x_1=\ldots=x_5=3} = \\ = \frac{3^5 + 4\cdot 3 + 5\cdot 3^3}{10} \;=\; 39.$$

Задача 4.6 (о раскраске сторон квадрата). Сколько существует различно окрашенных квадратов, если их стороны раскрашивают в r цветов?

Решение. Группа самосовмещения квадрата в пространстве — группа диэдра $D_4 = \langle t, f, s \rangle$, $|D_4| = 8$, которая порождается тремя образующими:

t : вращение на 90° вокруг центра в выбранном направлении;

f : симметрия относительно оси, проходящей через середины противоположных *сторон* — 2 оси;

s : симметрия относительно оси, проходящей через середины противоположных *вершин* — 2 оси.

При самодействии группы D_4 ($N = 4$) её элементы будут иметь следующие веса:

e : единичная перестановка оставит все стороны на месте, т. е. имеются 4 цикла длины 1, вес x_1^4 (одна перестановка);

t, t^3 : стороны циклически переходят друг в друга по и против часовой стрелке, длина цикла 4, вес x_4^1 (две перестановки);

t^2 : стороны переходят в противоположные, что даёт два цикла длины 2, вес — x_2^2 (одна перестановка);

f : две противоположные стороны на месте, остальные две меняются местами, т. е. имеются два единичных цикла и один длины 2, вес — $x_1^2 x_2^1$ (одна перестановка, 2 оси);

s : в двух парах смежных сторон элементы меняются местами, что даёт два цикла длины 2, вес — x_2^2 (одна перестановка, 2 оси).

Итого:

Элемент D_5	$Type(g)$	$w(g)$	# мономов
e	$\langle 5, 0, 0, 0 \rangle$	x_1^4	1
t, t^3	$\langle 0, 0, 0, 1 \rangle$	x_4	2
t^2	$\langle 0, 2, 0, 0 \rangle$	x_2^2	1
f	$\langle 2, 1, 0, 0 \rangle$	$x_1^2 x_2$	$1 \times 2 = 2$
s	$\langle 0, 2, 0, 0 \rangle$	x_2^2	$1 \times 2 = 2$
Всего			8

Цикловой индекс самодействия D_4:

$$Z_{D_4}(x_1, \ldots, x_4) = \frac{1}{8}\left[x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2 x_2 \right].$$

Число раскрасок квадрата в r цветов:

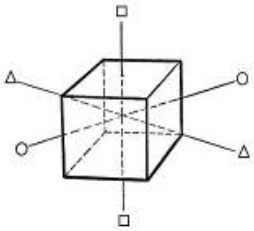
$$Z_{D_4}(r, \ldots, r) = \frac{1}{8}\left[r^4 + 2r + 3r^2 + 2r^3 \right].$$

В частности, в три цвета:

$$\#Col(3) = \frac{3^4 + 2 \cdot 3 + 3^4}{8} = \frac{81 + 6 + 81}{8} = 21.$$

Задача 4.7. Грани куба раскрашивают в 2 и 3 цвета. Сколько существует различно окрашенных кубов?

Решение. Напоминание: $G = O$, $|O| = 24$. $O = \langle t, f, r \rangle, t^4 = f^2 = r^3 = e$, где: t — вращение на 90° вокруг оси, проходящей через середины двух противоположных граней (□—□), таких осей 3;



f — вращение на 180° вокруг оси, проходящей через середины двух противоположных рёбер (○—○), таких осей 6;
r — вращение на 120° вокруг оси, проходящей через две противоположные вершины (△—△) таких осей 4.

Обозначим через F множество граней куба; $|F| = N = 6$. Выберем некоторую грань куба (квадрат) и обозначим её ①, а параллельную ей — ②.
Перенумеруем последовательно вершины грани ① числами 1, ..., 4, а вершины грани ② — числами 5, ..., 8 так, что вершина с номером i смежна с вершиной с номером $i+4$, $i = 1, 2, 3, 4$.

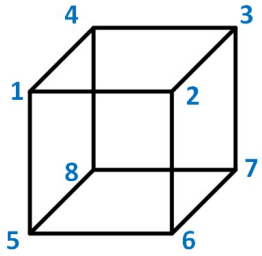
Перестановки далее указаны для случая, когда ось вращения

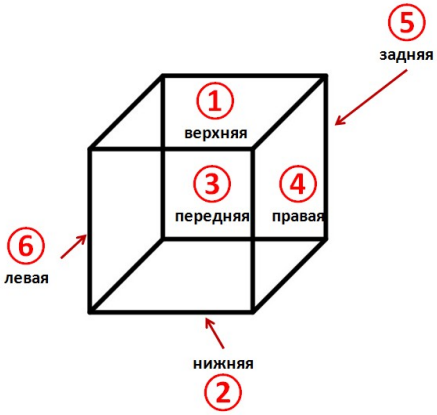
$\langle t \rangle$ проходит через середины граней ① и ②,

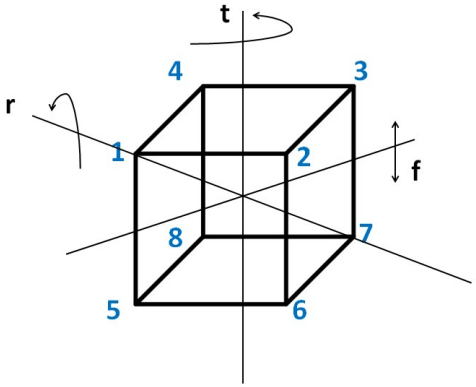
$\langle f \rangle$ проходит через середины рёбер (3-7) и (1-5),

$\langle s \rangle$ проходит через вершины (1) и (7),

а грани обозначены: (1-2-6-5) через ③, параллельная ей грань — ⑤, грань (2-3-7-6) — через ④, параллельная ей грань — ⑥.







$g \in O$	перестановка	$Type(g)$	$w(g)$	#
e	(①)…(⑥)	$\langle 6, 0, \ldots \rangle$	x_1^6	1
t, t^3	(①)(②)(③④⑤⑥)	$\langle 2, 0, 0, 1, 0, \rangle$	$x_1^2 x_4$	6
t^2	(①)(②)(③⑤)(④⑥)	$\langle 2, 2, 0, \ldots \rangle$	$x_1^2 x_2^2$	3
f	(①②)(③⑥)(④⑤)	$\langle 0, 3, 0, \ldots \rangle$	x_2^3	6
r, r^2	(①③⑥)(②④⑤)	$\langle 0, 0, 2, 0, \ldots \rangle$	x_3^2	8
Всего				24

$$Z(x_1, \ldots, x_6) = \frac{1}{24}\left[x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2\right].$$

$$\#Col(2) = \frac{1}{24}\left[2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 8\cdot 2^2\right] = 10,$$
$$\#Col(3) = \frac{1}{24}\left[3^6 + 12\cdot 3^3 + 3\cdot 3^4 + 8\cdot 3^2\right] = 48.$$

Цикловой индекс действия группы октаэдра на множестве R рёбер куба ($|R| = N = 12$):

$g \in O$	$Type(g)$	$w(g)$	$\#$
e	$\langle\, 12,\, 0,\, \ldots \rangle$	x_1^{12}	1
t, t^3	$\langle\, 0,\, 0,\, 0,\, 3,\, 0,\, 0 \rangle$	x_4^3	$3\cdot 2 = 6$
t^2	$\langle\, 0,\, 6,\, 0,\, \ldots \rangle$	x_2^6	3
f	$\langle\, 2,\, 5,\, 0,\, \ldots \rangle$	$x_1^2 x_2^5$	6
r, r^2	$\langle\, 0,\, 0,\, 4,\, 0,\, \ldots \rangle$	x_3^4	$4\cdot 2 = 8$

$$Z(O \underset{\alpha}{:} R) = \frac{1}{24}\left[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \,\right].$$

Цикловой индекс действия группы октаэдра на множестве V вершин куба ($|V| = N = 8$):

$g \in O$	$Type(g)$	$w(g)$	$\#$
e	$\langle\, 8,\, 0,\, \ldots \rangle$	x_1^8	1
t, t^3	$\langle\, 0,\, 0,\, 0,\, 2,\, 0,\, 0 \rangle$	x_4^2	$3\cdot 2 = 6$
t^2	$\langle\, 0,\, 4,\, 0,\, \ldots \rangle$	x_2^4	3
f	$\langle\, 0,\, 4,\, 0,\, \ldots \rangle$	x_2^4	6
r, r^2	$\langle\, 2,\, 0,\, 2,\, 0,\, \ldots \rangle$	$x_1^2x_3^2$	$4\cdot 2 = 8$

$$Z(O \underset{\alpha}{:} V) = \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$

Цикловые индексы самодействия S_n, $\mathbb{Z}_n$, D_n и действия O на элементы куба

$$Z(S_n) = \sum_{\substack{(j_1,\dots,j_n)\in \mathbb{N}_0^n \\ 1j_1+2j_2+\dots+nj_n=n}} \frac{x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}}{(1^{j_1}j_1!)(2^{j_2}j_2!)\dots(n^{j_n}j_n!)},$$

$$Z(\mathbb{Z}_n) = \frac{1}{n}\sum_{d|n}\varphi(d)\,x_d^{n/d}, \quad \varphi - \text{функция Эйлера},$$

$$Z(D_n) = \frac{1}{2}Z(\mathbb{Z}_n) + \begin{cases} \frac{1}{2}\,x_1x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[\,x_2^{n/2} + x_1^2x_2^{n/2-1}\,\right], & n \text{ чётно}, \end{cases}$$

$$Z(O \underset{\alpha}{:} V) = \frac{1}{24}\left[\,x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2\,\right],$$

$$Z(O \underset{\alpha}{:} E) = \frac{1}{24}\left[\,x_1^{12} + 3x_2^6 + 8x_3^4 + 6x_1^2x_2^5 + 6x_4^3\,\right],$$

$$Z(O \underset{\alpha}{:} F) = \frac{1}{24}\left[\,x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2\,\right].$$

4.5 Задачи перечислительной комбинаторики

К множеству T, $|T| = N$, группе G, $|G| = n$ и действию $G \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \dots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T.

G, действуя на T, действует и на R^T.Придадим вес элементам R: $w(c_i) = y_i,\ i = \overline{1,r}$.

Теорема 4.13 (Редфилда – Пойа; 1927, 1937[4]). *Цикловой индекс действия группы G на R^T есть*

$$Z(G \underset{\alpha}{:} R^T, y_1, \ldots, y_r) = \\ = Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N)\Big|_{x_k = y_1^k + \ldots + y_r^k,\, k = \overline{1,N}}.$$

Следствие. Если все веса выбраны одинаковыми, т. е. $y_1 = \ldots = y_r = 1$, то $x_1 = \ldots = x_N = r$ и число классов эквивалентности

$$W(F) = Z(G \underset{\alpha}{:} T, r, \ldots, r)$$

— лемма Бёрнсайда.

Что можно определить (подсчитать) с помощью:

леммы Бёрнсайда — *общее число* неэквивалентных разметок (раскрасок);

теоремы Редфилда – Пойа — число разметок *данного типа*, т. е. содержащих данное количество элементов конкретного цвета (метки).

Усложним задачу об ожерельях:

Задача 4.3 (об ожерельях $N = 5$, $r = 3$, продолжение, более сложный вариант). Цвета — *красный*, синий, зелёный. Ожерелья одинаковы, если одно получается из другого поворотом и переворотом. Сколько имеется ожерелий, имеющих ровно 2 *красные* бусины?

[4] Теорема впервые опубликована *Джоном Говардом Редфилдом* в 1927 г., но его работа осталась незамеченной. Независимо доказана *Дьердем Пойа* в 1937 г. с демонстрацией применимости результата к перечислению химических соединений.

Решение. Было: $G = D_5$, цикловой индекс

$$Z_{D_5}(x_1, \ldots, x_5) = \frac{1}{10}\left[x_1^5 + 4x_5 + 5x_1x_2^2\right],$$

всего ожерелий $Z_{D_5}(3, \ldots, 3) = 39$ («карусель» — 51). Подстановка:

$x_1 = y_1+y_2+y_3,\ \ x_2 = y_1^2+y_2^2+y_3^2,\ \ \ldots,\ \ x_5 = y_1^5+y_2^5+y_3^5.$

$$\left\{\begin{array}{ll} w(\textit{красный}) & = y_1, \\ w(\textit{синий}) & = y_2, \\ w(\textit{зелёный}) & = y_3 \end{array}\right. \Rightarrow \left\{\begin{array}{l} y_1 = y, \\ y_2 = y_3 = 1 \end{array}\right. \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{ll} x_1 & = y + 2, \\ x_2 & = y^2 + 2, \\ \ldots & \\ x_5 & = y^5 + 2. \end{array}\right. \quad x_k \mapsto y^k + 2,\ k = \overline{1,5};$$

$$Z(y) = \sum_{i=1}^{5} u_i y^i;$$

$\boxed{u_2 = ?}$

$$Z(y) = \frac{1}{10}\left[u_0 + u_1 y + u_2 y^2 + \ldots + u_5 y^5\right] =$$

$$= \frac{1}{10}\left[(y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2\right] =$$

$$= \frac{1}{10}\left[\ldots + C_5^2 2^3 y^2 + \ldots + 5(y+2)(y^4+4y^2+4)\right] =$$

$$= \frac{1}{10}\left[\ldots + (10 \cdot 8 + 5 \cdot 2 \cdot 4)\, y^2 + \ldots\right].$$

$u_2 = 8 + 4 = 12.$

Задача 4.8 (о раскраске куба). Вершины куба помечают красными и синим цветами. Сколько существует

1) разнопомеченных кубов — $\#Col(2)$?

2) кубов, у которых половина вершины красные — $\#Col(4,4)$?

3) кубов, у которых не более 2 красных вершин — $\#Col(\leqslant 2, *)$?

Решение.

Цикловой индекс действия O на вершины куба —

$$Z(O \underset{\alpha}{:} V;\, x_1, \dots x_8) \,=\, \frac{1}{24}\big[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\big]\,.$$

$$1)\quad \#Col(2) = Z(x_1, \dots, x_8)\Big|_{x_1=\dots=x_8=2} =$$

$$= \frac{2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 8\cdot 4\cdot 4}{3\cdot 2^3} = \frac{32+3+18+16}{3} = 23.$$

2) $w(\textit{красный}) = y$, $w(\textit{синий}) = 1 \;\Rightarrow$,

$x_k = y^k + 1$, $k = \overline{1,8}$:

$$\#Col(4,4) \,=\, \frac{1}{24}\big[\,(y+1)^8 + 9\cdot(y^2+1)^4 + 6\cdot(y^4+1)^2 + 8\cdot(y+1)^2(y^3+1)^2\,\big] \,=$$

$$= \frac{1}{24}\big[\,\dots + C_8^4 y^4 + \dots + 9(\dots 4y^2 + 6y^4 + \dots) + 6(\dots + 2y^4 + \dots) + 8(y^2+2y+1)(\dots + 2y^3 + \dots)\,\big]\,.$$

$$u_4 \,=\, \frac{1}{24}\big[\,70 + 9\cdot 6 + 6\cdot 2 + 8\cdot 2\cdot 2\,\big] \,=\, \frac{168}{24} \,=\, 7.$$

3) $\#Col(\leqslant 2, *) = u_0 + u_1 + u_2$, очевидно $u_0 = u_1 = 1$.

$$u_2 \,=\, \frac{1}{24}\big[\dots + 28y^2 + 9(\dots + 4y^2 \dots) + 8(\dots + y^2 + \dots)\big] \,=$$

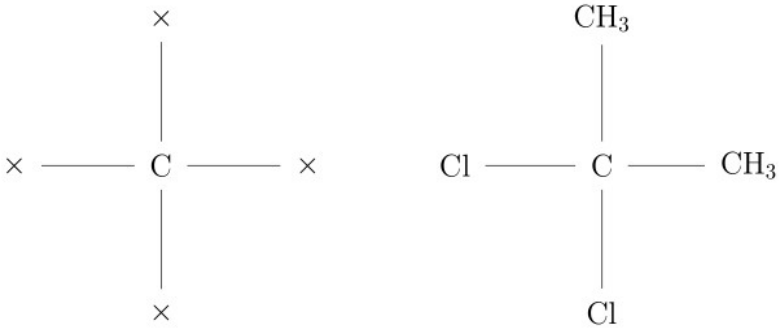
$$= \frac{28+36+8}{24} \,=\, 3.$$

$$\#Col(\leqslant 2, *) \,=\, 1+1+3 \,=\, 5.$$

Задача 4.9 (о числе молекул). Рассмотрим молекулы 4-валентного углерода C: где на на месте $\times$ могут находится CH_3 (метил), C_2H_5 (этил), H (водород) или Cl (хлор). Например — дихлорбутан.

Найти

1) общее число M всех молекул;
2) число молекул с $H = 0, 1, 2, 3, 4$ атомами водорода.



Решение. Какая группа действует и на каком множестве?
T на множестве вершин тетраэдра.
Находим цикловой индекс:

$g \in T$	$Type(g)$	$w(g)$	#
e	$\langle 4,0,0,0 \rangle$	x_1^4	1
$t,\ t^2$	$\langle 1,0,1,0 \rangle$	x_1x_3	$4 \cdot 2 = 8$
f	$\langle 0,2,0,0 \rangle$	x_2^2	3

$$Z(T \underset{\alpha}{:} V) = \frac{1}{12}\left[\, x_1^4 + 8x_1x_3 + 3x_2^2 \,\right]$$

1. Всего M молекул (4 радикала, $x_1 = \ldots = x_4 = 4$):

$$M = Z(x_1, \ldots, x_4) = \frac{4^4 + 8 \cdot 4 \cdot 4 + 3 \cdot 4^2}{3 \cdot 4} = 36.$$

2. Веса: $y_1 = \mathrm{H}$, $y_2 = y_3 = y_4 = 1$.
Подстановка в P: $x_k = \mathrm{H}^k + 3$, $k = \overline{1,4}$.

$$\begin{aligned} Z(H) &= \\ &= \frac{1}{12}\left[(\mathrm{H}+3)^4 + 8\,(\mathrm{H}+3)\left(\mathrm{H}^3+3\right) + 3\left(\mathrm{H}^2+3\right)^2 \right] = \\ &= \frac{1}{12}\left[\left(\mathrm{H}^4 + 4\cdot\mathrm{H}^3\cdot 3 + 6\cdot\mathrm{H}^2\cdot 9 + 4\cdot\mathrm{H}\cdot 27 + 81\right) + \right. \\ &\quad \left. +8\left(\mathrm{H}^4 + 3\mathrm{H}^3 + 3\mathrm{H} + 9\right) + 3\left(\mathrm{H}^4 + 6\mathrm{H}^2 + 9\right) \right] = \\ &= 1\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 6\cdot\mathrm{H}^2 + 11\cdot\mathrm{H} + 15. \end{aligned}$$

Итого имеется молекул с числом атома водорода: с четырьмя — 1 шт., с тремя — 3 шт., с двумя — 6 шт., с одним — 11 шт., без атомов водорода — 15 шт., всего — $1 + 3 + 6 + 11 + 15 = 36$.

Глава 5

Алгебраические основы криптографии

5.1 Основные понятия

Термины. Для многих криптологических терминов имеются различные определения разной степени точности. Нам будут достаточны нижеприведённые.

Криптография (cryptography, др.-греч. *тайнопись*) — наука о способах преобразования (зашифрования) информации с целью её защиты от незаконных пользователей, обеспечения целостности и реализации методов проверки подлинности.

Таким образом, если помехоустойчивое кодирование защищает информацию от естественных, природных воздействий, то криптографические методы призваны защитить информацию от осмысленных воздействий злоумышленника.

Открытый текст (plaintext) — сообщение, подлежащее зашифрованию.

Будем считать, что это двоичное слово x длины n, то есть $x \in \{0,1\}^n$.

Например, тексты на английском языке обычно представляют, используя *стандартную 27-*

значную кодировку

$$a = 01,\ b = 02,\ \ldots,\ z = 26,\ \text{пробел} = 00.$$

Шифртекст (ciphertext), или *криптограмма* — результат зашифрования открытого текста. Так же считаем, что шифртекст есть двоичное слово.

Шифр (cipher) — параметрическое семейство обратимых отображений множества последовательностей открытых текстов во множество последовательностей шифртекстов.

Ключ (key) или *криптопеременная* — параметр (обычно составной), определяющий выбор конкретного отображения из входящих в шифр.

Зашифрование (encryption) — процесс преобразования открытого текста в соответствующую криптограмму с помощью шифра и ключа к нему.

Расшифрование (decryption) — процесс, обратный к зашифрованию, осуществляемый при известном значении ключа.

Дешифрование (decryption) — процесс раскрытия криптограммы (злоумышленником или *криптоаналитиком*) без знания секретного ключа и обычно сводящийся к его нахождению.

Определения шифра и его ключа соответствуют принятому в современной криптографии правилу стойкости О. Керкгоффса[1)], согласно которому *в секрете держится только ключ, а сам алгоритм шифрования открыт.*

[1)] *Огюст Керкгоффс* (Auguste Kerckhoffs, 1835–1903) — нидерландский

Таким образом, *надёжность зашифрования определяется исключительно значением его ключа*, известному только легальным пользователям. Алгоритм шифрования тщательно разрабатывается и меняется в редких случаях. Ключ же при необходимости легко сменяется: защищённость системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить.

Секретность ключа шифра должна быть достаточна, чтобы сохранить стойкость к попыткам взлома. В современных криптосистемах ключ задается двоичным числом длиной не менее 128 и до 4096 бит.

Шифры подразделяются на:

блочные — сообщение разбивается на блоки фиксированной длины, которые при данном значении ключа зашифровываются независимо друг от друга, т. е. содержимое каждого блока никак не влияет на результат зашифрования других блоков (обычно они имеют длину 64 или 128 бит)[2)];

поточные — сообщение шифруется последовательно посимвольно (символом может быть как бит, так и некоторая совокупность битов), и каждый символ шифруется в зависимости не только от используемого ключа, но и от его расположения потоке открытого текста.

криптограф, лингвист, историк, математик, автор фундаментального труда «Военная криптография» (1883), в котором сформулированы общие требования к криптосистемам.

[2)] не путайте: коды — *блоковые*, а шифры — *блочные*

Типы шифрсистем. Сложность алгоритмов. Зашифрование открытого текста и его расшифровывание проводят с использованием, как правило, различных ключей, которые будем обозначать k_e и k_d соответственно. Множество их возможных значений называют *пространством ключей*.

Если $k_d = k_e$, или один ключ может быть легко получен из другого, то соответствующая криптосистема называется *симметрической*, а в противном случае — *асимметрической*.

Понятно, что при использовании симметрической системы оба ключа должны быть известны только легальным абонентам. Поэтому такие системы называют ещё *криптосистемами с секретным ключом* или *одноключевыми*. Они используются при передаче сообщений по защищённым линиям связи (правительственной, служебным или общедоступным), а также для проводки банковских платежей, денежных переводов и онлайн-оплаты.

Примером системы с совпадающими ключами является криптосистема *гаммирования* (или *шифр Вернама*), когда криптограмму $\widetilde{\beta}$ получают из открытого текста $\widetilde{\alpha}$ путём сложения его по mod 2 с некоторым случайным двоичным словом-ключём $\widetilde{\gamma}$ той же длины ($\widetilde{\beta} = \widetilde{\alpha}+\widetilde{\gamma}$), а вторичное такое сложение её расшифровывает. В этом случае, очевидно, криптограмма может оказаться результатом зашифрования любого открытого текста при подходящем выборе ключа $\widetilde{\gamma}$. Такая система обладает *абсолютной криптостойкостью* (стойкость к дешифрованию, обеспеченная фундаментальными законами природы, а не имеющимися технологическими возможностями), если ключ не содержит длинных повторяющихся последовательностей бит и

используется однократно[3)].

Утверждённая в России с 1.06.2019 в качестве стандарта криптосистема «Кузнечик» реализует симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной секретного ключа 256 бит.

Объявленная в США с 26.05.2002 стандартом криптосистема AES (Advanced Encryption Standard, пришедшая на смену системе DES, Data Encryption Standard), реализует симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 128/192/256 бит.

Основная проблема симметрической криптографии — обеспечение секретности при передаче ключей.

При асимметрическом шифровании *ключ расшифрования* k_d остаётся *секретным* (private, cipher key), а *ключ зашифрования* k_e делается *общедоступным* (public key). Поэтому асимметрические системы называют ещё *криптосистемами с открытым ключом* или *двуключевыми*.

Асимметричное шифрование применяют, когда, например, при выработке секретного ключа для симметрической криптосистемы по открытому каналу связи и создания цифровой подписи или сертификата. Определения приведённых понятий и способы реализации асимметричного шифрования будут рассмотрены далее.

Оперативно расшифровать криптограмму может

[3)] Использование данной и аналогичных криптосистем с *одноразовым шифрблокнотом* (содержащим наборы ключей $\widetilde{\gamma}_1, \widetilde{\gamma}_2, \ldots$) требует выработки длинных последовательностей ключей нужного качества, решения проблем их хранения, передачи и уничтожения после использования. На каждом из этих этапов жизненного цикла ключей имеется угроза их раскрытия. Все это делает данные системы непрактичными, дорогостоящими, и они применяются в исключительных случаях.

только абонент, которому известен секретный ключ. Криптосистема проектируется так, чтобы секретный ключ нельзя было определить (вычислить, подобрать) за приемлемое время.

Последнее означает, что неизвестен полиномиальный алгоритм решения соответствующей задачи. Напомним, что *полиномиальным* называется алгоритм, время работы которого в зависимости от длины ℓ входного слова ограничено сверху величиной ℓ^c для некоторой константы c, не зависящей от ℓ.

Всегда существует *экспоненциальный алгоритм* подбора ключа k_d, заключающийся в полном переборе (brute force) всех возможных секретных ключей. *Экспоненциальные* алгоритмы имеют оценку времени исполнения $exp(\ell)$.

Шифр считают *криптостойким*, если не существует метода его дешифрования, «взлома», существенно более быстрого, чем полный перебор элементов пространства ключей.

Обычно существует и *субэкспоненциальный* алгоритм подбора ключа k_d. Время работы субэкспоненциального алгоритма асимптотически меньше любой экспоненты, но больше любого полинома от ℓ.

На практике применяют гибридные криптографические системы, когда шифрование/расшифрование передаваемых данных проводится быстрыми симметричными алгоритмами, а для обмена ключами используют асимметричную криптографию (алгоритмы которой работают в тысячи раз медленнее).

Алгоритм быстрого возведения в степень. При возведении некоторого числа в натуральную степень x

используют её двоичную запись:

$$x = x_k 2^k + x_{k-1} 2^{k-1} + \ldots + x_0 2^0,\ x_i \in \{0,1\},\ i = \overline{0,k}.$$

Пусть, например, требуется вычислить a^{53}. Поскольку $53 = 2^5 + 2^4 + 2^2 + 1$, то

$$a^{53} = a^{2^5} \cdot a^{2^4} \cdot a^{2^2} \cdot a^{2^0}.$$

Нахождение первого сомножителя требует пяти умножений: $a^{2^5} = ((((a^2)^2)^2)^2)^2$. В процессе его вычисления запоминаются значения a, второго и третьего сомножителей. Их перемножение требует ещё трёх умножений. Таким образом, для вычисления a^{53} требуется только $5 + 3 = 8$, а не 52-х умножений.

При вычислении степени некоторого элемента по модулю n (*modular exponentiation*) возводят в квадрат не само число, а его остаток от деления на n, что существенно проще. Для этого вычисляют вектор

$$x = [\ x_0\ \ldots\ x_k\ ]_2$$

двоичного представления x и тогда

$$a^x = a_0^{x_0} \cdot a_1^{x_1} \cdot \ldots \cdot a_k^{x_k} \pmod{n},$$

где $a_0 = a$ и $a_{i+1} \equiv_n a_i^2$, $i = 0, \ldots, k-1$.

Ясно, что при возведении в степень x по данному алгоритму потребуется $O(\log_2 x)$ операций.

Пример 5.1. Вычислим $3^{11} \pmod 5$.

1. Находим вектор двоичного представления показателя степени: $11 = 2^0 + 2^1 + 2^3 \leftrightarrow [\ 1\ 1\ 0\ 1\ ]$. Поэтому $3^{11} \equiv_5 a_0^1 \cdot a_1^1 \cdot a_2^0 \cdot a_3^1$.

2. Находим $a_i,\ i = 0, 1, 2, 3$:

$$a_0 = 3 \equiv_5 3, \qquad a_1 = 3^2 = 9 \equiv_5 4,$$
$$a_2 = 4^2 = 16 \equiv_5 1, \qquad a_3 = 1^2 \equiv_5 1.$$

3. Окончательно $3^{11} = 3 \cdot 4 = 12 \equiv_5 2$.

Теоремы Ферма и Эйлера

Теорема 5.2 (Ферма, малая). *Если целое a не делится на простое число p, то* $a^{p-1} \equiv_p 1$.

Утверждение теоремы справедливо как следствие 3 теоремы 2.26 («Любой элемент поля $GF(q)$ удовлетворяет равенству $x^q - x = 0$», см. с. 61).

Обобщением малой теоремы Ферма является

Теорема 5.3 (*Эйлер*). *Если $n > 1$ и $(a, n) = 1$, то*

$$a^{\varphi(n)} \equiv_n 1. \tag{5.1}$$

Задача о рюкзаке: выбрать такие элементы вектор-строки $\boldsymbol{a} = [\ a_1\ \ldots\ a_n\ ]$ различных натуральных чисел, чтобы их сумма равнялась данному z («размер рюкзака»)[4].

Например, в векторе

$$\boldsymbol{a} = [\ 43\ \underline{129}\ 215\ \underline{473}\ \underline{903}\ 302\ \underline{561}\ \underline{1165}\ 697\ 1523\ ],$$

подчёркнуты элементы, дающие в сумме $z = 3231$, то есть решением задачи для данного z будет вектор-столбец $\boldsymbol{x} = [\ 0\,1\,0\,1\,1\,0\,1\,1\,0\,0\ ]^T$ позиций выбранных чисел: $\boldsymbol{a} \times \boldsymbol{x} = z$. Полиномиальные алгоритмы решения задачи о рюкзаке неизвестны.

[4] Предполагается, что решение существует и единственно (англ. knapsack problem); другие названия задачи — *об укладке ранца, проблема подмножества суммы.*

Односторонняя функция — центральное понятие криптографии.

Определение 5.4. *Односторонней* (или *однонаправленной*, one-way function) называется обратимая функция $f : X \to Y$, обладающая свойствами:

1) существует полиномиальный алгоритм вычисления значений $f(x)$;
2) не существует полиномиального алгоритма обращения функции f (то есть нахождения x по значению $y = f(x)$).

Иными словами, инъективную функцию $f(x)$ называют однонаправленной, если для всех $x \in X$ относительно легко вычисляется $y = f(x)$, но почти для всех $y \in Y$, нахождение любого $x \in X$, для которого $y = f(x)$, *вычислительно не осуществимо*.

До сих пор не доказано, что однонаправленные функции вообще существуют, и проблема их существования эквивалентна проблеме $P \stackrel{?}{=} NP$. Однако было предложено много функций, претендующие на односторонность. Они используют сложность решения задач теории чисел или комбинаторного анализа. Приведем некоторые из таких задач.

- Найти примарное разложение (большого) натурального числа — задача факторизации FACT.
- Для известных a, b, n найти такое x, что $a^x = b \pmod n$ — задача нахождения *дискретного логарифма*, DLP (Discrete Logarithm Problem[5]).

[5] не путать с технологиями предотвращения утечек конфиденциальной информации Data Leak Prevention

- Решить задачу о рюкзаке.
- Декодировать исправляющий ошибки линейный код общего вида.

Односторонняя функция с секретом (с лазейкой; trapdoor one-way function) — функция $f_k : X \to Y$ зависящая от параметра k, называемым *секретным ключом* или *лазейкой* и такая, что

1) вычисление значения $f_k(x)$ относительно несложно, и при этом не требуется знание параметра k;
2) вычисление значения $f_k^{-1}(y)$ для всех $y \in Y$ при известном k относительно несложно;
3) нахождение $f_k^{-1}(y)$ для почти всех k и $y \in Y$ вычислительно неосуществимо без знания k.

Заметим, что в приведённом общепринятом названии прилагательное “односторонняя” просто лишнее: если функция не является односторонней, то о какой лазейке вообще идёт речь?

Один из примеров, претендующих на то, чтобы являться односторонней функцией с лазейкой — функция $f(x) = y = x^m \pmod n$ *вычисления корня* m*-й степени по* mod n: нахождение $y = f(x)$ производится быстрым возведением в степень, а эффективный алгоритм обратного преобразования $f^{-1}(y)$ требует знания примарного разложения n. Эта информация может считаться лазейкой.

5.2 Криптографические протоколы

Криптографический протокол (cryptographic protocol) — набор правил, регламентирующих использование в информационных процессах криптографических преобразований и алгоритмов.

Электронная цифровая подпись (ЭЦП) — позволяет проверить авторство документа и отсутствие в нём искажений.

Для организации ЭЦП используют *хэш-функцию* H, которая каждому документу D сопоставляет битовую строку $H(D) = h$ установленной (небольшой) длины. Понятно, что хэш-функции осуществляют необратимые преобразование информации и выступает как компактный представитель (паспорт) документа.

Для того, чтобы снабдить документ электронной цифровой подписью —

1. Автор документа D вычисляет значение h его хэш-функции.
2. Используя свой секретный ключ k к односторонней функции с секретом f_k, автор вычисляет $x = f_k^{-1}(h)$ и посылает адресатам документ D, снабжённый хэшем h и значением x.
3. Проверку авторства документа a легко проводит любой адресат, вычисляя без знания k значение $f_k(x)$ и сравнивая результат с h.

Схема протокола:

$$D \to h, x \to (D, h, x) \overset{\text{пересылка адресатам}}{\longrightarrow} f(x) \overset{?}{=} h.$$

Определение 5.5. Хэш-функция H является *криптографически стойкой*, если она удовлетворяет трем требованиям:

1) *необратимость* (стойкость к восстановлению прообраза) — для заданного значения хэш-функции h должно быть вычислительно невозможно найти блок данных X, для которого $H(X) = h$.

2) *стойкость к коллизиям I-го рода* (восстановлению вторых прообразов) — для заданного сообщения M должно быть вычислительно невозможно подобрать другое сообщение N, для которого $H(N) = H(M)$.

3) *стойкость к коллизиям II-го рода* — должно быть вычислительно невозможно подобрать пару сообщений (M, M'), имеющих одинаковое значение хэш-функции.

Для хэширования часто используют кодирование циклическими кодами. Хотя такая хэш-функция не является криптографически стойкой, однако она широко применяется в различных приложениях для защиты от случайных ненамеренных изменений при передаче данных.

Сообщение разбивается на блоки по n битов (часто $n = 128$). Хэшем является циклический код сообщения. Кодирование задаётся порождающим неприводимом многочленом $g(x) \in \mathbb{F}_2[x]$, $\deg g(x) = m < n$.

Ясно, что снабдить ЭЦП какой-либо документ без знания секрета k трудновыполнимо.

Выработка общего секретного ключа по открытому каналу связи. Для использования любой шифрсистмы легальным пользователям необходимо иметь общий секретный ключ, который, кроме того, требуется периодически менять. Встаёт задача выработки такого ключа, при условии использования открытого канала связи. Покажем, как это можно сде-

лать на примере протокола DH Диффи – Хеллмана[6)].

Итак, пусть два лица с традиционными именами Алиса (A) и Боб (B) обмениваются сообщениями по открытому каналу. Для выработки общего секретного ключа они выбирают простое число p, а в поле Галуа $GF(p)$ — некоторый элемент α. Оба эти значения не являются секретом.

Затем A и B независимо друг от друга выбирают по одному случайному числу из $GF(p)$, которые уже держат в секрете; обозначим их x и y соответственно. Далее каждый из абонентов вычисляет по $\bmod p$ значения:

$$A:\ X = \alpha^x, \qquad B:\ Y = \alpha^y, \qquad (*)$$

которыми они обмениваются по открытому каналу.

Абонент A, получив Y, вычисляет ключ:

$$K = Y^x = \alpha^{yx} \pmod p,$$

и аналогично поступает абонент B, получив X:

$$K = X^y = \alpha^{xy} \pmod p.$$

Тем самым у Алисы и Боба появляется общий секретный ключ $K \in GF(p)$, который в дальнейшем используется в алгоритмах симметричного шифрования.

Пассивный злоумышленник, перехватывающий, но не изменяющий сообщений, традиционно Ева (E,

[6)] Предложен в 1976 г. сотрудниками MIT *Бейли Уитфилдом Диффи* (Bailey Whitfield 'Whit' Diffie, 1944), *Мартином Эдвардом Хеллманом* (Martin Edward Hellman, 1945) и независимо от них *Ральфом Чарльзом Мерклем* (Ralph Charles Merkle, 1952). Этот протокол положил начало использованию криптографии с открытым ключом.

от eavesdropper, подслушивающий) не может узнать ключ K: его нахождение связано с решением одного из уравнений $(*)$, а это вычислительно трудная задача дискретного логарифмирования.

Заметим, что DLP принадлежит классу NP, но её NP-полнота не доказана[7)].

Протокол DH устойчив к пассивной атаке, но беззащитен от активного вмешательства типа «*человек посередине*» (man-in-the-middle attack): при обмене сообщениями ни A, ни B не могут достоверно определить, кем является их контактёр. Действительно, если к каналу связи имеет доступ *активный злоумышленник*, традиционно Меллори (M, от malicious, злонамеренный), который может перехватывать сообщения, изменять или полностью подменять их, то, выработав два ключа — общий с A и общий с B, он может представляться Алисе Бобом, а Бобу — Алисой[8)].

Таким образом, протокол DH позволяет передавать секретный ключ по *частично защищенному* (от прослушивания, но не от подмены) каналу связи.

Обмен шифртекстами по открытому каналу связи. Приведём пример использования односторонней функции с лазейкой при решении задачи о рюкзаке, задаваемую вектор-строкой $\boldsymbol{a}$.

Пусть открытый текст состоит из двоичных векторов $\boldsymbol{x}^1$, …, $\boldsymbol{x}^n$. Умножая $\boldsymbol{a}$ на эти векторы-столбцы, получим шифртекст $\boldsymbol{y} = [\ y_1\ \ldots\ y_n\ ]$. Таким образом, шифрование осуществляется элементарно.

[7)] С помощью квантового *алгоритма Шора* дискретный логарифм можно вычислить за полиномиальное время.

[8)] Вспоминаем «Сказку о царе Салтане» *А. С. Пушкина*: «… И в суму его пустую // Суют грамоту другую.».

Для расшифрования полученного сообщения потребуется решать задачу о рюкзаке: по значению y_i находить вектор $\boldsymbol{x}^i$ такой, что $\boldsymbol{a} \times \boldsymbol{x}^i = y_i$, $i = \overline{1,n}$, что без знания лазейки трудновыполнимо.

Покажем, в чём здесь состоит лазейка. Рассмотрим *сверхрастущие векторы* $\boldsymbol{a}$, в которых каждый элемент *больше суммы всех предыдущих элементов*. В этом случае задача решается очень просто.

Действительно, пусть, например,

$$\boldsymbol{a} = [\ \underline{25}\ 27\ \underline{56}\ 112\ 231\ \underline{452}\ \underline{916}\ 1803\ ] \quad \text{и} \quad z = 1449.$$

Поскольку $z < 1803$, то последний элемент данного вектора не входит в решение. Далее, поскольку $z > 916$, то 916 обязательно входит в решение, так как сумма всех предыдущих элементов a меньше 916. После этого вычисляем $z - 916 = 833$, и последовательно рассуждая аналогично, получаем код позиций выбираемых элементов: [1 0 1 0 0 1 1 0].

Преобразуем сверхрастущий вектор $\boldsymbol{a}$ в некоторый вектор $\boldsymbol{b}$. Для этого выберем *модуль* m, больший суммы всех элементов $\boldsymbol{a}$, и возьмем некоторое u, взаимно простое с m (что гарантирует существование элемента $v = u^{-1} \pmod m$).

Вектор $\boldsymbol{b}$ будем вычислять по правилу

$$\boldsymbol{b} = u \cdot \boldsymbol{a} \pmod m.$$

Он уже не является сверхрастущим, и может быть опубликован в качестве открытого ключа, а лазейкой будут выбранные значения m и u.

Пример 5.6. Рассмотрим сверхрастущий вектор $\boldsymbol{a} = [\ 1\ 2\ 4\ 8\ 16\ ]$ с суммой элементов 31.

Пусть передаваемые сообщения представляют собой 5-разрядные двоичные коды

$$\boldsymbol{x}^1 = [\,1\;0\;1\;1\;0\,]^T,\ \boldsymbol{x}^2 = [\,0\;1\;1\;0\;1\,]^T,\ \boldsymbol{x}^3 = [\,1\;0\;0\;0\;1\,]^T,$$

образующие матрицу $X = [\ \boldsymbol{x}^1\ \boldsymbol{x}^2\ \boldsymbol{x}^3\ ]$.

Для преобразования вектора $\boldsymbol{a}$ в вектор $\boldsymbol{b}$ выберем $m = 37 > 31$ и взаимно простое с ним значение $u = 40$. Тогда открытым ключом будет вектор

$$\boldsymbol{b} = [\ 3\ 6\ 12\ 24\ 11\ ].$$

Умножив $\boldsymbol{b}$ на матрицу X, получаем шифртекст:

$$\boldsymbol{b} \times X = [\ 3\ \ 6\ \ 12\ \ 24\ \ 11\ ] \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = [\ 39\ \ 29\ \ 14\ ] = \boldsymbol{y}.$$

Легальный получатель сообщения:

1) зная лазейку $(m, u) = (37,\ 40)$, находит элемент v, обратный к u по mod m: $u \cdot v \equiv_m 1$; в нашем случае $v = 25$;
2) восстанавливает вектор $\boldsymbol{a} \equiv_m v \cdot \boldsymbol{b}$ —
$$25 \cdot [\ 3\ 6\ 12\ 24\ 11\ ] \equiv_{37} [\ 1\ 2\ 4\ 8\ 16\ ] = \boldsymbol{a};$$
3) находит вектор $\boldsymbol{z} \equiv_m v \cdot \boldsymbol{y} = [\ z_1\ z_2\ z_3\ ]$ —
$$\boldsymbol{z} = 25 \cdot [\ 39\ 29\ 14\ ] \equiv_{37} [\ 13\ 22\ 17\ ];$$
4) легко решает три задачи о рюкзаке со сверхрастущим $\boldsymbol{a}$ и $z_1 = 13$, $z_2 = 22$, $z_3 = 17$, определяя передаваемые сообщения $\boldsymbol{x}^1$, $\boldsymbol{x}^2$, $\boldsymbol{x}^3$.

5.3 Система шифрования RSA

RSA — исторически первая асимметрическая криптосистема. В ней открытым ключом является пара (n, e) значений *модуля* n и *экспоненты* e.

Зашифрование открытого текста x в системе RSA производится преобразованием

$$y = x^e \pmod{n}. \tag{5.2}$$

Для расшифрования криптограммы y нужно решить сравнение (5.2) относительно x.

Искомое решение может быть представлено в виде

$$x = y^d \pmod{n}, \tag{5.3}$$

которое будет единственным, когда модуль n свободен от квадратов, а значения экспоненты e и $\varphi(n)$ взаимно просты. Пара $(\varphi(n), d)$ является секретным ключом криптосистемы RSA.

Функция $f_e(x) = x^e$ легко вычисляется с помощью алгоритма быстрого возведения в степень, также как и при известном d — обратная к ней функция $f_d(y) = y^d$.

Покажем, как можно было бы найти секретный ключ расшифрования d. Ясно, что он должен удовлетворять условию

$$x^{e \cdot d} \equiv_n x.$$

Поскольку по теореме 5.3 Эйлера имеем

$$x^{\varphi(n)} \equiv_n 1, \quad \text{то и} \quad x^{k \cdot \varphi(n)} \equiv_n 1$$

для любого целого k. Отсюда

$$x^{1+k \cdot \varphi(n)} = x = x^{e \cdot d} \pmod{n},$$

и заключаем, что для d должно выполняться условие

$$d \cdot e = 1 \pmod{\varphi(n)}. \tag{5.4}$$

Решить это сравнение можно было бы, например, с помощью обобщённого алгоритма Евклида 2.3 со с. 48. Но для этого надо знать $\varphi(n)$. В свою очередь, $\varphi(n)$ легко вычислить, найдя факторизацию несекретного модуля n. А вот эта задача чрезвычайно трудоёмка.

Таким образом, *схема шифрования RSA основана на сложности задачи FACT*. Также как и DLP, эта задача принадлежит классу NP, но её NP-полнота не доказана.

Шифрсистема RSA опубликована в 1978 г., и её название есть аббревиатура от фамилий авторов из MTI *Рональда Линна Ривéста* (Ronald Linn Rivest, 1947), *Ади Шамира* (Adi Shamir, 1952) и *Леонарда Макса Áдлемана* (Leonard M. Adleman, 1945).

Однако согласно рассекреченным британским правительством в 1997 г. сведениям, идея основных принципов криптографии с открытым ключём принадлежит сотруднику Главного управления связи Великобритании (GCHQ, г. Челтнем) *Джеймсу Х. Эллису*, который высказал её в 1970 г., но не смог найти для неё практической реализации, поскольку для выполнения целочисленных операций над данными огромной длины тогда требовались чрезвычайно дорогие вычислительные средства.

Первооткрывателем алгоритма RSA в 1973 г. стал *Клиффорд Кокс*, а впервые реализовал то, что известно как протокол Диффи–Хеллмана — в следующем году *Малколъм Дж. Уильямсон* (все из GCHQ).

Алгоритм RSA используется в большом числе криптографических приложений.

Конкретно, авторы этой схемы предложили выбирать число n в виде произведения двух больших про-

стых разных множителей p и q. Тогда

$$\varphi(n) \;=\; \varphi(pq) \;=\; (p-1)(q-1). \qquad (5.5)$$

Условием на выбор экспоненты e будет её взаимная простота с $p-1$ и $q-1$, гарантирующая существование $e^{-1} = d \pmod{\varphi(n)}$. Отметим, что число, представимое в виде произведения двух простых чисел, называют *полупростым*.

Утверждение 5.7. *Пусть известное значение n представимо в виде произведения простых чисел p и q: $n = pq$. Тогда знание p, q равносильно знанию $\varphi(n)$.*

Доказательство. Зная p и q, легко находят

$$\varphi(n) = (p-1)(q-1).$$

Обратно, зная $\varphi(n) = pq - (p+q) + 1$, имеем

$$\begin{cases} p+q \;=\; n+1-\varphi(n), \\ pq \;=\; n \quad \text{(это значение открыто)}. \end{cases}$$

Теперь p и q могут быть получены как корни квадратного уравнения $z^2 + (\varphi(n) - n - 1)\, z + n = 0$. □

Итак, шифрованная переписка с помощью системы RSA происходит следующим образом.

1. Организатор системы выбирает два разных достаточно больших простых числа p и q, и находит произведение $pq = n$.

2. Затем он выбирает экспоненту $e < n$, взаимно простую с числами $p-1$ и $q-1$, перемножая их, получает $\varphi(n)$, и по (5.4) — определяет d.

3. Числа n и e публикуются, числа d и $\varphi(n)$ остаются секретными.

4. Теперь любой абонент может отправлять зашифрованные с помощью (5.2) сообщения организатору этой системы, который легко расшифровывает их с помощью (5.3).

Сделаем некоторые замечания относительно использования криптосистемы RSA.

- Большие простые p и q должны быть такими, чтобы значение $|p-q|$ было также не мало, иначе их несложно подобрать в окрестности $\sqrt{n}$.
- В настоящее время Лаборатория RSA рекомендует для обычных задач значения n размером не менее 1024 бита, а для особо важных задач — 2048 бит.
- Для упрощения зашифрования экспоненту e выбирают с малым числом единиц; при этом часто пользуются *простыми числами Ферма* (вида $2^{2^k}+1$, например, 65537), представление которых содержит лишь две единицы.

Пример 5.8. Пусть $p = 11$, $q = 13$, тогда $n = pq = 143$.

Выберем значение $e = 13$, оно простое, и заведомо взаимно просто с $p-1 = 10$ и $q-1 = 12$. Вычисляем $\varphi(143) = 10 \cdot 12 = 120$.

Возьмём фрагмент текста, соответствующий, например, числу $x = 42$, и зашифруем его:

$$y \;=\; 42^{13} \;=\; 1\,265\,437\,718\,438\,866\,624\,512 \;\equiv_{143}\; 3.$$

Для получения ключа расшифрования легальный пользователь зная $\varphi(n) = 120$ решает сравнение

$$d \cdot 13 \;=\; 1 \pmod{120}.$$

Применим для этого алгоритм GE-InvZm:

1	120	0	
2	13	1	$q = 9 \quad (\ 117\ 9\ )$
3	3	-9	$q = 4 \quad (\ 12\ \ -36\ )$
4	1	**37**	$q = 3$
5	0		

и получим $d = 37$ (действительно, $37 \cdot 13 = 481 = 4 \cdot 120 + 1$).

Теперь легальный получатель легко расшифровывает полученную криптограмму $y = 3$:

$$3^{37} \ = \ 450\,283\,905\,890\,997\,363 \ \equiv_{143} \ 42 \ = \ x.$$

Перескажем близко к тексту отрывок из [16].

Для иллюстрации своего метода Р. Ривест, А. Шамир и Л. Адлеман в 1977 г. зашифровали предложенным ими способом некоторую английскую фразу. Сначала она стандартным образом была представлена числом в 27-ричной системе исчисления, записана в виде целого x, а затем зашифрована с помощью отображения (5.2) при модуле n, содержащим 129 десятичных знаков (число RSA-129) и экспоненте $e = 9007$. Эти два числа были опубликованы, причем дополнительно сообщалось, что $n = pq$, где p и q — простые числа, записываемые соответственно 64 и 65-ю десятичными знаками.

Первому, кто дешифрует криптограмму y, длиной 123 знака была обещана символическая награда в \$100.

Предполагалось, что для расшифровки понадобится порядка 40 квадрильонов лет. Однако в 1994 г., то есть всего через 17 лет, задача была решена: были определены числа p и q, а в результате дешифровки получилась фраза «*The magic words are squeamish ossifrage*» (*Волшебные слова — привередливая скопа*[9)]; по-видимому, нарочито бессмысленная фраза).

Выполнение вычислений потребовало огромных по тем временам ресурсов: в работе, возглавлявшейся четырьмя авторами

[9)] скопа — крупная хищная птица отряда ястребообразных

проекта дешифровки и продолжавшейся после предварительной теоретической подготовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединенных в интернете.

То, что за 17 лет никто не смог дешифровать указанную криптограмму считалось подтверждением стойкости системы RSA-129. Однако в последние десятилетия в области поиска эффективных алгоритмов факторизации был достигнут большой прогресс, и в 2015 г. для дешифрования этого сообщения при использовании облачных вычислений потребовалось около одного дня.

С 2013 г. браузеры Mozilla перестали поддерживать сертификаты удостоверяющих центров с ключами RSA меньше 2048 бит.

При использовании схемы шифрования RSA используются довольно большие натуральные числа, порядка 250–300 десятичных разрядов.

5.4 Факторизация натуральных чисел

Тесты на простоту числа. Элементарный *метод пробных делений* проверки простоты натурального N состоит в проверке делимости N на все простые числа от 2 до $\lfloor \sqrt{N} \rfloor$. Однако для чисел порядка 10^{40} и более этот метод уже неприменим.

Несложной является проверка на основе малой теоремы Ферма.

Тест Ферма проверки, является число N составным или вероятно простым

Из интервала $[\ 2,\ N-1\ ]$ выбирается случайное число

a, подчиняющееся равномерному дискретному распределению; символически $a \xleftarrow{\$} [\ 2,\ N-1\ ]$.

Если окажется, что $a \mid N$, или же

$$a^{N-1} \not\equiv_N 1, \tag{5.6}$$

то N, очевидно, составное. Иначе вопрос остаётся открытым, и N испытывается при другом значении a.

С одной стороны, проверка (5.6) не требует больших вычислений: имеется алгоритм быстрого возведения в степень. С другой — имеется бесконечно много составных чисел, которые проходят данную проверку при всех a, взаимно простых с N. Эти числа называют *псевдопростыми* или *числами Кармайкла*[10]; $561 = 3 \cdot 11 \cdot 17$ — наименьшее такое число. Однако по мере возрастания чи́сла Кармайкла становятся всё более редкими.

Отметим, что для составления *таблиц простых чисел* наилучшим является известный метод решета Эратосфена, несмотря на то, что он требует большого объёма памяти.

На сегодняшний день разработаны быстрые и эффективные детерминированные алгоритмы определения простоты числа. Все они основаны на обобщениях теоремы Ферма.

Генерация ключей. Один из возможных способов получения ключа шифрования — использовать *генератор псевдослучайных чисел (ГПСЧ)*. Хорошие по статистическим свойствам последовательности псевдослучайных чисел получаются по формуле *линейного конгруэнтного метода* (linear congruential):

[10] *Роберт Дэниэл Кармайкл* (R. D. Carmichael, 1879–1967) — американский математик.

$$r_{i+1} \equiv_m a \cdot r_i + b, \quad i = 1, 2, \ldots,$$

где a, b, m — некоторые целые взаимно простые числа, от которых и зависит качество такой последовательности. Например, для $a = 8$, $b = 9$, $m = 10$ и $r_1 = 7$ получим последовательность

$$7, 5, 9, 1, 7, 5, 9, 1, \ldots$$

т. е. при использовании данного метода крайне важен удачный выбор параметров.

Очевидно, в любом случае рассматриваемая последовательность будет периодической, но показано, что её период может достигать значения m. Обычно данный генератор используют с параметрами

$$a = 214\,013, \quad b = 2\,531\,011, \quad m = 2^{32},$$

а в качестве r_1 берут текущее время с точностью до тика таймера компьютера.

Ясно, что значение r_1 однозначно определяет значения всех следующих членов последовательности. Например, если каждое r_i есть короткое целое число (16 бит), то различных ключей будет только 2^{16} вне зависимости от длины ключа. Отсюда следует вывод: линейный конгруэнтный метод *не обладает криптографической стойкостью.*

Часто используется *ГПСЧ Фибоначчи с запаздыванием*, который порождает последовательность по правилу

$$r_{i+1} \equiv_m r_{i-k} + r_{i-j} \quad j > k \geqslant 1,$$

где m — чётное число, а $r_0, \ldots, r_{m-1}$ — произвольные целые. Числа k и j называют *запаздыванием.* Конкретно полагают $m \geqslant 55$ и $k = 24$, $j = 54$.

Специалисты считают, что источником истинно случайной последовательности может быть только какой-нибудь физический процесс: радиоактивный распад, тепловое движение атомов или молекул и т. п.[11)] Процесс оцифровывается и после определенной обработки используется в качестве случайной последовательности. Различные методы типа вычисления адреса памяти или номера сектора на диске с извлечением данных оттуда, использование интервалов между нажатиями клавиш пользователем и т. д. раскритикованы как непригодные для применения в криптографии.

Построение больших простых чисел. На сегодняшний день созданы быстрые и эффективные алгоритмы для решения этой задачи. Опишем наиболее простой из них.

Пусть уже имеется простое число S. Для построения существенно большего простого N нужно:

1) выбрать *четное* число $R \xleftarrow{\$} [\, S+1,\, 4S+2 \,]$ и положить $N = SR + 1$;
2) проверить число N на отсутствие малых простых делителей;
3) испытать N на простоту каким-либо не слишком трудоёмким тестом достаточно много раз;
4) если выяснится, что N — составное, то выбрать новое значение R и повторить вычисления.

Если N выдерживает испытания данным алгоритмом, то, скорее всего, N — простое, и тогда следует попы-

[11)] Это согласуется с естественнонаучной точкой зрения, что природа любой случайности — квантовая. «*Каждый, кто рассматривает арифметические методы получения случайных чисел — безусловно заблудшая душа*» (*Дж. фон Нейман*).

таться доказать это с помощью более мощных и трудоёмких тестов.

Для вычислений с большими числами созданы специальные языки программирования, например PARI и UBASIC.

Многим известна

Теорема 5.9 (постулат Бертрана). *Для любого $n \in \mathbb{N}$ интервале $[n, 2n]$ лежит хотя бы одно простое число.*

Но при больших n можно дать значительно лучшую оценку. Самый точный из известных на сегодняшний день результатов о существовании простых чисел — асимптотический:

Теорема 5.10 (Бейкер, Харман, Пинц (2001)). *Для любого достаточно большого n в интервале $[n, n^{21/40}]$ лежит хотя бы одно простое число.*

К настоящему времени созданы эффективные алгоритмы для построения больших простых чисел.

Факторизация натурального числа n — это нахождение его *примарного разложения*

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

где p_i — разные простые числа, а α_i — натуральные, $i = \overline{1, s}$.

Стойкость к взлому многих криптосистем основывается на трудности решения задачи FACT. Факторизация числа значительно сложнее проверки его на простоту: например, распознавание простоты целого числа с 125-ю десятичными цифрами на существующих

компьютерах может быть выполнено за несколько минут, в то время как его факторизация потребует миллионы лет вычислений, то есть вычислительно неосуществима.

Сплиттингом (расщеплением) натурального n называют представление его в виде

$$n = a \cdot b, \;\; a \in [\, 2, \;\lfloor n/2 \rfloor \,],$$

а сомножители a и b — *нетривиальными факторами* числа n.

ρ-алгоритм сплиттинга составного целого n, которое не есть степень простого числа

1. Полагаем $a = 2, \;\; b = 2, \;\; f(x) = x^2 + 1$.
2. Перевычисляем
$$a := f(a), \;\; b := f(f(b)) \pmod{n}.$$
3. Вычисляем $d = \text{НОД}\,(a - b, n)$.
4. Если
   - $d \in [\, 2, \;\; n - 1 \,]$, то d — делитель n;
   - $d = 1$, то переход к шагу 2;
   - $d = n$, то алгоритм заканчивает работу, и вопрос о нетривиальных факторах в n остается открытым.

ρ-алгоритм Полларда[12)] для сплиттинга числа n

[12)] Предложен в 1975 г. британским математиком *Джоном Поллардом* (John M. Pollard, 1941). Название объясняется тем, что алгоритм строит числовую последовательность, элементы которой, начиная с некоторого, образуют цикл, что иллюстрируется расположением чисел в виде греческой буквы ρ.

требует $O\left(n^{1/4}\right)$ модулярных умножений и эффективен при поиске малых делителей.

Пример 5.11. 1. Разложим на нетривиальные сомножители число $n = 163\,829$.

1. $a = b = 2$.
2. $a = 5,\ b = 26$.
3. $a - b = 5 - 26 = -21 \equiv_{163\,829} 163\,808$ и $d = \text{НОД}\,(163\,808, 163\,829) = 23$.
4. Поскольку $d \in [\ 2,\ n-1\ ]$, то $23 \mid 163\,829$.

Дальнейший анализ показывает, что $n/23 = 7\,123 = 17 \cdot 419$.

2. Пусть $n = 455\,459$.

Результаты вычислений по ρ-алгоритму Полларда приведены в таблице

	a	b	d
1	5	26	1
2	26	2 871	1
3	677	179 685	1
4	2 871	155 260	1
5	44 380	416 250	1
6	179 685	43 670	1
7	121 634	164 403	1
8	155 260	247 944	1
9	44 567	68 343	743

Следовательно, 743 и $455\,459/743 = 613$ есть два нетривиальных делителя $n = 455\,459$; заметим, они оказываются простыми числами.

В 1991 г. фирмой RSA Laboratories были опубликованы 54 полупростых числа (их называют RSA-числами) длиной от 100 до 617 десятичных знаков и организован конкурс на их факторизацию. Наименьшее RSA-число было разложено за несколько дней. Большинство чисел до сих пор не разложено и предполагается, что многие из них останутся таковыми ещё довольно долго.

Хотя сам конкурс был официально закрыт ещё в 2007 г., до сих пор энтузиасты пытаются факторизовать ещё не разложенные RSA-числа. Так, отечественными исследователями Н. Л. Замарашкиным, Д. А. Желтковым и С. А. Матвеевым в 2020 г. с использованием суперкомпьютеров «Ломоносов» (МГУ им. М. В. Ломоносова) и «Жорес» (Сколтех) было получено разложение числа RSA-232 (232 десятичных знака, 768 бит).

Наибольшее из RSA-чисел, для которых найдена пара их простых делителей — RSA-250 (829 бит), оно было факторизовано в феврале 2020 г. группой французских исследователей с использованием вычислительных ресурсов Франции и Германии. Объявлен денежный приз в \$100 000 за факторизацию числа RSA-1024 (1024 бита, 309 десятичных знаков). Его успешная факторизация важна: наиболее часто используемая длина ключа как раз составляет 1024 бита.

5.5 Дискретное логарифмирование

DLP и криптосистема Эль-Гамаля. Пусть G — мультипликативная абелева группа порядка n и $a, b \in G$. Задача решения сравнения $a^x \equiv_n b$ называется *задачей (проблемой) дискретного логарифмирования* в группе G. Её решение x, если оно существует, называют *дискретным логарифмом элемента b по основанию a*, символически $\log_a b$.

На сложности DLP базируется ряд асиметричных

шифрсистем с отрытым ключом, в частности рассмотренная ранее система Диффи – Хелмана DH и система Elgamal, разработанная Т. Эльджимали[13)].

Рассмотрим вариант последней, когда G есть мультипликативная группа простого поля $\mathbb{F}_p$, то есть

$$|G| \;=\; n \;=\; p-1.$$

Пусть α — некоторый (часто — порождающий) элемент G. Будем далее использовать изоморфизм групп $\mathbb{F}_p^*$ по умножению и $\mathbb{Z}_{p-1}$ по сложению.

Для организации обмена Алиса и Боб выбирают в группе G каждый соответственно по своему секретному ключу

$$x_A \xleftarrow{\$} [\,2,\; p-2\,], \quad x_B \xleftarrow{\$} [\,2,\; p-2\,]$$

и вычисляют значения

$$d_A \;=\; \alpha^{x_A} \quad \text{и} \quad d_B \;=\; \alpha^{x_B}.$$

Открытыми ключами, которыми обмениваются Алиса и Боб, являются тройки (p, α, d_A) и (p, α, d_B).

Пусть абонент A хочет передать абоненту B сообщение $m \in \mathbb{F}_p^*$. Для этого A выбирает ещё одно случайное число

$$s \xleftarrow{\$} [\,1,\; p-2\,],$$

называемое *сеансовым (раундовым) ключом*[14)], вычисляет по $\bmod p$ пару чисел

[13)] *Та́хер Эльджимали́* (англ. Taher A. Elgamal, 1955) — американский криптограф египетского происхождения; на русском языке утвердилось написание его фамилии Эль-Гамаль.

[14)] Такие ключи генерируются процедурой *расширения ключа* (key expansion), осуществляющей, как правило, перестановки битов секретного ключа.

$$a = \alpha^s \quad \text{и} \quad b = m \cdot (d_B)^s,$$

и передаёт шифртекст (a, b) абоненту B по открытому каналу. Длина криптограммы в схеме Elgamal, ясно, вдвое длиннее исходного сообщения m.

Для расшифрования криптограммы, B вычисляет по $\bmod p$ значение m:

$$m = b \cdot (d_B)^{-s} = b \cdot (\alpha^{x_B})^{-s} = b \cdot (\alpha^s)^{-x_B} = b \cdot a^{p-1-x_B}.$$

Очевидно, криптосистема Elgamal фактически является одним из способов выработки открытых ключей по протоколу DH Диффи – Хеллмана.

Пример 5.12. Алиса передаёт Бобу своё сообщение BUJ, используя шифрсистему Elgamal.

Вычисление ключей. Боб:

1) выбирает простое $p = 2357$ и находит порождающий элемент $\alpha = 2$ мультипликативной группы поля $\mathbb{F}_p$;

2) выбирает свой секретный ключ — случайное число $x_B = 1751 \in [\,2,\, p-2\,]$ и вычисляет

$$d_B = \alpha^{x_B} \equiv_{2\,357} 1\,185;$$

3) передаёт Алисе свой открытый ключ

$$(\,p,\, \alpha,\, d_B\,) = (\,2\,357,\ 2,\ 1\,185\,).$$

Шифрование сообщения. Алиса:

1) получает открытый ключ Боба;

2) представляет свой текст BUJ в виде натурального числа $m \in [\,0,\, p-1\,]$ с помощью 27-ричной системы счисления:

$$m = \underbrace{2}_{B} \cdot 27^2 + \underbrace{21}_{U} \cdot 27^1 + \underbrace{10}_{J} = 2\,035;$$

3) выбирает случайный сеансовый ключ

$$s = 1\,520 \in [\,1,\, p-2\,];$$

4) вычисляет по $\bmod 2\,357$ чи́сла $a = \alpha^s = 1\,430$ и

$$b = m \cdot (d_B)^s \equiv 2035 \cdot 1\,185^{1520} \equiv 697;$$

5) посылает шифртекст $(\,a = 1\,430,\, b = 697\,)$ Бобу.

Расшифрование сообщения. Боб:

1) получает криптограмму от Алисы;

2) вычисляет значение

$$a^{p-1-x_B} = 1\,430^{605} \equiv_{2\,357} 872$$

и получает $m = 872 \cdot 697 \equiv_{2\,357} 2\,035$;

3) представляет m в 27-ричной системе счисления: $m = 2\,035_{10} = [\ 2\ 21\ 10\ ]_{27}$ и получает исходный текст BUJ.

Замечание: на практике значение p выбирают длиной не менее, чем 2048 бит.

Заметим, что сложность решения DLP зависит от конкретной группы G, на которой она задана.

Например, для аддитивной группы $\mathbb{Z}_m$ эта задача сводится к решению линейного сравнения первой степени вида $ax \equiv_m b$, и не представляет трудности.

Гораздо сложнее решение этой задачи в мультипликативной группе $\mathbb{F}_p^*$, где p — большое простое число.

В настоящее время размер этого простого числа должен составлять порядка 1000 бит, чтобы эта задача была трудно решаема и ее можно было использовать при построении стойких криптосистем. Понятно, что реализация таких систем требует больших объемов памяти.

Очевидно, что найти такой элемент x в группе $\mathbb{Z}_m$, что $a^x = b$ можно лишь если b принадлежит подгруппе, порожденной элементом a. Если же группа G циклическая, а a — её порождающий элемент группы, то вопрос снимается.

Алгоритм согласования. Рассмотрим сравнение

$$a^x \equiv_p b \tag{5.7}$$

в мультипликативной группе простого поля Галуа $G = \mathbb{F}_p^*$, где p — простое число. Будем предполагать, что a — примитивный элемент группы G.

С помощью перебора можно решить сравнение (5.7) за $O(p)$ арифметических операций.

Известна формула $\log_a b = \sum_{j=1}^{p-2} (1 - a^j)^{-1} b^j \pmod{(p-1)}$, однако сложность вычисления по ней, очевидно, хуже, чем для простого перебора.

Алгоритм согласования решения сравнения (5.7)

1. Положить $H = \lceil \sqrt{p} \rceil$.
2. Найти $c = a^H \pmod p$.
3. Составить таблицу степеней $c^u \pmod p$ для $u = 1, \ldots, H$.

4. Составить таблицу значений $b \cdot a^v \pmod p$ для $v = 0, \ldots, H$.

5. Найти совпавшие элементы данных таблиц: для них

$$c^u \equiv_p b \cdot a^v \quad \text{откуда} \quad a^{Hu-v} \equiv_p b.$$

Выдать $x \equiv_{p-1} Hu - v$.

Докажем, что алгоритм работает корректно. Любое целое число $x \in [\, 0,\ p-2\,]$ можно представить в виде

$$x \equiv_{p-1} Hu - v, \text{ где } u \in [\, 1,\ H\,],\ v \in [\, 0,\ H\,].$$

Действительно, набор из $H(H+1)$ чисел вида

$$\begin{gathered} H,\ H-1,\ H-2,\ \ldots,\ H-H \\ 2H,\ 2H-1,\ \ldots,\ 2H-H,\ \ldots, \\ H^2,\ H^2-1,\ \ldots,\ H^2-H \end{gathered}$$

содержит в себе, в частности, все числа

$$0,\ 1,\ \ldots,\ p-2,$$

поскольку $H^2 > p$.

На практике после выполнения Шагов 3 и 4 проводят упорядочение таблиц по возрастанию выходных значений.

Пример 5.13. Решим сравнение $6^x \equiv_{11} 8$.

Имеем $p = 11,\ a = 6,\ b = 8$.

1. $H = \lceil \sqrt{11}\, \rceil = 4$.

2. $6^4 = 1\,296 \equiv_{11} 9 = c$.

3. $u = 1, 2, 3, 4$ (во 2-й строке — величины $9^{u-1} (\mathrm{mod}\ 11) \cdot 9$):

u	1	2	3	4
	9	$9 \cdot 9 = 81$	$4 \cdot 9 = 36$	$3 \cdot 9 = 27$
$9^u \pmod{11}$	9	4	3	5

4. $v = 0, 1, \ldots, 4$

v	0	1	2	3	4
6^v	1	6	36	216	1 296
$8 \cdot 6^v$	8	48	288	1 728	10 368
$8 \cdot 6^v \pmod{11}$	8	4	2	1	6

5. Совпал элемент 4 таблиц при $u = 2$, $v = 1$, поэтому $x = Hu - v = 7 \equiv_{10} 7$.

Алгоритм согласования применим для вычисления дискретного логарифма в произвольной циклической группе.

Пример 5.14. Пусть требуется решить сравнение

$$2^x = 17 \pmod{25}.$$

Для этого рассмотрим группу $G = \mathbb{Z}_{25}^*$. Понятно, что $|G| = \varphi(25) = \varphi(5^2) = 5^1 \cdot \varphi(5) = 20 = n$, конкретно,

$$G = \mathbb{Z}_{25} \setminus \{\ 0,\ 5,\ 10,\ 15,\ 20\ \},$$

и легко убедится, что $G = \langle 2 \rangle$. Далее применяем описанный алгоритм, заменяя p на основание сравнения 25, кроме первого шага, где заменяем p на $n = 20$.

1. $H = \lceil \sqrt{20} \rceil = 5$.
2. $c = 2^5 \equiv_{25} 7$.

3. $u = 1, 2, \ldots, 5$

u	1	2	3	4	5
$7^u \pmod{25}$	7	24	18	1	7

4. $v = 0, 1, \ldots, 5$

v	0	1	2	3	4	5
$17 \cdot 2^v \pmod{25}$	17	9	18	11	22	19

5. Совпал элемент 18 таблиц при $u = 3$, $v = 2$, поэтому $x = Hu - v = 13 \equiv_{19} 13$.

Разработаны и другие (субэкспоненциальные) алгоритмы дискретного логарифмирования, основанные на различных идеях.

5.6 Криптосистемы Мак-Элиса и Ниддеррайтера

Криптосистема Мак-Элиса. Данная система зашифрования с открытым ключом основана на трудности решения задачи *декодирования линейного кода*, исправляющего ошибки[15)]; эта задача, как уже было указано, NP-трудна.

Система разработана в 1978 г. американским математиком и инженером *Робертом Мак-Элисом* (Robert J. McEliece, 1942) и является исторически первой криптосистемой, использующая в процессе шифрования

[15)] Эта задача декодирования множества данных (Information Set Decoding Problem, ISD Problem) и состоит указании вероятностной стратегии, которая пытается определить позиции $\leqslant \lfloor d/2 \rfloor$ ошибок в принятом, возможно искажённом слове $[k, n, d]$-кода.

рандомизацию — внесение случайностей в данные. Кратко опишем её простейший вариант.

Каждый абонент создаёт свой секретный и открытый ключи. Для этого он

1. Выбирает исправляющий достаточно большое число r ошибок линейный $[n, k, 2r+1]$-код C. Пусть код C задаётся порождающей матрицей $G_{k\times n}$.

2. Генерирует случайные квадратные матрицы:

S порядка k — невырожденную;

P порядка n — перестановочную.

3. Вычисляя $k \times n$-матрицу

$$\widetilde{G} = S \times G \times P,$$

«маскирующую» матрицу G, строит тем самым новый код.

Заметим, что преобразование $G \times P \to G'$ задаёт переход к порождающей матрице G' эквивалентного к C кода.

Секретным ключом является тройка матриц (S, G, P), а открытым — пара $(\widetilde{G}, r)$. Абоненты обмениваются своими открытыми ключами.

Алиса, получив открытый ключ $(\widetilde{G}_B, r)$ Боба, и желая зашифровать своё сообщение u длины k:

1) выбирает случайный n-вектор e с не более чем r единицами;
2) вычисляет вектор $w = u\widetilde{G}_B + e$ и пересылает его Бобу.

Для расшифрования криптограммы w Боб:

1) вычисляет вектор $w' = wP^{-1}$;
2) используя какой-либо алгоритм декодирования кода C, получает из w' вектор u'.
3) вычисляет $u = u'S^{-1}$.

Описанная схемы расшифрования действительно восстанавливает исходное сообщение u. Действительно, имеем:

$$w' = wP^{-1} = \left[u\widetilde{G}_B + e\right]P^{-1} = \\ = \left[uSGP + e\right]P^{-1} = (uS)G + eP^{-1}.$$

Поскольку вектор eP^{-1} содержит не более r единиц, алгоритм декодирования кода C корректирует w' до $u' = uS$. Преобразование $u'S^{-1} = u$ завершает расшифрование.

Шифрсистема Мак-Элиса основана на следующих предположениях.

1. Предполагается, что задача NCP поиска кодового слова, ближайшего к принятому, даже при известной порождающей матрице трудна для «почти всех» кодов. Значит, даже зная хороший алгоритм декодирования кода с матрицей G, трудно декодировать код с матрицей $G \times P$.
2. Домножение сообщения u на S перед кодированием призвано разрушить внутреннюю структуру сообщения, чтобы трудно было его «угадать».

По сравнению с RSA криптосистема Мак-Элиса имеет преимущество в скорости зашифрования и рас-

шифрования, а также более высокую степень защиты при данной длине ключа.

К недостаткам системы относятся большие размеры открытого ключа и криптограммы w, которая оказывается значительно длиннее сообщения u.

Пример значений реально используемых параметров шифрсистемы Мак-Элиса: $n = 6960$, $k = 5413$, $r = 119$, размер открытого ключа — 8 373 911 бит.

Криптосистема Нидеррайтера — предложенная в 1986 г. Х. Нидеррайтером[16] модификация системы Мак-Элиса.

В отличие от неё, криптосистема Нидеррайтера использует проверочную $H_{m\times n}$, а не порождающую матрица $[n, k, 2r+1]$-кода, и не использует рандомизацию данных.

Открытым ключом является пара (H', r), где $H' = S \times H \times P$, а S и P — выбранные Алисой квадратные матрицы: случайная невырожденная порядка $n - k$ и перестановок порядка n соответственно. Секретный ключ — тройка (S^{-1}, H, P^{-1}). В данной системе сообщениями являются все n-векторы с весом, не превосходящим r.

Поскольку система не использует случайные параметры, результат шифрования одного и того же текста будет одинаковым, что позволяет использовать её для создания ЭЦП.

Размер открытого ключа в криптосистеме Нидер-

[16] *Харальд Нидеррайтер* (Harald G. Niederreiter, 1944) — австрийский математик.

райтера в $\frac{n}{n-k}$ раз меньше, чем в системе Мак-Элиса, а по сравнению с RSA скорость шифрования выше приблизительно в 50 раз, а дешифрования — в 100 раз.

Однако для её использования необходим алгоритм перевода исходного сообщения в n-вектор веса r и размер криптограммы намного больше, чем размер открытого текста.

Для ряда частных случаев системы Мак-Элиса и Нидеррайтера взломаны российскими криптоаналитиками, однако они остаются стойкими при условии использовании кодов Гоппы[17)].

[17)] Криптосистема Мак-Элиса на кодах Гоппы рассматривается Еврокомиссией как перспективная.

Глава 6

Начала эллиптической криптографии

6.1 Эллиптическая криптография: введение

Зачем нужна эллиптическая криптография? *Эллиптическая криптография* (ECC, Elliptic-curve cryptography) изучает асимметричные криптосистемы, основанные на эллиптических кривых (ЭК) над конечными полями.

Преимущество эллиптической криптографиии состоит в следующием. Во-первых, эллиптические кривые удобнее мультипликативных групп конечных полей, так как существует бóльшая свобода в выборе такой кривой, чем в выборе конечного поля. И во-вторых, самое главное: алгоритмы дискретного логарифмирования, разработанные для конечных полей, оказываются бесполезными в случае эллиптических кривых (задача ECDLP), для которых наиболее быстрые имеют субэкспоненциальную сложность.

На ЭК реализуют алгоритмы асимметричного шифрования, ЭЦП, протоколы выработки общего секретного ключа для симметричного шифрования, генераторы псевдослучайных последовательностей.

Криптосистемы на основе эллиптических кривых в 1985 г. независимо друг от друга были предложены в работах американских математиков *Виктора Миллера* (Victor Saul Miller, 1947) и *Нила Коблица* (Neal I. Koblitz, 1948).

Основные понятия. *Алгебраическая кривая E порядка n над полем K* есть множество точек, удовлетворяющих уравнению

$$F(x, y) = 0,$$

где $(x, y) \in K^2$, а $F(x, y)$ — полином степени n.

Например, *прямая* определяется уравнением

$$ax + by + c = 0,$$

а *кривая второго порядка (коника)* — уравнением

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0.$$

Определение 6.1. *Точку кривой* E, задаваемой полиномом $F(x, y)$ называют *неособенной*, если в ней хотя бы одна из частных производных $\partial F/\partial x$ и $\partial F/\partial y$ отлична от нуля, и *особенной* — в противном случае.

Кривая E есть *гладкая* (*неособенная*, *несингулярная*), если все её точки неособенные.

Ясно, что в любой точке (x_0, y_0) гладкой кривой $F(x, y) = 0$ можно провести касательную — прямую

$$(x - x_0)\,\frac{\partial F(x_0, y_0)}{\partial x} + (y - y_0)\,\frac{\partial F(x_0, y_0)}{\partial y} = 0.$$

Утверждение 6.2. *Всякую неособенную алгебраическую кривую E третьего порядка над произвольным полем можно преобразовать к виду*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (6.1)$$

называемому длинной формой Вейерштрасса.

Определение 6.3. Алгебраическую кривую третьего порядка над произвольным полем K с добавленной точкой $\mathcal{O} \notin K^2$, называемой *бесконечно удалённой* или *бесконечной*, и для которой выполняются равенства

$$(x, y) + \mathcal{O} = \mathcal{O} + (x, y) = (x, y) \quad \text{и} \quad \mathcal{O} + \mathcal{O} = \mathcal{O},$$

называют *эллиптической кривой E над полем K*, символически $E(K)$.

Ясно, что точки $(x, y) \in K^2$, лежащие на $E(K)$, удовлетворяют уравнению (6.1), а $\mathcal{O}$ есть нейтральный элемент (ноль) по сложению в $E(K)$.

Легко проверить, что если $P = (x_0, y_0)$ точка ЭК E, то точка

$$-P = (x_0, -a_1x_0 - a_3 - y_0) \qquad (6.2)$$

также удовлетворяет (6.1), то есть также принадлежит E. Будем называть её *противоположной* к P.

Если $\operatorname{char} K$ не есть 2 или 3 (например, в случае вещественного поля), то уравнение (6.1) при подходящей замене переменных упрощается и принимает вид

$$y^2 = x^3 + a_4x + a_6,$$

называемый *короткой формой Вейерштрасса*. Обычно для $a, b \in K$ её записывают в виде

$$y^2 = x^3 + ax + b. \tag{6.3}$$

В этом случае противоположная к $P = (x_0, y_0)$ точка эллиптической кривой E есть

$$-P = (x_0, -y_0). \tag{6.4}$$

Почему используется странная нумерация индексов, а кривые называются эллиптическими? Формы Вейерштрасса при больших x ведут себя как полукубическая парабола $y^2 = x^3$ (см. рис. 6.1). При параметризации считаем, что x имеет степень 2, а y — степень 3. Тогда индексы i коэффициентов a_i, $i = \overline{1,6}$ (6.1) указывают степени, которые должны быть им даны, чтобы степень каждого слагаемого была равна 6 и уравнение стало однородным. Кривым $y^2 = f(x)$ соответствуют *эллиптические интегралы* вида $\int \frac{dx}{\sqrt{f(x)}}$, не берущиеся в элементарных функциях и связанные с вычислением длин дуг эллипсов.

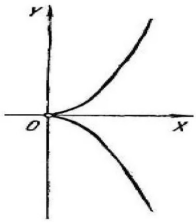


Рис. 6.1. Полукубическая парабола (парабола Нейла)

Короткую форму Вейерштрасса называют *канонической* для ЭК над полями K с характеристикой $\operatorname{char} K \neq 2, 3$. Однако существуют и другие представления эллиптических кривых: формы *Лежандра*, *Монтгомери* и др. Использование той или иной формы может увеличить эффективность операций над точками ЭК.

Эллиптические кривые над полем вещественных чисел не применяются в криптографии, но имеют наглядную графическую интерпретацию как плоских кривых 3-го порядка (*кубик*) и простое объяснение своих важных свойств.

Пусть $E = E(\mathbb{R})$ есть ЭК в короткой форме Вейерштрасса, описывающаяся уравнением

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}.$$

Над полем $\mathbb{R}$ гладкость эллиптических кривых алгебраически означает, что *дискриминант*

$$\Delta \stackrel{\text{def}}{=} -16(4a^3 + 27b^2) \neq 0. \tag{6.5}$$

Тогда кубический многочлен x^3+ax+b не имеет кратных корней, и, конкретно, при $\Delta > 0$ имеет три разных действительных корня, а при $\Delta < 0$ — один действительный корень и два комплексных.

Геометрически гладкость ЭК над $\mathbb{R}$ означает, что её график

- не имеет самопересечений,
- не имеет *точек возврата*, в которых кривая разделяется на две ветви с общей касательной[1)];
- состоит при $\Delta > 0$ из двух связных компонент, а при $\Delta < 0$ — из одной (см. рис. 6.2).

Далее нашей целью будет задание на E такой операции сложения, чтобы эллиптическая кривая превратилась в аддитивную абелевую группу.

[1)] Полукубическая парабола имеет точку возврата $(0, 0)$

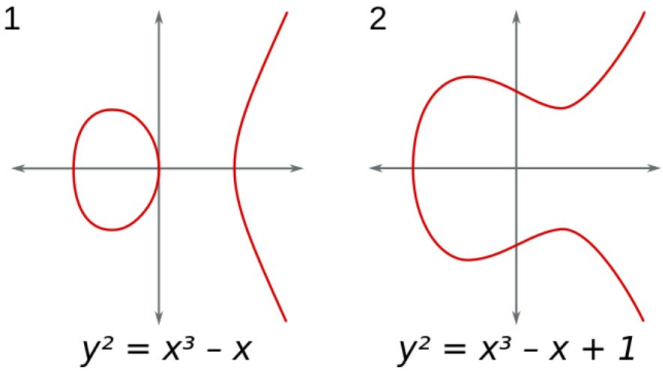


Рис. 6.2. Графики ЭК над $\mathbb{R}$ при (1) $\Delta = 64 > 0$ и (2) $\Delta = -368 < 0$

Заметим, что на некоторых плоских кривых это можно осуществить, и простейшими примерами таких кривых являются прямая и окружность. Например, суммой двух точек $(\cos\alpha, \sin\alpha)$ и $(\cos\beta, \sin\beta)$, окружности $x^2 + y^2 = 1$ будем считать точку $(\cos(\alpha+\beta), \sin(\alpha+\beta))$.

Замечательным свойством ЭК с $\Delta > 0$ является то, что прямая, проходящая через две различные точки кривой, пересересечёт её ещё только в одной точке. Кроме того, касательная (если только она не параллельна OY) пересекает ЭК также в единственной точке. Именно эти свойства и позволяют задать групповую операцию, называемую *сложением точек эллиптической кривой*.

Для этого рассмотрим ЭК с $\Delta > 0$ и положим, что если три точки P, Q и R эллиптической кривой лежат на одной прямой, то их сумма равна $\mathcal{O}$. Это свойство позволяет описать правила сложения точек ЭК:

$$P + Q = -R. \tag{6.6}$$

Проведём через две точки P и Q на кривой E пря-

мую ℓ. Она будет однозначно задавать третью точку R на E. При этом

- если $\ell \nparallel OY$, то точка пересечения R прямой ℓ с E всегда существует;
- если $\ell \parallel OY$, то полагаем $R = \mathcal{O}$ (то есть считаем, что ℓ пересекает E в бесконечной точке);
- если ℓ является касательной к E в некоторой точке, то такая точка считается дважды.

Такое определение сложения справедливо и для ЭК над любыми полями.

Пример 6.4. На рис. 6.3 показано нахождение точки $P + Q$ в случае $Q \neq \pm P$ на действительной ЭК $y^2 = x^3 - x$.

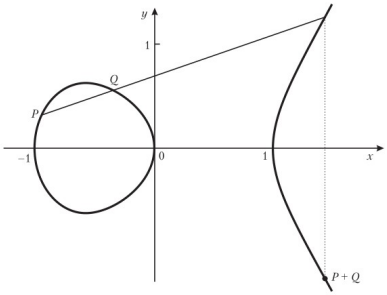


Рис. 6.3

Заманчивая идея назвать суммой P и Q саму точку R несостоятельна: при этом $P + Q = R \not\Rightarrow P = R - Q$.

Для особых точек определить операцию сложения не удается. Поэтому для наделения точек кривой структурой абелевой группы необходимо рассматривать гладкие кривые.

Пусть $P = (x_1, y_1)$ и $Q = (x_2, y_2)$. Тогда можно показать, что координаты (x_3, y_3) точки $R = -(P+Q)$ вычисляются по следующим формулам.

1. $P + \mathcal{O} = \mathcal{O} + P = P, \quad -\mathcal{O} = \mathcal{O}.$

2. Пусть $Q = -P$ (то есть $x_1 = x_2$ и $\ell \parallel 0Y$)
   Тогда $R = \mathcal{O}$, и поэтому
   $$Q = -P = -(x_1, y_1) = (x_1, -y_1).$$
   В частном случае, если точка P имеет координаты $(x_1, 0)$ ($\ell \parallel 0Y$ и P есть точка перегиба), то, по общему правилу $P + P = 2P = \mathcal{O}$, откуда $P = -P$.

3. Пусть $Q \neq \pm P$ (тогда $x_1 \neq x_2$ и $\ell \nparallel 0Y$).
   В этом случае прямая ℓ пересечет ЭК E ещё в одной точке R, $P + Q = -R = (x_3, y_3)$ и
   $$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \quad (6.7)$$

4. Если $Q = P$, то ℓ есть касательная к кривой E в точке P и формулы для удвоения точки $P + P = 2P = -R = (x_3, y_3)$ суть
   $$\begin{cases} x_3 = \lambda^2 - 2x_1, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{3x_1^2 + a}{2y_1}. \quad (6.8)$$

Геометрическую иллюстрацию формул суммирования и удвоения точек ЭК см. на рис. 6.4.

Пример 6.5. На ЭК $y^2 = x^3 - 36x$ находятся точки $P = (-3, 9)$ и $Q = (-2, 8)$. Требуется найти $P + Q$ и $2P$.

Решение Имеет место случай 3 определения формул сложения точек ЭК.

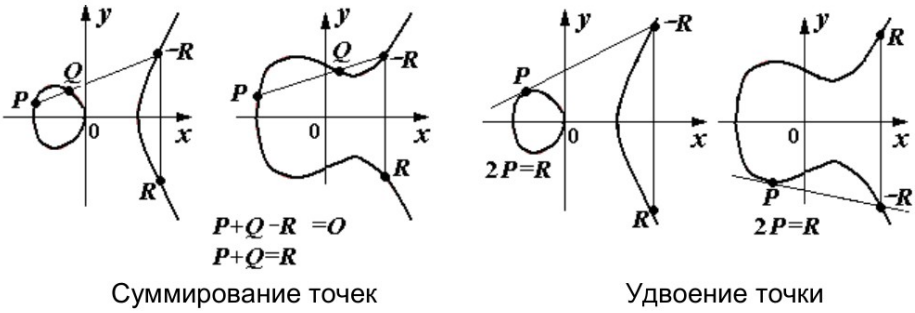


Рис. 6.4. Суммирование и удвоение точек на ЭК

1. Подстановка $x_1 = -3$, $y_1 = 9$, $x_2 = -2$, $y_2 = 8$ в первое из уравнений (6.7) даёт $x_3 = 6$.
2. Тогда второе уравнение даёт $y_3 = 0$ и $P + Q = (6, 0)$ оказалась точкой перегиба.
3. Далее, подставляя $x_1 = -3$, $y_1 = 9$, $a = -36$ в первое уравнение из (6.8) получаем для x-координаты $2P$ значение $25/4$, а второе уравнение даёт для y-координаты значение $-35/8$.

Отметим, что приведённые формулы для суммы и удвоения точек ЭК $E(K)$ останутся справедливыми для всех полей, в которых остаётся верной короткая форма Вейерштрасса (6.3), то есть если $\operatorname{char} K \neq 2, 3$.

Теорема 6.6 (*Пуанкаре*). *Множество $E(K)$ точек эллиптической кривой вместе с бесконечной точкой $\mathcal{O}$ с операцией сложения, описанной выше, является аддитивной абелевой группой.*

Доказательство для случая $\operatorname{char} K \neq 2, 3$.

Легко проверяется *устойчивость* введённой операции сложения:

$$P, Q \in E(K) \Rightarrow P + Q \in E(K).$$

Коммутативность сложения прямо следует из приведённых формул и тождества

$$\frac{y_2 - y_1}{x_2 - x_1} \cdot x_1 - y_1 = \frac{y_2 - y_1}{x_2 - x_1} \cdot x_2 - y_2.$$

Наличие в $E(K)$ *нейтрального элемента* $\mathcal{O}$ уже отмечалось.

Используя приведённый формулы сложения, можно показать и его *ассоциативность*, однако эти вычисления достаточно громоздки (выводится из *теоремы о 9-и точках на кубической кривой*). □

Приведённая теорема А. Пуанкаре справедлива для ЭК над любым полем K при определении сложения в общем виде (6.6).

Умножение точки P на целое положительное k, называемое *скалярным умножением*, определяется как сумма k точек P:

$$kP = P + \ldots + P \quad (k \text{ раз}).$$

6.2 Эллиптические кривые в конечных полях

Порядок эллиптической кривой. Приведём вначале «графики» ЭК $y^2 = x^3 - 7x + 10 \pmod p$ для

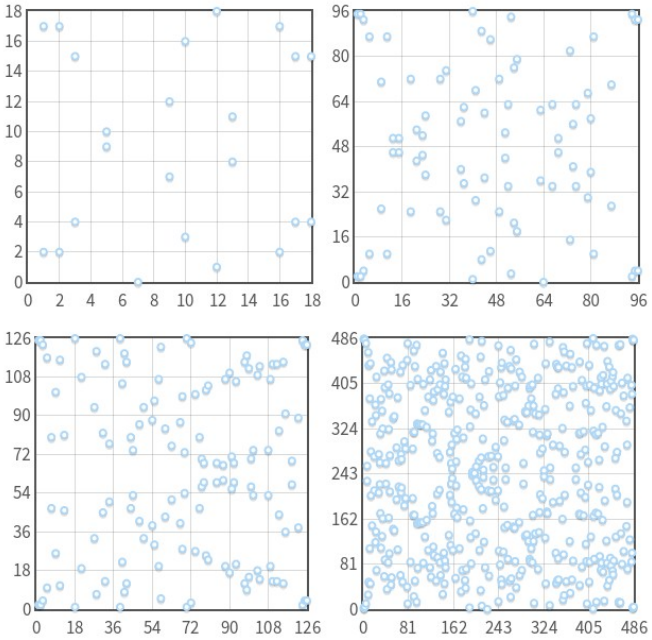


Рис. 6.5. Эллиптическая кривая $y^2 = x^3 - 7x + 10 \pmod p$ при $p = 19,\ 97,\ 127\,487$.

$p = 19, 97, 127, 487$. Видно, что они имеют симметрию относительно $y = p/2$.

Множества точек эллиптической кривой над конечным полем, естественно, конечно. Порядок этой группы будем называть *порядком эллиптической кривой*.

Легко увидеть, что эллиптическая кривая над полем $K = GF(q)$, $q = p^n$, не может содержать более, чем $2q + 1$ точек: это бесконечная точка и не более, чем $2q$ пар $(x, y) \in K^2$, поскольку для каждого из q возможных значений $x \in K$ имеется не более 2-х значений y.

Это грубая мощностная оценка. И так как лишь у половины элементов K^* имеются квадратные кор-

ни, следует сразу ожидать, что порядок эллиптической кривой примерно q.

Сильным результатам является

Теорема 6.7 (*Хассе*, 1934). *Пусть N — порядок эллиптической кривой $E(GF(q))$. Тогда*

$$| N - (q+1) | \leqslant 2\sqrt{q}.$$

Утверждение 6.8. *Группа точек эллиптической кривой над конечным полем есть либо циклическая группа, либо является прямой суммой двух циклических групп.*

Прямая сумма циклических групп не обязательно является циклической группой.

Одним из основных вопросов криптографичесих приложений эллиптических кривых является вычисление или хотя бы оценка их порядков. Эта задача далеко не всегда проста: полиномиальные алгоритмы нахождения порядка ЭК не известны. При этом известны некоторые частные способы выбора ЭК над конечными полями, допускающими достаточно простое вычисление порядка.

Пример 6.9. 1. При $a = 1, b = 0$ короткая форма Вейерштраса (6.3) над $K = GF(7) \cong \mathbb{Z}_7$ принимает вид

$$y^2 = x^3 + x.$$

Будем подставлять вместо x элементы

$$\mathbb{Z}_7 = \{\ 0,\ \pm 1,\ \pm 2,\ \pm 3\ \},$$

и, если возможно, находить значения $y \in \mathbb{Z}_7$:

x	x^3+x	y	x	x^3+x	y
0	0	0	-2	4	± 2
1	2	± 3	3	2	± 3
-1	5	—	-3	5	—
2	3	—			

Перечислим все точки рассматриваемой ЭК:

$$\{\,(0;0),\ (1;\pm 3),\ (3;\pm 3),\ (-2;\pm 2),\ \mathcal{O}\,\};$$

её порядок $N = 8$.

2. Оценим по теореме Хассе порядок N группы E точек ЭК, задаваемой тем же уравнением над простым полем $\mathbb{F}_{23}$:

$$|N-24| \leqslant 2\cdot 5 \ \Rightarrow\ -10 \leqslant N-24 \leqslant +10 \ \Rightarrow$$
$$\Rightarrow\ 14 \leqslant N \leqslant 34.$$

Прямой подсчёт показывает, что $N = 24$:

$$E = \{\,\mathcal{O}, (0,0),\ (1,\pm 5),\ (9,\pm 5),\ (11,\pm 10),$$
$$(13,\pm 5),\ (15,\pm 3),\ (16,\pm 8),\ (17,\pm 10),\ (18,\pm 10),$$
$$(19,\pm 1),\ (20,\pm 4),\ (21,\pm 6)\,\}.$$

3. При $a = b = 1$ уравнение (6.3) над $K = \mathbb{Z}_7$ принимает вид $y^2 = x^3 + x + 1$ и

$$E = \{\,(0;\pm 1),\ (2;\pm 2),\ \mathcal{O}\,\}$$

и $N = 5$.

Теорема Хассе для $q = 7$ даёт оценку $N \leqslant 13$.

4. Рассмотрим то же уравнение $y^2 = x^3 + x + 1$ над $K = \mathbb{Z}_5$, и найдём, что порядок задаваемой им группы ЭК есть $N = 9$:

$$E = \{ (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm), \mathcal{O} \}.$$

Порядком точки эллиптической кривой называют наименьшее натуральное k такое, что $kP = \mathcal{O}$. Понятно, что такого k может и не существовать, и тогда точка имеет *бесконечный порядок*.

Арифметика эллиптических кривых не содержит прямых формул для вычисления кратного для заданной точки $P = (x, y)$, и нахождение kP выполняют с использованием операций сложения, вычитания и удвоения точки.

Умножение точки на число аналогично возведению в степень в случае RSA и требует небольшого числа сложений. Например, для умножения точки на число длины 200 бит будет выполнено в среднем 100 операций удвоения точки и 66 операций сложения точек. Для сравнения: при возведении числа в степень с показателем длины 200 бит в среднем выполняется 300 операций умножения.

Ясно, что если точка P имеет порядок n, то множество

$$\{ \mathcal{O},\ P,\ 2P,\ \ldots,\ (n-1)P \}$$

образует циклическую подгруппу в группе точек ЭК и порядок точки n делит величину N — число точек ЭК.

Пример 6.10. 1. ЭК $y^2 = x^3 - x + 3$ над полем $GF(37)$ имеет порядок $N = 42$. Её подгруппы могут иметь

порядок $n = 1, 2, 3, 6, 7, 14, 21, 42$.

Найдём подгруппу точек этой ЭК, порождённую точкой $P = (2, 3)$. Вычисляя точки jP для $j = 1, 2, \ldots$, получим:

$$1P \neq \mathcal{O}, \quad 2P \neq \mathcal{O}, \quad \ldots, \quad 7P = \mathcal{O},$$

то есть порядок данной точки и порождённой ею подгруппы равен 7.

2. Эллиптическая кривая, определяемая уравнением $y^2 = x^3 - x + 1$ над полем $GF(29)$, имеет порядок $N = 37$, которое является простым числом. Поэтому её подгруппы могут иметь порядок только $n = 1$ или $n = 37$. Тогда при $n = 1$ подгруппа содержит только бесконечно удалённую точку, а при $n = 37$ — все точки данной ЭК.

Криптографически интересны эллиптические кривые, для которых строящиеся с их помощью криптосистемы будут стойки к взлому. Факторизация порядка таких эллиптических кривых не должна содержать малых простых множителей: тогда решение задачи дискретного логарифмирования сильно затруднено. Именно для этого и надо знать порядок ЭК.

В отечественном стандарте требуется, чтобы наименьшим делителем порядка группы точек ЭК было простое число из интервала $[2^{254}, 2^{256}]$.

Алгоритм вычисления порядка n точки P ЭК над полем $GF(p)$

1. Найти максимальную оценку порядка группы точек ЭК по теореме Хассе $N_1 = p + 1 + 2\sqrt{p}$ и вычислить $m = \lceil \sqrt{N_1} \rceil$.

2. Построить таблицу пар (j, jP) для $j = \overline{1, m}$.
3. Вычислить $\alpha = -mP$.
4. Положить $\gamma = \mathcal{O}$.
5. Для $i = 1, 2, \ldots, m-1$:
   5.1 проверить, будет ли точка γ содержаться в таблице, построенной на шаге 2;
   5.2 если $\gamma = jP$, то положить $n = mi + j$; ОСТАНОВ;
   5.3 положить $\gamma = \gamma + \alpha$.

Пример 6.11. Найти порядок точки $P = (0, 1)$ эллиптической кривой

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

над полем $GF(5)$.

Решение.

$$N_1 = 6 + 2\sqrt{5} \approx 10 \Rightarrow m = \left\lceil \sqrt{10} \right\rceil = 4.$$

Строим таблицу

j	1	2	3	4
jP	$(0,1)$	$(4,2)$	$(2,1)$	$(3,4)$

Находим

$$\alpha = -mP = -4(0,1) = -(3,4) = (3,-4) \equiv_5 (3,1).$$

Положим $\gamma = \mathcal{O}$. Эта точка в таблице не содержится. Далее находим

$i = 1 \Rightarrow \gamma = \gamma + \alpha = \mathcal{O} + (3,1) = (3,1)$
— этого значения нет в таблице;

$i = 2 \Rightarrow \gamma = \gamma + \alpha = (3,1) + (3,1) = (0,1)$
— это значение есть в таблице при $j = 1$; поэтому порядок n точки $P = (0,1)$ есть

$$n = mi + j = 4 \cdot 2 + 1 = 9.$$

Поиск порождающей точки для подгруппы ЭК. Для алгоритмов ECC требуются подгруппы с высоким порядком. Поэтому обычно сначала выбирается эллиптическая кривая, вычисляется её порядок N, в качестве порядка группы n выбирается большой делитель, а потом находится точка, порождающая соответствующую подгруппу (base point).

Удобно, если n — простое число. По теореме Лагранжа $N = n \cdot h$. Значение h (индекс подгруппы группы точек ЭК) называют *кофактором* (сомножителем).

Из приведённого соотношения следует, что точка $Q = hP$ создаёт подгруппу порядка n (за исключением случая $Q = hP = \mathcal{O}$, в котором подгруппа имеет порядок 1).

Во многих криптографических протоколах, требующих высокой скорости шифрования, в схеме согласования ключей Диффи – Хеллмана (ECDH) используется эллиптическая кривая

$$y^2 = x^3 + 486662x^2 + x$$

над простым полем $GF(2^{255} - 19)$, что и дало ей название *Curve25519*.

Порядок группы, ясно, есть $N = 2^{255} - 20$. Стартовой является точка кривой с абциссой $x = 9$ (при реализации используется сжатая форма, когда хранятся только x-координаты). Эта точка Q порождает циклическую подгруппу простого порядка

$$n = 2^{252} + 27\,742\,317\,777\,372\,353\,535\,851\,937\,790\,883\,648\,493$$

индекса $h = 8$. Умножение точек проходит за фиксированное время. Размеры секретного и открытого ключей на практике составляют всего 32, 64 или 128 бит.

Алгоритм нахождения точки, порождающей подгруппу заданного порядка в группе точек ЭК

1. Вычисляется порядок N эллиптической кривой.
2. Выбирается порядок n — простое число, делящее N, и вычисляется кофактор $h = N/n$.
3. На ЭК выбирается случайная точка P.
4. Вычисляется точка $Q = hP$.
5. Если $Q = \mathcal{O}$, то возврат к п. 3.

   Иначе точка Q порождает в ЭК подгруппу порядка n с кофактором h.

Формулы сложения точек ЭК над конечными полями. Рассмотрим подробнее эллиптические кривые над полями K конечной характеристики, для которых выполняется (6.5), то есть $\Delta \neq 0$ по $\mathrm{mod}\,(\mathrm{char}\,K)$.

Далее будем для точек

$$P = (x_1, y_1), \quad Q = (x_2, y_2)$$

данной ЭК находить точки $P+Q$ и $2P$ этой же кривой, координаты которых будем обозначать (x_3, y_3).

$\mathrm{char}\,K > 3$. В этом случае справедливо представление эллиптической кривой в короткой форме Вейерштрасса

$$y^2 = x^3 + ax + b, \quad a, b \in K.$$

Если полином $x^3 + ax + b$ не имеет кратных корней, то приведённые на с. 209 формулы для суммы её точек остаются справедливыми. Множество точек таких

ЭК будем обозначать $E_p(a,b)$ или, при фиксированной характеристике поля, $E(a,b)$.

Пример 6.12. В п. 3 примера 6.9 найдены 9 элементов ЭК $y^2 = x^3 + x + 1$ над $K = \mathbb{Z}_5$:

$$E_5(1,1) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,1), (4,4)\}.$$

Покажем, что данная группа — циклическая и $(0,1)$ — её порождающий элемент: по формулам сложения имеем:

$$\begin{aligned}
&(0,1) + \mathcal{O} = (0,1), && (3,1) + (0,1) = (2,4),\\
&(0,1) + (0,1) = (4,2), && (2,4) + (0,1) = (4,3),\\
&(4,2) + (0,1) = (2,1), && (4,3) + (0,1) = (0,4),\\
&(2,1) + (0,1) = (3,4), && (0,4) + (0,1) = \mathcal{O},\\
&(3,4) + (0,1) = (3,1).
\end{aligned}$$

Для некоторых $p > 3$ задача нахождения задача нахождения порядка ЭК над $\mathbb{Z}_p$ решается достаточно просто.

Теорема 6.13. *Над полем $\mathbb{Z}_p$ группа $E_p(a,b)$ либо циклическая, либо есть прямая сумма циклических групп порядков N_1 и N_2, причём $N_2 \mid N_1$ и $N_2 \mid p-1$.*

Теорема 6.14. *Если p — простое и $p \equiv_3 2$, то при любом $b \in \mathbb{Z}_p^*$ порядок группы $E_p(0,b)$ равен $p+1$, и эта группа циклическая.*

char $K = 3$. В этом случае уравнение (6.1) при подходящей замене переменных принимает вид

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in GF(3^n). \qquad (6.9)$$

Будем далее считать, что полином $x^3 + ax + b$ не имеет кратных корней.

Сразу получим, что $-P = -(x_0, y_0) = (x_0, -y_0)$.

Можно получить следующие формулы сложения точек данных ЭК.

3. При $x_1 \neq x_2$ — формулы (6.7) для координат точки $P + Q = 2P$ остаются справедливыми.

4. При $x_1 = x_2$ точка $P+Q = 2P$ имеет координаты

$$\begin{cases} x_3 = \lambda^2 - a + x_1, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{ax_1 - b}{y_1}. \qquad (6.10)$$

Пример 6.15. Найти порядок ЭК

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

над полем $F = \mathbb{F}_3^3 = \mathbb{F}_3[t]/(t^3 + 2t + 1)$.

Решение. Найдём все точки данной ЭК.

Ясно, что $|F| = 27$. Составим таблицу элементов поля F, записанных многочленами от примитивного элемента t с учётом $t^3 = t - 1$.

степень	полином	степень	полином
t	t	t^8	$-t^2 - 1$
t^2	t^2	t^9	$t + 1$
t^3	$t - 1$	t^{10}	$t^2 + t$
t^4	$t^2 - t$	t^{11}	$t^2 + t - 1$
t^5	$-t^2 + t - 1$	t^{12}	$t^2 - 1$
t^6	$t^2 + t + 1$	t^{13}	-1
t^7	$t^2 - t - 1$	t^{13+k}	$-t^k$, $k = \overline{1, 13}$

С её помощью составим таблицу значений многочлена $z(x) = x^3 + 2x + 1$ и величины $y = \pm\sqrt{z(x)}$.

x	$z(x)$	y	x	$z(x)$	y
0	1	± 1			
1	1	± 1	-1	1	± 1
t	0	0	$-t$	-1	—
t^2	t^3	—	$-t^2$	t^{14}	$\pm t^7$
t^3	0	0	$-t^3$	-1	—
t^4	t	—	$-t^4$	t^{22}	$\pm t^{11}$
t^5	t^{22}	$\pm t^{11}$	$-t^5$	t^3	—
t^6	t^9	—	$-t^6$	t^{16}	$\pm t^8$
t^7	t	—	$-t^7$	t^{22}	$\pm t^{11}$
t^8	t^{14}	$\pm t^7$	$-t^8$	t^3	—
t^9	0	0	$-t^9$	-1	—
t^{10}	t^9	—	$-t^{10}$	t^{16}	$\pm t^8$
t^{11}	t^9	—	$-t^{11}$	t^{16}	$\pm t^8$
t^{12}	t^3	—	$-t^{12}$	t^{14}	$\pm t^7$

Перечислим все вычисленные 28 точек этой ЭК:

$$(0, \pm 1),\ (\pm 1, \pm 1),\ (t, 0),\ (t^3, 0),\ (t^9, 0), (-t^2, \pm t^7),$$
$$(-t^4, \pm t^{11}),\ (t^5, \pm t^{11}),\ (-t^6, \pm t^8),\ (-t^7, \pm t^{11}),$$
$$(t^8, \pm t^7),\ (-t^{10}, \pm t^8),\ (-t^{11}, \pm t^8),\ (-t^{12}, \pm t^7),\ \mathcal{O}.$$

<u>char $K = 2$</u>. В этом случае кривая (6.1) в зависимости от значений коэффициентов a_2, a_3, a_4, a_6 из $GF(2^n)$ эквивалентна одной из следующих форм кривых:

суперсингулярная — $y^2 + a_3 y = x^3 + a_4 x + a_6$,

несуперсингулярная — $y^2 + xy = x^3 + a_2 x^2 + a_6$.

В рассматриваемом случае не имеется ограничений на кратность корней полиномов в правых частях указанных уравнений.

Одно из значений слова *сингулярность* — особенность. Приведённым терминам отвечают русские *супервырожденная* и *несупервырожденная кривая* соответственно.

Рассмотрим формы этих кривых.

А. *Суперсингулярные кривые.* Для удобства переобозначим коэффициенты суперсингулярной кривой:

$$y^2 + ey \;=\; x^3 + ax + b.$$

Легко показывается, что

$$-(x_0, y_0) = (x_0, y_0 + e).$$

Приведём формулы для вычисления суммы и удвоения точки.

3. При $x_1 \neq x_2$ точка $P + Q$ имеет координаты :

$$\begin{cases} x_3 \;=\; \lambda^2 + x_1 + x_2, \\ y_3 \;=\; \lambda(x_1 + x_3) + y_1 + e, \end{cases} \qquad \lambda = \frac{y_2 + y_1}{x_2 + x_1}.$$

4. При $x_1 = x_2$ точка $P+Q = 2P$ имеет координаты

$$\begin{cases} x_3 \;=\; \lambda^2, \\ y_3 \;=\; \lambda(x_1 + x_3) + y_1 + e, \end{cases} \qquad \lambda = \frac{x_1^2 + a}{e}.$$

Пример 6.16. Найти группу точек ЭК E над $GF(2)$, заданной уравнением

$$y^2 + y \;=\; x^3 + x.$$

При $x = 0$ имеем $y = 0$ и $y = 1$, как и при $x = 1$. В итоге получаем

$$E \;=\; \{\,(0,0),\,(0,1),\,(1,0),\,(1,1),\,\mathcal{O}\,\}.$$

Порядок суперсингулярных ЭК достаточно легко вычисляется. В зависимости от значений коэффициентов e, a, b различают *классы суперсингулярных кривых*. Так, при нечётном n над $GF(2^n)$ имеется 3 неизоморфных таких класса, а при чётном — 7 классов.

Главный недостаток суперсингулярных ЭК заключается в том, что для них известно сведение ECDLP к аналогичной задаче для конечных полей с повышением размерности поля в некоторую константу, зависящую от класса кривой.

Б. *Несуперсингулярные кривые.* Для удобства переобозначим коэффициенты несуперсингулярной ЭК:

$$y^2 + xy = x^3 + ax^2 + b.$$

Приведём формулы для вычисления суммы $P + Q = (x_3, y_3)$ при $P = (x_1, y_1)$, $Q = (x_2, y_2)$.

3. При $x_1 \neq x_2$ точка $P + Q$ имеет координаты :

$$\begin{cases} x_3 = \lambda^2 + \lambda + a + x_1 + x_2, \\ y_3 = \lambda(x_1 + x_3) + y_1. \end{cases} \qquad \lambda = \frac{y_2 + y_1}{x_2 + x_1}.$$

4. При $x_1 = x_2$ точка $P+Q = 2P$ имеет координаты

$$\begin{cases} x_3 = \lambda^2 + \lambda + a, \\ y_3 = x_1^2 + (\lambda + 1)x_3, \end{cases} \qquad \lambda = x_1 + \frac{y_1}{x_1}.$$

Такие ЭК представляют большой криптографический интерес, поскольку задача ECDLP для них существенно более трудна, чем для суперсингулярных ЭК.

Для практической реализации берут кривые вида

$$y^2 + xy = x^3 + x^2 + \gamma, \quad \gamma \in GF(2^n),$$

где либо $\gamma = 1$, либо $\gamma^3 = \gamma + 1$.

6.3 Криптосистемы на эллиптических кривых

Как правило, в криптографических приложениях в качестве поля выбираются $GF(p)$ или $GF(2^n)$, где p, n достаточно велики. Но исследования ведутся и для произвольных конечных полей $GF(q)$, $q = p^n$.

Задача ECDLP. Вообще задача нахождения дискретного логарифма может быть поставлена для любой группы G, в том числе и для группы точек эллиптической кривой. Следует только действия над элементами мультипликативной группы заменить соответствующие действия над элементами ЭК с понижением ступени — см. рис. 6.6.

Тогда задача ECDLP принимает вид нахождения целого числа m из соотношения

$$m \cdot P = Q \tag{6.11}$$

для точек P и Q ЭК.

Использование группы точек ЭК при построении криптосистем позволило уменьшить параметры криптосистем при сохранении их стойкости.

Термины и понятия	Криптосистема над простым конечным полем	Криптосистема на эл. кривой над конечным полем
Группа	$Z_p{}^*$	$E(GF(p))$
Элементы группы	целые $\{1,2,...,p-1\}$	точки $P(x;y)$ на кривой и точка O
Групповая операция	умножение по модулю p	сложение точек
Обозначения	элементы g и h	точки P и Q
	обратный элемент g^{-1}	обратная точка $-P$
	деление $g \cdot h^{-1}$	вычитание точек $P-Q$
	возведение в степень g^a	скалярное умножение mP
Проблема дискретного логарифмирования	$g \in Z_p{}^*$; $h \equiv g^a \pmod p$; найти a	$P \in E(GF(p))$; $Q = mP$; найти m

Рис. 6.6. «Перевод» криптоалгоритма над конечным полем в аналогичный над эллиптической кривой

Криптологическая устойчивость систем на ЭК основана на сложности определения большого m из равенства (6.11) при заданных известных Q и P. Эта сложность связана с тем, что сложение точек на эллиптической кривой приводит к новой точке, местоположение которой не имеет очевидного отношения к расположению исходных, а итерация этого процесса дает точку mP, которая может оказаться где угодно на ЭК.

Приведём аналогию с точками окружности. Если указана некоторая точка P на окружности, то добавление, например, 67,89° к её углу приводит к точке, положение которой можно приблизительно указать. Однако (если не знать о периоде 360°), добавление $1001 \cdot 67{,}89°$ даёт точку, местоположение которой априори невозможно предугадать даже примерно. Следовательно инвертирование процесса умножении точки на число —

определение m из равенства (6.11) — может быть осуществлен только прямым перебором всех возможных m, то есть вычислительно неосуществимо при большом m.

Отметим, что при вычислении mP используется аналог алгоритма быстрого возведения в степень с использованием двоичного представления коэффициента m и формул удвоения точки.

Шифросистема Эль-Гамаля на эллиптических кривых над конечным полем $GF(q)$ основана на трудности решения задачи ECDL. Она аналогична шифрсистеме Эль-Гамаля на мультипликативной группе конечного поля.

Поскольку аддитивная группа точек ЭК циклической может и не быть, разработчику необходимо выбрать на ней циклическую подгруппу достаточно большого размера.

На практике для криптостойкости величина q задается бинарным числом с 1024 и более бит.

Проблема вычисления числа m по точке $m \cdot P$ на группе точек эллиптической кривой сложнее задачи дискретного логарифмирования, и потому для криптостойкости число это порядок группы G можно брать меньше.

Рассмотрим алгоритм работы системы EC-ElGamal.

Доменные (системные) параметры — выбираются и вычисляются организатором шифрсистемы. Ему необходимо:

1) описать конечное поле F, обычно оно простое;

2) задать уравнение ЭК E над полем F, найти порядок $\#(F)$ группы точек кривой E;
3) найти в E циклическую подгруппу G большого порядка N,

$$\#(F) = N \times k, \quad (k - \text{кофактор}),$$

и её порождающий элемент P.

Системные параметры (E, N, P) открыто передаются всем абонентам, заинтересованным в конфиденциальной переписке.

Вычисление ключей. Абонент B для получения информации от абонента A должен выполнить следующее.

1. Выбрать свой секретный ключ

$$k \xleftarrow{\$} [\ 1,\ N-1\ ] = \mathbb{Z}_N^*.$$

2. Вычислить свой открытый ключ $Y = k \cdot P$.

Открытый ключ Y абонент B передаёт A (и всем заинтересованным лицам).

Шифрование. Абонент A составляет текст t, зашифровывает его, пользуясь открытым ключом абонента B, и отправляет шифртекст адресату B, выполняя следующее.

1. Получает открытый ключ Y от абонента B.
2. Представляет свой текст t натуральным числом $m \in [\ 1,\ N-1\ ]$.
3. Вкладывает сообщение m в точку M эллиптической кривой E.

4. Выбирает одноразовый случайный сеансовый ключ $r \xleftarrow{\$} [\ 1,\ N-1\ ]$.
5. Вычисляет

$$\begin{aligned} d &= r \cdot Y, \\ g &= r \cdot P, \\ h &= M + d. \end{aligned}$$

Шифртекст $c = (g, h)$ отправляется абоненту B.

Расшифрование. Адресат B расшифровывает криптограмму $c = (g, h)$, пользуясь своим секретным ключом k. Для этого он должен выполнить следующее.

1. Вычислить $s = k \cdot g = k \cdot r \cdot P$.
2. Вычислить $s_1 = -s$.
3. Вычислить $M = s_1 + h$.
4. Извлечь сообщение m из M.
5. По числу m получить исходный текст t.

Обоснование справедливости алгоритма расшифрования:

$$\begin{aligned} s_1 + h \ = \ -s + M + d \ = \ -k \cdot g + M + r \cdot Y \ = \\ = \ -k \cdot r \cdot P + M + r \cdot k \cdot P \ = \ M. \end{aligned}$$

Пример 6.17. Пусть Алисе необходимо передать Бобу некоторое секретное сообщение t. Для этого она организует шифрсистему Эль-Гамаля на группе точек ЭК.

Построение системы и передача сообщения проходит следующим образом.

Алиса задаёт системные параметры.

1. F есть простое поле Галуа $GF(2971)$.
2. Эллиптическая кривая E над F определяется уравнением

$$y^2 = x^3 + 1965x.$$

   Порядок (число точек) кривой E есть $\#(F) = 2\,972$.
3. Порядок подгруппы некоторой группы есть делитель порядка группы.

   Собственные делители $2\,972$ суть $2, 4, 743, 1\,486$.

   На E выбирается циклическая подгруппа G набольшего порядка $N = 1\,486$ (кофактор $k = 2$) и определяется её порождающий элемент $P = (8, 2123)$.

Системные параметры — открытый ключ — набор (E, N, P).

Далее все вычисления проводятся по $\bmod N$ и формулам (6.4) и (6.7) для ЭК над с характеристикой > 3.

Боб вычисляет ключи, для чего —

1. Выбирает натуральное $k = 1391 \in \mathbb{Z}_N^*$ — свой секретный ключ.
2. Вычисляет свой открытый ключ:

$$Y = k \cdot P = 1391 \cdot (8, 2123) = (589, 1045).$$

Открытый ключ Y Боба публикуется.

Алиса проводит зашифрование своего секретного текста $t =$ FA, пользуясь открытым ключом Боба. Конкретно, Алисе необходимо выполнить следующее.

1. Получить от Боба его открытый ключ Y.
2. Представить свой текст $t =$ FA в 27-ричной системе счисления:
$$m = \underbrace{6}_{\text{код } F} \cdot 27 + \underbrace{1}_{\text{код } A} = 163.$$
3. Вложить сообщение m в точку M эллиптической кривой E.

   Точка с абсциссой m в подгруппе G выбранной ЭК может не существовать. Припишем к m такую цифру δ, чтобы для абциссы $m\delta$ указанная точка существовала.

   Возможно, потребуется приписать несколько цифр. Информация о числе приписанных цифр *становится системным параметром.*

   В нашем примере найдем, что к m достаточно приписать цифру $\delta = 4$, и тогда точка
$$M = (1634, 2494)$$
   принадлежит подгруппе G выбранной ЭК.
4. Выбрать случайный сеансовый ключ $r \in [\,1,\, N-1\,]$; пусть выбрано $r = 1325$.
5. Вычислить
$$d = r \cdot Y = 1325 \cdot (589, 1045) = (2047, 1793),$$

$$g = r \cdot P = 1325 \cdot (8, 2123) = (192, 742),$$
$$h = M + d = (1634, 2494) + (2047, 1793) = (351, 33).$$

Шифртекст $c = (g, h)$ отправляется Бобу.

Боб проводит расшифрование полученной криптограммы c с помощью своего секретного ключа k, выполняя следующие действия.

1. Вычисление
$$s = k \cdot g = 1391 \cdot (192, 742) = (2047, 1793).$$
2. Вычисление
$$s_1 = -s = -(2047, 1793) = (2047, -1793) = (2047, 1179).$$
3. Вычисление
$$M = s_1 + h = (2047, 1179) + (351, 33) = (1634, 2494).$$
4. Извлечение сообщение из M (удаляя из абциссы последнюю цифру 4); получено $m = 163$.
5. Получение по числу $m = 163_{10} = 6, 1_{27}$ сообщения $t = \text{FA}$.

Глава 7

Вопросы и задачи

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) нецелые 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 взаимно-однозначные 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?

Решение. (1) Да, (2) нет (противоположного элемента), (3) нет (устойчивости), (4) нет (нейтрального элемента 0, замкнутости: $1/2 - 1/2 = 0$, 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.

Решение. 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 — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle \cong \mathbb{Z}_{24}$;

$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;
$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_8$;
$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_6$;
$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_4$;
$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_3$;
$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_2$;
$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — единичная.

2. Циклическая группа $\mathbb{Z}_{24}$ имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \cdot \varphi(2) \cdot \varphi(3) = 4 \cdot 1 \cdot 2 = 8$ порождающих элементов. Они взаимно просты с 24 и суть 1, 5, 7, 11, 13, 17, 19, 23.

1.3. Вычислите функцию Эйлера для:

$$\text{а) } n = 375; \quad \text{б) } n = 720; \quad \text{в) } n = 988.$$

Решение.
а) $\varphi(375) = \varphi(3 \cdot 5^3) = 2 \cdot 5^2 \cdot \varphi(5) = 2 \cdot 25 \cdot 4 = 200$.
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. Показать, что если $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ — примарное разложение n, то

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

Решение. $\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) =$

$$= p_1^{\alpha_1 - 1} \varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1} \varphi(p_k) =$$

$$= p_1^{\alpha_1-1} \cdot \ldots \cdot p_k^{\alpha_k-1} \varphi(p_1) \cdot \ldots \cdot \varphi(p_k) =$$
$$= \frac{n}{p_1 \cdot \ldots \cdot p_k} \cdot (p_1 - 1) \cdot \ldots \cdot (p_k - 1) =$$
$$= n \cdot (1 - 1/p_1) \cdot \ldots \cdot (1 - 1/p_k) .$$

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

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

Решение. Все — кольца: (1) обратной матрицы может не быть; (2), (3) многочлены $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ в случае $a_0 = 0$ необратимы).

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

Решение. Нет! Хотя $f(x+y) = 2(x+y) = 2x+2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$.

1.7. Показать, что множество векторов координатного пространства с операциями сложения и векторного умножения является кольцом.

Является ли оно ассоциативным? коммутативным?

Решение. 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

$$\begin{aligned} \boldsymbol{x} \times (\boldsymbol{y} + \boldsymbol{z}) &= \boldsymbol{x} \times \boldsymbol{y} + \boldsymbol{x} \times \boldsymbol{z}, \\ (\boldsymbol{y} + \boldsymbol{z}) \times \boldsymbol{x} &= \boldsymbol{y} \times \boldsymbol{x} + \boldsymbol{z} \times \boldsymbol{x}. \end{aligned}$$

Кольцо $\langle V, +, \times, 0 \rangle$ 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:

$$\begin{aligned} &\boldsymbol{x} \times \boldsymbol{y} = -\boldsymbol{y} \times \boldsymbol{x} \ \text{(антикоммутативность)}, \\ &(\boldsymbol{x} \times \boldsymbol{y}) \times \boldsymbol{z} + (\boldsymbol{y} \times \boldsymbol{z}) \times \boldsymbol{x} + \\ &\qquad + (\boldsymbol{z} \times \boldsymbol{x}) \times \boldsymbol{y} = \mathbf{0} \ \text{(тождество Якоби)}. \end{aligned}$$

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

Решение. В кольце $\mathbb{Z}_6$ классы вычетов по идеалу $(3) = \{0, 3\}$ суть

$$\begin{aligned} 0 + (3) &= 3 + (3) = (0, 3), \\ 1 + (3) &= 4 + (3) = (1, 4), \\ 2 + (3) &= 5 + (3) = (2, 5). \end{aligned}$$

1.9. Является ли поле $\mathbb{Z}_2$ подполем поля $\mathbb{Z}_5$?

Решение. 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. Построить все изоморфизмы между мультипликативной группой поля $\mathbb{F}_7$ и аддитивной группой $\mathbb{Z}_6$.

Решение. Имеем $\mathbb{F}_7^* = \{1, 2, \ldots, 6\}$ и $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}$. Эти группы — циклические, поэтому отображение между любыми порождающими элементами этих групп с естественным продолжением на остальные элементы, задаст искомый изоморфизм.

Группы имеют по $\varphi(6) = 2$ порождающих элементов. Найдём их.

В $\mathbb{Z}_6$ это числа взаимно простые с 6 из интервала $[1, 5]$, то есть 1 и 5.

Покажем, что, например, $g_1 = 3$ — один из порождающий элементов группы $\mathbb{F}_7^*$:

k	0	1	2	3	4	5	6	7	...
$3^k \pmod 7$	1	3	2	6	4	5	1	3	...

Второй порождающий элемент g_2 может быть найден как 3^k, где k взаимно просто с $p-1 = 6$ (см. с. 36). Ясно, что $k = 5$, и поэтому $g_2 = 3^5 = 5$.

2.2. С помощью алгоритма Евклида вычислите НОД (a, b)

a) $a = 589$, $b = 43$; *b*) $a = 6188$, $b = 4709$;
c) $a = 12606$, $b = 6494$; *d*) $a = 20989$, $b = 2573$.

Решение. *Ответ*: *a*) 1, *b*) 17, *c*) 382, *d*) 1.

2.3. 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) $3^{-3} \pmod{8}$.

Решение. 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) $x \cdot 1 = 1 \Rightarrow 1^{-1} = 1$ 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) $1 = 3 \cdot 3 - 8,\ 3 \cdot 3 = 1 + 8,\ 3 \cdot 3 \equiv_8 1,$
$3^{-1} \equiv_8 3,\ 3^{-3} = (3^{-1})^3 = 3^3 = 27 = 3 \pmod 8$.

2.4. 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 — $3x \equiv_9 1$, 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 — $\{2, 5, 8\} \pmod 9$.

2.5. 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.

Решение. Имеем

$$F = \mathbb{F}_2[x]/\left(x^2+x+1\right) = \{\,0, 1=\alpha^3, \alpha, \alpha+1=\alpha^2\,\},$$

где α — порождающий элемент мультипликативной группы F^*. Поэтому

$$\begin{aligned} P = \prod_{i=1}^{3}(x-\beta_i) &= (x+1)(x+\alpha)(x+\alpha+1) = \\ &= (x+1)\left(x^2+\alpha x+x+\alpha x+\alpha^2+\alpha\right) = \\ &= (x+1)\left(x^2+x+\alpha^2+\alpha\right) = \\ &= \left(x^3+(\alpha+1)x^2+(\alpha+1)x^2+(\alpha^2+\alpha+1)x+\right. \\ &\qquad \left.+\alpha^2+\alpha\right) = x^3+1, \end{aligned}$$

и, поскольку любой элемент поля $GF(q)$ удовлетворяет равенству $x^q - x = 0$, имеем

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

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

Решение. 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.

2.7. Доказать, что

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

При $p=2$ утверждение тривиально.

Решение. 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 $(p-1)! \equiv_p -1$.

2.8. Построить поле из 4-х элементов.

Решение. 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

2.9. В расширении $F_{(3)}$ 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.

Решение. Поле $F_{(3)} = \mathbb{F}_2[x]/\big(x^3 + x + 1\big)$ 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 $F_{(3)}$ 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 $F_{(3)}$ суть порождающие его мультипликативной группы, и их м. м. будут совпадать с $a(x)$.

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

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

Решение. 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: $x^5 + x^3 + x^2 + 1 = (x + 1)^3 \left(x^2 + x + 1\right)$.

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

Решение.

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.
$$\begin{array}{rl|r} x^3+2x^2+4x+1 & & x+3 \\ \cline{3-3} x^3+3x^2 & & x^2+4x+2 \\ \cline{1-1} \quad 4x^2+4x & & \\ \quad 4x^2+2x & & \\ \cline{1-1} \qquad\quad 2x+1 & & \\ \qquad\quad 2x+1 & & \\ \cline{1-1} \qquad\quad 0 & & \end{array}$$

3. Перебором элементов $\mathbb{F}_5$ убеждаемся, что многочлен
x^2+4x+2 неприводим над $\mathbb{F}_5$.

Ответ: $x^3+2x^2+4x+1=(x+3)\left(x^2+4x+2\right)$.

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

Решение.

1. 0, 1, 2 — не корни $f(x)\ \Rightarrow\ f(x)$ линейных делителей не имеет.

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: $f(x)=x^4+x^3+x+2\ =$
$=\ \left(x^2+1\right)\left(x^2+x+2\right)$.

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

Решение. 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: $f(x) = \big(x^2 + x + 1\big)\,\big(x^2 + 2x + 4\big)$.

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

Решение. Необходимо и достаточно, чтобы $\deg f(x) = 1$ и $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

Перебором коэффициентов $b, c \in \{\,0,\ 1,\ 2\,\}$ в выражении $x^2 + bx + c$, находим подходящие многочлены:

$$f_1(x) = x^2{+}1, \quad f_2(x) = x^2{+}x{+}2, \quad f_3(x) = x^2{+}2x{+}2.$$

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

Решение. Необходимо и достаточно, чтобы $\deg f(x) = 1$ и $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$. Перебором находим

$$\begin{aligned}
&f_1(x) = x^3 + 2x + 1, && f_2(x) = x^3 + 2x + 2,\\
&f_3(x) = x^3 + x^2 + 2, && f_4(x) = x^3 + 2x^2 + 1,\\
&f_5(x) = x^3 + x^2 + x + 2, && f_6(x) = x^3 + x^2 + 2x + 1,\\
&f_7(x) = x^3 + 2x^2 + x + 1, && f_8(x) = x^3 + 2x^2 + 2x + 2.
\end{aligned}$$

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

Решение. 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 —

2. Факторкольцо $\mathbb{F}_5[x]/\big(x^2+2x+4\big)$ *является полем*; в нём $x^2=-2x-4=3x+1$ и $a(4x^2+2)=$

$$\begin{aligned}
&= \big(2(2x^2+1)\big)^3+2\cdot 2(2x^2+1)+4\ = \\
&= 3(3x^6+2x^4+x^2+1)+3x^2+3\ =\ 4x^6+x^4+x^2+1\ = \\
&= 4(3x+1)^2+3x^2+x+x^2+1\ = \\
&= x^2+4x+4+3x^2+x+x^2+1\ =\ 0\ —\ \text{да, является.}
\end{aligned}$$

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

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

Решение. 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.

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

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

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

Решение. $\beta = x + x^2 = x(x+1)$.

Мультипликативная группа указанных полей состоит из $2^4 - 1 = 15$-и 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 $F_{(4)}$ $\operatorname{ord}\beta = 3$.

2. $\underline{x^4 = x^3 + 1}$

$$\begin{aligned}\beta^2 &= x^4 + x^2 = x^3 + x^2 + 1,\\ \beta^3 &= x(x+1)\left(x^3 + x^2 + 1\right) = \\ &= x\left(x^4 + x^2 + x + 1\right) = x\left(x^3 + x^2 + x\right) = \\ &= x^4 + x^3 + x^2 = x^2 + 1 \neq 1,\\ \beta^5 &= x^2x^3 = \left(x^3 + x^2 + 1\right)\left(x^2 + 1\right) = \\ &= \left(x^5 + x^4 + x^2 + x^3 + x^2 + 1\right) = \ldots\\ \ldots &= \left(x^3 + 1\right)x = x^4 + x = x^3 + x + 1 \neq 1.\end{aligned}$$

Ответ: В поле F $\operatorname{ord}\beta = 15$.

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

Решение. Мультипликативная группа поля

$$\mathbb{F}_2[x]/\left(x^6+x^3+1\right)$$

состоит из $2^6-1=63$-х 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.*

2.21. Найти количество I_p^n нормированных неприводимых многочленов

1) степени 7 над полем $\mathbb{F}_2$;
2) степени 6 над полем $\mathbb{F}_5$.

Решение. 1) $\sum\limits_{d|7} d\cdot I_2^d=2^7=1\cdot I_2^1+7\cdot I_2^7=128$;
$I_2^1=2$: это x и $x+1$, отсюда $I_2^7=\frac{128-2}{7}=18$;

2) $I_5^6=\dfrac{1}{6}\sum\limits_{d|6}\mu(d)\,5^{\frac{6}{d}}=$

$$=\frac{1}{6}\left[\,\mu(1)5^6+\mu(2)5^3+\mu(3)5^2+\mu(6)5\,\right]=$$

$$=\frac{15\,625-125-25+5}{6}=2\,580.$$

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

С её помощью вычислить выражение

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

Решение. 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:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} = \\ = x^6 + x^4 = \left(x^2\right)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \cancel{1} + \cancel{2} = \\ = 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

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

Решение. 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 порождающим элементом 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 $\alpha^i\cdot\alpha^j$.

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

Решение. Многочлен $f(x) = x^2+x+2$ неприводим: ни одно из значений $f(x)$, $x \in \mathbb{F}_3$ не равно 0.

Проверим, является ли $f(x)$ делителем x^4+1:

$$x^4+1 \;=\; \left(x^2+x+2\right)\cdot\left(x^2+2x+2\right) \;-\text{ да, является.}$$

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 $(f(x), a(x))$.

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

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

Решение. Для квадратных матриц порядка 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*

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

Шаг 1. // *Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком*

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= 4x+4, \\ r_0(x) &= 1, \ // \ \deg r_0 = 0 \Rightarrow \textit{СТОП} \\ y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = \\ &= -q_0(x) = -4x-4 = x+1. \end{aligned}$$

3. Вычислим обратную матрицу

$$M^{-1} = (x+1)\begin{bmatrix} 3x+2 & 4x+2 \\ 4x+3 & 3x+4 \end{bmatrix} = \begin{bmatrix} x+3 & 1 \\ 4x & 3x \end{bmatrix}.$$

2.26. Разложить на неприводимые множители многочлен

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

Решение. 1. $f(0) = f(1) = 1$, значит $f(x)$ не имеет корней в $\mathbb{F}_2$, т. е. не имеет линейных делителей.

2. Неприводимый многочлен степени 2 над $\mathbb{F}_2$ единственен: $x^2 + x + 1$.

При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = \big(x^2 + x + 1\big) \times \\ \times (\underbrace{x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1}_{g(x)}).$$

Делим частное $g(x)$ на $x^2 + x + 1$:

$$g(x) = x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ = \big(x^2 + x + 1\big) \cdot \big(x^7 + x^4 + x^3 + x^2 + x + 1\big) + x$$

— 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 $x^3 + x + 1$:

$$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 =$$

$$= \left(x^3+x+1\right)\underbrace{\left(x^6+x^5+x^3+x^2+1\right)}_{h(x)} \quad \text{— делится!}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

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

Поскольку многочлен $h(x)$ 6-й степени не имеет делителей 3-й и меньших степеней, то он является неприводимым.

Ответ: В $\mathbb{F}_2[x]$ справедливо разложение

$$f(x) = x^{11}+x^9+x^8+x^4+x^3+x^2+1 = \left(x^2+x+1\right)\left(x^3+x+1\right)\left(x^6+x^5+x^3+x^2+1\right).$$

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

Решение. 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:

$$\alpha^2 = -2\alpha - 2 = \alpha + 1,$$
$$\alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha = 2\alpha + 1$$

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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right) = GF(3^2)$.

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

Решение.

$\beta \in \{\, 0,\, 1,\, \alpha,\, \ldots,\, \alpha^{14} \,\} = F, \quad x^4 = x + 1.$

$\beta = 0$: $m_0(x) = x$.

$\beta = 1$: $m_1(x) = x + 1$.

$\beta = \alpha$: 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. —

$$m_{\alpha^3}(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) =$$
$$= x^4 + \big(\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12}\big)\, x^3 +$$
$$+ \big(\alpha^3\alpha^6 + \alpha^3\alpha^9 + \alpha^3\alpha^{12} + \alpha^6\alpha^9 + \alpha^6\alpha^{12} + \alpha^9\alpha^{12}\big)\, x^2 +$$
$$+ \big(\alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^9\alpha^{12} + \alpha^6\alpha^9\alpha^{12}\big)\, x +$$
$$+ \big(\alpha^3\alpha^6\alpha^9\alpha^{12}\big) = x^4 + \big(\alpha^3 + (\alpha^3 + \alpha^2) + (\alpha^3 + \alpha) +$$
$$+ (\alpha^3 + \alpha^2 + \alpha + 1)\big)\, x^3 + (\ldots)\, x^2 + (\ldots)\, x + \alpha^{30} =$$
$$= x^4 + x^3 + x^2 + x + 1.$$

$\beta = \alpha^5$: единственный сопряжённый с α^5 элемент — α^{10} (т. к. $\alpha^{20} = \alpha^5$), их м. м. —

$$m_{\alpha^5}(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1$$

— единственный неприводимый многочлен степени 2.

$\beta = \alpha^7$: сопряжённые с α^7 элементы — α^{14}, $\alpha^{28} = \alpha^{13}$, $\alpha^{56} = \alpha^{11}$, их м. м. —

$$m_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) = \\ = x^4 + x^3 + 1.$$

2.29. Найти $m_{\alpha^3}(x)$, где α — примитивный элемент поля $F = \mathbb{F}_5[x]/\big(x^2+x+2\big)$.

Решение. 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 $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\alpha^3 = \alpha\cdot\alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = \\ = 4(4\alpha+3) + 3\alpha = 4\alpha + 2,$$

$$\alpha^{15} = (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = \\ = 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\ = 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3,$$

$$\alpha^3 + \alpha^{15} = 4\alpha + 2 + \alpha + 3 = 0,$$

$$\alpha^{18} = \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\ = 4(4\alpha+3) + 4\alpha + 1 = 3.$$

Ответ: $m(x) = x^2 + 3$.

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

Решение. 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

$$I_2^6 \; = \; \frac{1}{6} \sum_{d|6} \mu(d) \cdot 2^{\frac{6}{d}} \; =$$

$$= \; \frac{1}{6} \left[\, \mu(1) \cdot 2^6 + \mu(2) \cdot 2^3 + \mu(3) \cdot 2^2 + \mu(6) \cdot 2^1 \, \right] \; =$$

$$= \; \frac{1}{6} \left[\, 64 - 8 - 4 + 2 \, \right] \; = \; 54/6 \; = \; 9.$$

2.31. Найти корни многочлена

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

Решение. 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 $\big\{ \, x, \, x^5 \, \big\}$ и $x^2 = -x - 2 = 4x + 3$.

Вычисляем:

$$x^5 = \left(x^2\right)^2 x = x(4x+3)^2 = x\left(x^2+4x+4\right) =$$
$$= x(4x+3+4x+4) = x(3x+2) = 3x^2+2x =$$
$$= 2x+4+2x = 4x+4.$$

Ответ: $\{3,\ x,\ 4x+4\}$.

2.32. Является ли многочлен

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

примитивным?

Решение. 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:

$$x^4 = \left(x^2\right)^2 = (4x+3)^2 = x^2+4x+4 = \ldots$$
$$\ldots = 3x+2 \neq 1,$$
$$x^8 = \left(x^4\right)^2 = (3x+2)^2 = -x^2+2x+4 = \ldots$$
$$\ldots = 3x+1 \neq 1.$$
$$x^{12} = x^8x^4 = (3x+1)(3x+2) = \ldots = 4 \neq 1.$$

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\left(x^2+x+2\right)$.

2.33. 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?

Решение. 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 $\mathbb{F}_5[x]$:

$$
\begin{aligned}
x^8-1 = (x+1)(x-1)(x+2)(x-2)\times\\
\times\left(x^2+2\right)\left(x^2-2\right).
\end{aligned}
$$

В результате удаётся получить разложение рассматриваемого бинома на полем $GF(25)$:

$$
\begin{aligned}
x^{40}-1 = (x+1)^5(x-1)^5(x+2)^5(x-2)^5\times\\
\times\left(x^2+2\right)^5\left(x^2-2\right)^5.
\end{aligned}
$$

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

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

Решение. $\deg f(x)=2$, и поэтому $f(x)$ имеет 2 корня.

(1) Полином $f(x)$ неприводим над $\mathbb{F}_2$ $\Rightarrow$ его корни суть x и x^2.

(2) Полином $f(x)$ приводим над $\mathbb{F}_3$:

$$x^2+x+1 = x^2-2x+1 = (x-1)^2,$$

поэтому $f(x)$ над $\mathbb{F}_3$ имеет корень 1 степени 2.

(3) Полином $f(x)$ неприводим над $\mathbb{F}_5$ $\Rightarrow$ его корни x и x^5.

2.35. Найти корни многочлена

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

Решение. 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[1)].

Рассматриваем поле $F = \mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$. Ясно, что $2 \in F$, и корнями многочлена $f_2(x)$ в нём будут $x,\ x^5,\ x^{25}$.

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 &= x^2(3x+1) = 3x^3 + x^2 = 4x + 3 + x^2 = \\ &= x^2 + 4x + 3; \\ x^{25} &= \big(x^5\big)^5 = \big(x^2 + 4x + 3\big)^5 = x^{10} + 4^5 x^5 + 3^5 = \\ &= x^{10} + 4\big(x^2 + 4x + 3\big) + 3 = x^{10} + 4x^2 + x. \end{aligned}$$

[1)] а если бы это был многочлен 4-й степени?

(поскольку $4^5 = 2^{10} = 102\underline{4}$ и $3^5 = 81 \cdot 3 = 24\underline{3}$).

Найдём отдельно x^{10}:

$$\begin{aligned} x^{10} &= \bigl(x^5\bigr)^2 = \bigl(x^2+4x+3\bigr)^2 = \\ &= x^4 + x^2 + 3^2 + 3x^3 + 4x + x^2 = \\ &= x^4 + 3x^3 + 2x^2 + 4x + 4 = \\ &= \cancel{3}x^2 + \cancel{x} + \cancel{4}x + 3 + \cancel{2}x^2 + 4x + 4 = 4x + 2. \end{aligned}$$

Продолжаем:

$$x^{25} = x^{10} + 4x^2 + x = \cancel{4}x + 2 + 4x^2 + \cancel{x} = 4x^2 + 2.$$

Ответ: корни многочлена $f(x) = 2x^4 + x^3 + 4x^2 + 4 \in \mathbb{F}_5[x]$ суть 2, x, x^2+4x+3, $4x^2+2$; они лежат в поле $F = \mathbb{F}_5[x]/\bigl(x^3+2x+4\bigr)$.

2.36. Найти корни многочлена

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

Решение. Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{\bigl(x^4+x^3+1\bigr)}_{f_1(x)}\underbrace{\bigl(x^4+x^3+x^2+x+1\bigr)}_{f_2(x)}.$$

Уравнения $f_1(x) = 0$ и $f_2(x) = 0$ ранее были решены: их корни соответственно суть

x, x^2, x^3+1, x^3+x^2+x

— в поле $F_1 = \mathbb{F}_2[x]/\bigl(x^4+x^3+1\bigr)$ и

$x,\ x^2,\ x^3,\ x^3+x^2+x+1$
— 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 уравне-ния $f(x)=0$ 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 её для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле F_1:

$$\begin{aligned} x &\mapsto x+1,\\ x^2 &\mapsto (x+1)^2 = x^2+1,\\ x^3 &\mapsto (x+1)^3 = x^3+x^2+x+1,\\ x^3+x^2+x+1 &\mapsto \left(x^3+x^2+x+1\right)+\left(x^2+1\right)+\\ &\quad +(x+1)+1 = x^3. \end{aligned}$$

Проверим, что, например, x^2+1 — корень $f(x)$:

$$\begin{aligned} f\left(x^2+1\right) &= \left(x^2+1\right)^8+\left(x^2+1\right)^4+\left(x^2+1\right)^2+\\ &\quad +\left(x^2+1\right)+1 =\\ &= \left(x^{16}+1\right)+\left(x^8+1\right)+\left(x^4+1\right)+x^2. \end{aligned}$$

Ясно: $x^{16} = x$, $x^4 = x^3 + 1$ 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 $f(x^2+1)$ 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, $x^3 + 1$, $x^3 + x^2 + x$, $x + 1$, $x^3 + x^2 + x + 1$.

2.37. Найти корень многочлена

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

Решение. Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных:

$$f(x) \;=\; x^4 + 2x + 2 \;=\; \left(x^2 + ax + b\right)\left(x^2 + cx + d\right) \;=$$
$$=\; x^4 + cx^3 + dx^2x + ax^3 + acx^2 + adx + bx^2 + bcx + bd \;=$$
$$=\; x^4 + (a+c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd.$$

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.

Таким образом полином $f(x)$ над $\mathbb{F}_3$ *неприводим*.

Теперь рассмотрим поле $\mathbb{F}_3[x]/\big(x^4+2x+2\big)$.

В нём $x^4+2x+2=0$, или $x^4=x+1=0$, а корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3}.

Вычислим x^9 и x^{27}:

$$x^9 = \big(x^4\big)^2 x = (x+1)^2 x = x^3+2x^2+x;$$
$$x^{27} = \big(x^9\big)^3 = \big(x^3+2x^2+x\big)^3 = x^9+2x^6+x^3 = \\ = \ldots = x^3+x^2+x.$$

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 $\mathbb{F}_3[x]/(f(x))$.

2.38. Найти корни многочлена $f(x)=x^5+x^2+1$ над $\mathbb{F}_2$.

Решение. Поскольку $f(0)=f(1)=1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

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

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\big(x^5+x^2+1\big)$.
В нём

$$f(x)=x^5+x^2+1=0, \text{ то есть } x^5=x^2+1=0,$$

и его корни суть x, x^2, x^{2^2}, x^{2^3}, x^{2^4}.

Вычислим x^8 и x^{16}:

$$x^8 = x^5x^3 = \big(x^2+1\big)x^3 = x^5+x^3 = x^3+x^2+1;$$
$$x^{16} = \big(x^8\big)^2 = \big(x^3+x^2+1\big)^2 = x^6+x^4+1 =$$

$$= x^5x + x^4 + 1 = (x^3 + x) + x^4 + 1 =$$
$$= x^4 + x^3 + x + 1.$$

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 простейших кодов (1) утраивания и (2) одной проверки на чётность.

Решение.

1. Код утраивания является линейным $[\,3,\,1,\,3\,]$-кодом, у которого

$$G_{1\times 3} = \left[\begin{array}{c|cc} 1 & 1 & 1 \end{array}\right], \quad I_1 = \left[1\right], \quad P_{1\times 2} = \left[1\ 1\right],$$
$$P^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad H_{2\times 3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

2. Код проверки на чётность есть $[\,n,\,n-1\,]$-код, задаваемый порождающей матрицей

$$G_{(n-1)\times n} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 & 1 \\ & & \ldots & & & \\ 0 & 0 & \ldots & 0 & 1 & 1 \end{bmatrix}$$

или проверочной матрицей

$$H_{1\times n} = \left[\begin{array}{c|c} 1\ \ldots 1 & I_1 \end{array}\right] = \left[1\ 1\ \ldots\ 1\right].$$

3.2. Для кода Хэмминга, 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

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

Решение. 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 $\begin{bmatrix} I_3 & P^T \end{bmatrix}$, 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:

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

$$\begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \end{bmatrix} \times G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Очевидно был задан $[\,7,\,4\,]$-код Хэмминга.

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

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

Решение. 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 они представляются как

$$[\,a,\,b,\,c,\,a,\,b,\,c,\,a,\,b,\,c\,],$$

то есть рассматривается код трёхкратного повторения, у которого $d = 3$.

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 $g(x)$:

$$\begin{array}{l|l}
x^8 + x^7 & x^6 + x^3 + 1 \\
\cline{2-2}
x^8 \quad + x^5 \quad + x^2 & x^2 + x \\
\cline{1-1}
\quad x^7 + x^5 \quad + x^2 & \\
\quad x^7 \quad + x^4 \quad + x & \\
\cline{1-1}
\qquad\qquad x^5 + x^4 + x^2 + x &
\end{array}$$

Таким образом $r(x) = x^5 + x^4 + x^2 + x$ и
$v(x) = x^8 + x^7 + x^5 + x^4 + x^2 + x \;\leftrightarrow\; [0\,1\,1\,0\,1\,1\,\underline{0\,1\,1}]$.

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

Решение. Разложение F^* над $\mathbb{F}_2$ есть

$$\{\alpha^0 = 1 = \alpha^{31}\},\ \{\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8\,\alpha^{16}\},$$
$$\{\alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^{24},\ \alpha^{17}\},\ \{\alpha^5,\ \alpha^{10},\ \alpha^{20},\ \alpha^9,\ \alpha^{18}\},$$
$$\{\alpha^7,\ \alpha^{14},\ \alpha^{28},\ \alpha^{25},\ \alpha^{19}\},\ \{\alpha^{11},\ \alpha^{22},\ \alpha^{13},\ \alpha^{26},\ \alpha^{21}\},$$
$$\{\alpha^{15},\ \alpha^{30},\ \alpha^{29},\ \alpha^{27},\ \alpha^{23}\}.$$

3.5 (шутка). Построить код БЧХ длиной $n = 3$, исправляющий $r = 1$ ошибку.

Решение. Поскольку $n = 3 = 2^t - 1$, то $t = 2$. Мультипликативная группа поля $\mathbb{F}_2^2$ разбивается на два циклотомических класса

$$C_0 = \{\alpha^0 = 1 = \alpha^3\}, \quad C_1 = \{\alpha,\ \alpha^2\},$$

где α — примитивный элемент поля. Нули α, α^2 кода находятся в классе C_1.

Поле $\mathbb{F}_2^2$ может быть построено единственным образом, как $\mathbb{F}_2[x]/\left(x^2+x+1\right)$. В нем $\alpha = x$, $\alpha^2 = \alpha+1$ и м. м. класса C_1 есть $m_\alpha(x) = x^2+x+1 = g(x)$. Имеем $\deg g(x) = 2 = m$ и $k = 1$, т. е. закодированы могут быть два однобитных сообщения: $S = \{0, 1\}$.

Кодирование:

$$0 \cdot (x^2+x+1) \equiv 0 \leftrightarrow [0, 0, 0],$$
$$1 \cdot (x^2+x+1) = x^2+x+1 \leftrightarrow [1, 1, 1],$$

и получен код утраивания.

3.6. Пусть α — примитивный элемент поля $F_{(4)} = \mathbb{F}_2^4 = \mathbb{F}_2[x]/\left(x^4+x+1\right)$. Для кода БЧХ с нулями α, α^2, α^3, α^4 и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

Решение. Поле $F_{(4)}$ есть факторкольцо по идеалу примитивного многочлена $x^4 + x + 1$, в нём $\alpha = x$ и $\alpha^4 = \alpha + 1$.

Таблица соответствий между степенным и полиномиальным представлением элементов поля:

α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100

α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1001
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001
α^{15}	1	0001

Вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14}+\alpha^{10}+\alpha^5+\alpha^4 = \\
&= (\alpha^3+1)+(\alpha^2+\alpha+1)+(\alpha^2+\alpha)+(\alpha+1) = \\
&= \alpha^3+\alpha+1 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12}+1+1+\alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \left(w(\alpha^2)\right)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Поэтому синдромный полином есть

$$s(x) = \alpha^{13}x^4+\alpha^{14}x^2+\alpha^7x+1.$$

Нулей кода всего 4, следовательно число исправляемых ошибок ν не более $2 = r$. Решим соотношение Безу

$$x^{2r+1}a(x)+s(x)\sigma(x) = \lambda(x), \quad \deg\lambda(x) \leqslant r = 2.$$

с помощью обобщённого алгоритма Евклида.

$$\begin{aligned}
\text{Шаг 0.}\quad & r_{-2}(x) = x^5,\\
& r_{-1}(x) = s(x),\\
& \sigma_{-2}(x) = 0,\\
& \sigma_{-1}(x) = 1.
\end{aligned}$$

$$\begin{aligned}
\text{Шаг 1.}\quad & r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),\\
& q_0(x) = \alpha^2 x,\\
& r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x,\\
& \sigma_0(x) = -q_0(x) = \alpha^2 x.
\end{aligned}$$

$$\begin{aligned}
\text{Шаг 2.}\quad & r_{-1}(x) = r_0(x)q_1(x) + r_1(x),\\
& q_1(x) = \alpha^{12} x + \alpha^5,\\
& r_1(x) = \alpha^{14} x^2 + 1,\\
& \quad \deg r_1(x) = 2 \leqslant r,\\
& \sigma_1(x) = \sigma_{-1}(x) - \sigma_0(x)q_1(x) =\\
& \qquad = 1 + \alpha^2 x(\alpha^{12} x + \alpha^5) =\\
& \qquad = \underbrace{\alpha^{14} x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} = \sigma(x).
\end{aligned}$$

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

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 $w(x)$.

Решение. 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.

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1,\\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = \mathbf{0},\\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^7) &= \alpha^{16} + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^8) &= \alpha^{18} + \alpha^{14} + 1 = \mathbf{0}.
\end{aligned}$$

Дальше можно не вычислять: оба корня $\sigma(x)$ найдены. Итак, данный полином локаторов ошибок имеет корни α^5 и α^8. Определяем позиции ошибок:

$$-5 \equiv_{15} 10, \qquad -8 \equiv_{15} 7.$$

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

Решение. Имеем $n = 31 = 2^5 - 1$, $t = 5$, $2r = 6$.

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 3.4 на с. 272 о разложение F^* на классы было установлено, что эти классы также будут пятиэлементными:

$$C_2 = \{\, \alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^{24},\ \alpha^{17} \,\};$$
$$C_3 = \{\, \alpha^5,\ \alpha^{10},\ \alpha^{20},\ \alpha^9,\ \alpha^{18} \,\}.$$

На с. 40 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[2)] 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 —

$$\left(x^5 + x^4 + x^3 + x + 1\right)\Big|_{x=\alpha^5} = \alpha^{25}+\alpha^{20}+\alpha^{15}+\alpha^5+1 =$$
$$= (\alpha^3+1)^5+(\alpha^3+1)^4+(\alpha^3+1)^3+\alpha^5+1 = \ldots = 0.$$

[2)] см., например, [8], Том 1, Таблица C.

Таким образом,
$g_2(x) = x^5+x^3+x^2+x+1,\ g_{\alpha^5}(x) = x^5+x^4+x^3+x+1$
и порождающий многочлен для $[31, 16, 7]$-кода БЧХ есть

$$g(x) = g_1(x)\cdot g_2(x)\cdot g_3(x) =$$
$$= x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1,$$
$$\deg g(x) = m = 15,\ k = n-m = 16.$$

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

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить позиции ошибок в данном слове.

Решение. Для вычислений в поле $F_{(4)}$ нам понадобится таблица, уже построенная на с. 45.

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = \alpha^6 x + 1 = (\alpha^3+\alpha^2)\,x + 1.$$
$$\sigma(\alpha) = \alpha^4+\alpha^3+1 = \alpha+\alpha^3 \neq 0;$$
$$\sigma(\alpha^2) = \alpha^5+\alpha^4+1 = \alpha^2+\alpha+\alpha+1+1 = \alpha^2 \neq 0;$$
$$\ldots\ldots$$
$$\sigma(\alpha^9) = \alpha^{12}+\alpha^{11}+1 =$$
$$= (\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+1 = \mathbf{0}.$$

Полином $\sigma(x)$ линеен, и поэтому имеет лишь один корень $x = \alpha^{15-6} = \alpha^9$.

Находим позицию единственной ошибки:

$$-9 \equiv_{15} 6.$$

4. Теорема Пойа

4.1. Найдите порядок стабилизаторов произвольной (а) вершины, (б) ребра, (в) грани куба при действии группы октаэдра O на соответствующие элементы. Какие перестановки в них содержатся?

Решение.

(а) Пусть O действует на вершины куба и v — некоторая вершина.
Тогда $\mathrm{Stab}\,(v) = \{\, e, s, s^2 \,\} \leqslant O$ — группа вращений на 120° (в выбранном направлении) вокруг диагонали куба, проходящей через данную вершину, $\mathrm{Stab}\,(v) \cong \mathbb{Z}_3$.

(б) Пусть O действует на рёбра куба и r — некоторое ребро.
Тогда $\mathrm{Stab}\,(r) = \{\, e, f \,\} \leqslant O$ — группа вращений на 180° вокруг оси, проходящей через середины рёбер (данного и ему противоположного) куба, $\mathrm{Stab}\,(r) \cong \mathbb{Z}_2$.

(в) Пусть O действует на грани куба и f — некоторая грань.
Тогда $\mathrm{Stab}\,(f) = \{\, e, t, t^2, t^3 \,\} \leqslant O$ — группа вращений на 90° (в выбранном направлении) вокруг вокруг оси, проходящей через середины граней (данной и ей противоположной) куба, $\mathrm{Stab}\,(f) \cong \mathbb{Z}_4$.

4.2. Найти цикловой индекс для следующим образом определённых самодействий четверной группы Клейна

$$V_4 = \{\, e,\, a,\, b,\, c \mid a^2 = b^2 = c^2 = e^2 = e,\, ab = ba = c \,\}:$$

1.
$$e : \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, \qquad a : \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix},$$
$$b : \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, \qquad c : \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix};$$

2.
$$e : \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, \qquad a : \begin{pmatrix} e & a & b & c \\ a & e & b & c \end{pmatrix},$$
$$b : \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \qquad ab : \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix}.$$

Решение. Везде группа Клейна V_4 действует на свои же элементы.

1)

g	$Type(g)$	$w(g)$	#
e	$\langle \underline{4},\, 0,\, 0,\, 0 \rangle$	x_1^4	1
$a,\, b,\, ab$	$\langle 0,\, 2,\, 0,\, 0 \rangle$	x_2^2	3

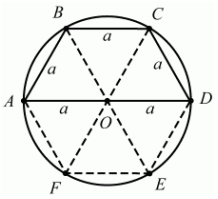
$$Z_{V_4} = \frac{1}{4}\left[\, x_1^4 + 3x_2^2 \,\right].$$

2)

g	$Type(g)$	$w(g)$	#
e	$\langle \underline{4},\, 0,\, 0,\, 0 \rangle$	x_1^4	1
$a,\, b$	$\langle \underline{2},\, 1,\, 0,\, 0 \rangle$	$x_1^2 x_2$	2
ab	$\langle 0,\, 1,\, 0,\, 0 \rangle$	x_2	1

$$P'_{V_4} = \frac{1}{4}\left[\, x_1^4 + 2x_1^2 x_2 + x_2 \,\right].$$

4.3. Найти цикловой индекс транзитивного самодействия группы $\mathbb{Z}_6$.



Решение. Обозначим последовательно вершины правильного шестиугольника буквами $A, \ldots, F$, $\mathbb{Z}_6 = \langle t \rangle$, t — поворот на $60°$.

$g \in \mathbb{Z}_6$	$Type(g)$	$w(g)$
$e = (A)\ldots(F)$	$\langle\, 6,\, 0,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^6
$g = (ABCDEF)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6
$g^2 = (ACE)(BDF)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^3 = (AD)(BE)(CF)$	$\langle\, 0,\, 3,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_2^3
$g^4 = (AEC)(BFD)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^5 = (AFEDCB)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6

$$Z_{\mathbb{Z}_6} \;=\; \frac{1}{6}\left[\, x_1^6 + x_2^3 + 2x_3^2 + 2x_6 \,\right] \;=\; \frac{1}{6}\sum_{d|6} \varphi(d)\, x_d^{6/d};$$

$$D(6) \;=\; \{\, 1, 2, 3, 6 \,\},\; \varphi(1) = \varphi(2) = 1,\; \varphi(3) = \varphi(6) = 2.$$

4.4. Найти число различных вариантов раскраски *граней* куба в 2 и 3 цвета.

Решение. Цикловой индекс:

$$Z(O \underset{\alpha}{:} F) \;=\; \frac{1}{24}\left[\, x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2 \,\right].$$

$$\#Col(2) \;=\; \frac{2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5}{3\cdot 2^3} \;=\; 10.$$

$$\#Col(3) \;=\; \frac{3^6 + 12\cdot 3^3 + \cdot 3^5 + 8\cdot 3^2}{3\cdot 8} \;=\; 57.$$

4.5. Определить число различных раскрасок всех граней правильной 4-угольной пирамиды П в 3 цвета.

Решение. Занумеруем последовательно боковые грани П числами 1, ... 4, а основание — 5.
$G \cong \mathbb{Z}_4 = \langle t \rangle$, t — вращение на 90°.

$g \in \mathbb{Z}_4$	$Type(g)$	$w(g)$	#
$e = (1)(2)(3)(4)(5)$	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
$t, t^3 = (1234)(5)$	$\langle 1, 0, 0, 1, 0 \rangle$	$x_1 x_4$	2
$t^2 = (12)(34)(5)$	$\langle 1, 2, 0, 0, 0 \rangle$	$x_1 x_2^2$	1

$$Z(x_1, \ldots, x_5) = \frac{1}{4}\left[x_1^5 + 2x_1x_4 + x_1x_2^2\right],$$

$$Z(3, \ldots, 3) = \frac{3^5 + 2 \cdot 3^2 + 3^3}{4} = \frac{9 \cdot 32}{4} = 72.$$

4.6. Найти число раскрасок всех граней усечённой правильной 4-угольной пирамиды в 3 цвета.

Решение. Пронумеруем грани П: боковые — с 1 по 4 по часовой стрелке, основания — 5 и 6. Группа, действующая на П — $\mathbb{Z}_4 = \langle t \rangle$, t — поворот на 90° по часовой стрелке.

$g \in \mathbb{Z}_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\ldots(6)$	$\langle 6, 0, \ldots \rangle$	x_1^6	1
t, t^3	$(1234)(5)(6)$	$\langle 2, 0, 0, 1, 0, 0 \rangle$	$x_1^2 x_4$	2
t^2	$(12)(34)(5)(6)$	$\langle 2, 2, 0, \ldots \rangle$	$x_1^2 x_2^2$	1

Цикловой индекс $P = \frac{1}{4}\left[x_1^6 + 2x_1^2x_4 + x_1^2x_2^2\right]$.

$$\#Col(3) = \frac{3^6 + 2 \cdot 3^2 + 3^4}{4} = \frac{3^3(27 + 2 + 3)}{4} = 216.$$

4.7. Найти число различных вариантов раскраски *граней* тетраэдра в 2 и 3 цвета.

Решение. Цикловой индекс:

$$Z(T \underset{\alpha}{:} F, x_1, \ldots, x_4) = \frac{1}{12}\left[\, x_1^4 + 8x_1x_3 + 3x_2^2 \,\right].$$

$$\#Col(2) \;=\; \frac{2^4 + 11 \cdot 2^2}{3 \cdot 2^2} \;=\; \frac{4 + 11}{3} \;=\; 5\,.$$

$$\#Col(3) \;=\; \frac{3^4 + 11 \cdot 3^2}{3 \cdot 4} \;=\; \frac{27 + 33}{4} \;=\; \frac{60}{4} \;=\; 15.$$

4.8. Найти число различных вариантов раскраски *рёбер* тетраэдра в 2 и 3 цвета.

Решение. Группа $T = \langle t, f \rangle$, $t^3 = f^2 = e$, $|T| = 12$, где

t — вращение на 120° вокруг оси, проходящей через вершину и центр симметрии, 4 оси;

f — вращение на 180° вокруг оси, проходящей через середины противоположных рёбер, 3 оси.

Обозначим через E множество рёбер тетраэдра — $|E| = 6$ — и обозначим их цифрами от 1 до 6, считая, что рёбра 1, 2 и 3 инцидентны одной вершине, а ось вращения, задаваемого элементом f, проходит через середины рёбер 1 и 6.
Найдём цикловой индекс.

$g \in T$	$Type(g)$	$w(g)$	#
$e = (1)\ldots(6)$	$\langle\, 6,\, 0,\, \ldots \,\rangle$	x_1^6	1
$t, t^2 = (123)(456)$	$\langle\, 0,\, 0,\, 2,\, 0,\, \ldots \,\rangle$	x_3^2	8
$f = (1)(23)(45)(6)$	$\langle\, 2,\, 2,\, 0,\, \ldots \,\rangle$	$x_1^2x_2^2$	3

$$Z(T \underset{\alpha}{:} E, x_1, \ldots, x_6) = \frac{1}{12}\left[\, x_1^6 + 8x_3^2 + 3x_1^2x_2^2 \,\right].$$

$$\#Col(2) \;=\; \frac{2^6 + 8\cdot 2^2 + 3\cdot 2^4}{3\cdot 2^2} \;=\; \frac{15+9+12}{3} \;=\; 12,$$
$$\#Col(3) \;=\; \frac{3^6 + 8\cdot 3^2 + 3\cdot 3^4}{3\cdot 4} \;=\; 87.$$

4.9. Найти число различных вариантов раскраски *рёбер* куба в 2 цвета.

Решение. Цикловой индекс:

$$Z(O \underset{\alpha}{:} R) \;=\; \frac{1}{24}\left[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \,\right].$$

$$\#Col(2) \;=\; \frac{2^{12} + 6\cdot 2^3 + 3\cdot 2^6 + 7\cdot 2^7}{3\cdot 2^3} \;=\; 218.$$

4.10. Найти число различных вариантов раскраски *вершин* куба в 2 и 3 цвета.

Решение. Цикловой индекс:

$$Z(O \underset{\alpha}{:} V) \;=\; \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$
$$\#Col(2) \;=\; \frac{1}{3\cdot 2^3}\left[\, 2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 2^7 \,\right] \;=\; 23,$$
$$\#Col(3) \;=\; \frac{1}{3\cdot 8}\left[\, 3^8 + 6\cdot 3^2 + 9\cdot 3^4 + 8\cdot 3^4 \,\right] \;=\; 333.$$

4.11. Назовём две булевы функции f_1 и f_2 от n переменных *подобными*, если при подходящей перестановке $(i_1, \ldots, i_n)$ индексов $(1, \ldots, n)$ окажется, что

$$f_1(x_1, \ldots, x_n) \;=\; f_2(x_{i_1}, \ldots, x_{i_n})$$

для всех $(x_1, \ldots, x_n) \in B^n$. Определить, сколько имеется существенно различных (т. е. неподобных) таких функций[3)].

Решение. Здесь $G = S_n$, но она действует не на $\{1, \ldots, n\}$ а на B^n.

Для $n = 4$ результат действия, например, подстановки $g = (1,2)(3,4)$ на четвёрку $(a, b, c, d) \in B^4$ есть (b, a, d, c).

Очевидно, $\mathrm{Fix}\,(g)$ состоит из тех функций, которые постоянны на области действия каждого цикла из g. В нашем случае, например, для $g = (1,2)(3,4)$ получаем $|\,\mathrm{Fix}\,(g)| = 2 \cdot 2 = 4$.

Группа S_4 разбивается на следующие классы сопряжённости:

1) id;
2) шесть 2-циклов — $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$;
3) три произведения по два 2-цикла — $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$;
4) восемь 3-циклов — $(1)(2,3,4)$, $(1)(2,4,3)$, …;
5) шесть 4-циклов — $(1,2,3,4)$, $(1,3,2,4)$, ….

Подстановка id (1) фиксирует все 16 четвёрок (a, b, c, d), $a, b, c, d \in \{0, 1\}$, определяя моном x_1^{16} в цикловом индексе.

Далее, (2) даёт $6x_1^8x_2^4$, т. к., например, $(1,2)$ порождает четыре 2-цикла $(\,(0,1,c,d), (1,0,c,d)\,)$ на B^4 и

[3)] Эта задача для $n = 4$ была решена численно в 1951 г. с помощью компьютерной программы, осуществившей перебор всех $2^{2^4} = 65\,536$ булевых функций. Задача, однако, допускает аналитическое решение.

фиксирует все четвёрки $(0,0,c,d)$ и $(1,1,c,d)$, порождая восемь 1-циклов, и т. д.

Многочлен цикловых индексов группы G, действующий на B^4, имеет вид

$$Z(G) \,=\, \frac{1}{24}\,\left[x_1^{16} + 6x_1^8x_2^4 + 3x_1^4x_2^6 + 8x_1^4x_3^4 + 6x_1^2x_2x_4^3\right].$$

Подставляя $x_1 = \ldots = x_4 = 2$, получаем 3 984 класса подобных булевых функций от 4-х переменных.

Замечание. Если к группе G добавить взятие дополнения как новую симметрию (т. е. считать, что $f_1(x_1,\ldots,x_n) = f_2(x_1^{\sigma_1},\ldots,x_n^{\sigma_n}) \Rightarrow f_1 \sim f_2$, $\sigma_i \in \{0,1\}$), то искомым числом (*классов Шеннона – Поварова*) вместо будет 222.

4.12. Боковые грани правильной 6-угольной пирамиды окрашиваются в красный, синий и зелёный цвета. Определить

(а) число различных 2- и 3-цветных пирамид;

(б) число пирамид с одной красной гранью;

(в) число пирамид, у которых не менее трёх красных граней.

Решение. Имеем транзитивное самодействие $\mathbb{Z}_6$.

(а) *Общее число пирамид.*

$$Z(\mathbb{Z}_6) \,=\, \frac{1}{6}\sum_{d|6}\varphi(d)\,x_d^{6/d} \,=\, \frac{1}{6}\,\left[\,x_1^6 + x_2^3 + 2x_3^2 + 2x_6\,\right].$$

$$\#Col(2) \,=\frac{1}{2\cdot 3}\,\left[\,2^6 + 2^3 + 2\cdot 2^2 + 2\cdot 2\,\right] \,=\, \frac{4\cdot 21}{3} \,=\, 14.$$

$$\#Col(3) = \frac{1}{6}\left[3^6 + 3^3 + 2\cdot 3^2 + 2\cdot 3\right] = \frac{780}{6} = 130.$$

(б, в) *Число пирамид с* 1 *и* 3 $\leqslant$ *красными гранями.* Полагаем $y_1 = y,\ y_2 = y_3 = 1$ (следим только за красными гранями), $x_1 = y + 2,\ x_2 = y^2 + 2,\ x_3 = y^3 + 2.$

$$Z(y) = \frac{1}{6}\left[(y+2)^6 + (y^2+2)^3 + 2(y^3+2)^2 + \right.$$
$$\left. +2(y^6+2)\right] = \frac{1}{6}\left[u_0 + u_1 y + u_2 y^2 + \ldots + u_6 y^6\right] =$$
$$= \frac{1}{6}\left[\left(2^6 + 2^3 + 2^3 + 4\right) + 6\cdot 2^5\, y + \right.$$
$$\left. + \left(16\cdot 15 + 2\cdot 3\cdot 2^2\right) y^2 + \ldots\right].$$
$$u_0 = 84/6 = 14,\ u_1 = 2^5 = 32,$$
$$u_2 = (240 + 24)/6 = 44.$$

Число пирамид с:

(б) одной красной гранью — $u_1 = 32$,

(в) не менее, чем 3 красными гранями — $\#Col(3) - (u_0 + u_1 + u_2) = 130 - (14 + 32 + 44) = 130 - 90 = 40.$

4.13. Имеются плоские бусины, окрашенные с одной стороны в красный, синий и зелёный цвета. Из них составляют ожерелья, содержащие по 8 в равноотстоящих точках окружности. Определить

а) число различных 3-цветных ожерелий;

б) число ожерелий, у которых не менее трёх красных бусин?

Решение. Здесь везде — транзитивное самодействие циклической группы $\mathbb{Z}_8$.

$D(8) = \{1, 2, 4, 8\},\ \varphi(1) = \varphi(2) = 1,\ \varphi(4) = 2,\ \varphi(8) = 4,$

$$Z(\mathbb{Z}_8) \,=\, \frac{1}{8}\sum_{d|8}\varphi(d)\,x_d^{8/d} \,=\, \frac{1}{8}\left[\,x_1^8 + x_2^4 + 2x_4^2 + 4x_8\,\right].$$

а) *Общее число ожерелий*:

$$\#Col(3) \,=\, \frac{3^8 + 3^4 + 2\cdot 9 + 4\cdot 3}{8} \,=\, 834.$$

б) Подсчитаем *число X ожерелий, в которых число красных бусин не более* 3 (т. е. 0, 1 и 2) и вычтем полученное количество из 834.

Полагаем $y_1 = y,\ y_2 = y_3 = 1$ (следим только за бусинами красного цвета).

Найдём коэффициенты u_0, u_1, u_2 при y_0, y_1, y_2 в производящем многочлене W при подстановке $x_k = y^k + 2,\ k = 1, \ldots, 8.$

$$Z(\mathbb{Z}_8) \,=\, \frac{1}{8}\left[\,x_1^8 + x_2^4 + 2x_4^2 + 4x_8\,\right]$$

$$W \,=\, \frac{1}{8}\left[\,(y+2)^8 + (y^2+2)^4 + 2(y^4+2)^2 + 4(y^8+2)\,\right] \,=$$

$$= \,u_0 + u_1 y + u_2 y^2 + \ldots + u_8 y^8 \,=$$

$$= \,\frac{1}{2^3}\left[\,(2^8 + 2^4 + 2\cdot 2^2 + 8) + 8\cdot 2^7 y + \right.$$

$$\left. +(C_8^2\cdot 2^6 + 4\cdot 2^3)\,y^2 + \ldots\,\right].$$

$$u_0 \,=\, 2^5 + 2 + 1 + 1 \,=\, 36, \qquad u_1 \,=\, 128,$$

$$u_2 \,=\, 28\cdot 8 + 4 \,=\, 224 + 4 \,=\, 228.$$

Отсюда

$\#Col(3 \leqslant) = 834 - (36 + 128 + 228) = 834 - 392 = 442.$

4.14. Грани куба раскрашивают в два цвета — красный и синий. Сколько существует кубов

1) различно окрашенных?
2) у которых не менее 4 граней красные?

Решение. Цикловой индекс:

$$Z(O \underset{\alpha}{:} F) = \frac{1}{3 \cdot 2^3}\left[x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2 \right].$$

$$1)\ \#Col(2) = \frac{2^6 + 12 \cdot 2^3 + 3 \cdot 2^4 + 2^5}{3 \cdot 2^3} = \frac{30}{3} = 10.$$

2) Полагаем
$w(1) = y,\ w(2) = 1,\ x_k = y^k + 1,\ k = \overline{1,6}.$

$$W = \frac{1}{24}\left[(y+1)^6 + 6(y+1)^2(y^4+1) + \right.$$
$$\left. + 3(y+1)^2(y^2+1)^2 + 6(y^2+1)^3 + 8(y^3+1)^2 \right].$$

$\#Col(\geqslant 4) = u_4 + u_5 + u_6$ — число кубов с 4, 5 и 6 красными гранями соответственно. Очевидно $u_5 = u_6 = 1$.

Раскрывая W, находим:

$$W = \frac{1}{24}\left[\ldots + C_6^4 y^4 + \ldots + 6(y^2+2y+1)(\underline{y^4}+1) + \right.$$
$$+3(\underline{y^2}+2y+1)(\underline{y^4}+2\underline{y^2}+1) +$$
$$\left. +6(y^6+3\underline{y^4}+3y^2+1) + 8(y^6+2y^3+1) \right].$$

$$u_4 = \frac{15+6+9+18}{3 \cdot 8} = \frac{5+2+3+6}{8} = \frac{16}{8} = 2.$$

Итого $\#Col(\geqslant 4) = 1 + 1 + 2 = 4$.

4.15. Для раскраски сторон квадрата на стеклянной пластинке используют 3 цвета — красный, синий и зелёный.
Сколько можно получить

1) разнораскрашенных квадратов?
2) квадратов с 1 красным ребром и не более 2 синих?

Решение. Цикловой индекс:

$$Z(D_4) = \frac{1}{8}\left[\, x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2x_2 \,\right]$$

$$1)\ \#Col(3) = \frac{1}{8}\left[\, 3^4 + 2\cdot 3 + 3\cdot 3^2 + 2\cdot 3^2\cdot 3 \,\right] = 21.$$

2) При раскраске в 3 цвета: $x_k = y_1^k + y_2^k + y_3^k,\ k = \overline{1,4}$. Следим только за красным (y_1) и синим (y_2) цветами: $x_k = y_1^k + y_2^k + 1\,,\ k = \overline{1,4}$. Находим $u_{10} + u_{11} + u_{12}$.

$$W = \frac{1}{8}\left[\, (y_1 + (y_2+1))^4 + 2(y_1^4 + y_2^4 + 1) + \right.$$
$$\left. +3(y_1^2 + (y_2^2+1))^2 + 2(y_1 + (y_2+1))^2(y_1^2 + y_2^2 + 1) \,\right] \boxed{=}$$

нас интересуют только члены с y_1^1 (одно красное ребро)

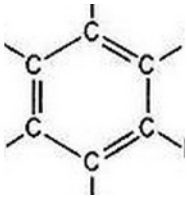
$$\frac{1}{8}\left[\, y_1^4 + 4y_1^3(y_2+1) + 6y_1^2(y_2+1)^2 + \underline{4y_1(y_2+1)^3} + \right.$$
$$+ (y_2+1) + \ldots$$
$$\left. +2(y_1^2 + \underline{2y_1(y_2+1)} + (y_2+1)^2)(y_1^2 + y_2^2 + 1) \,\right] =$$
$$= \frac{1}{8}\left[\, \ldots + 4y_1(y_2+1)^3 + 4y_1(y_2+1)(y_2^2+1)) \,\right] =$$

$$= \frac{1}{8}\Big[\ldots + 4y_1(y_2^3 + \underline{3y_2^2 + 3y_2^1 + 1}) + \\ + 4y_1(y_2^3 + \underline{y_2 + y_2^2 + 1})\Big] \boxed{=}$$

нас интересуют только члены с y_2^0, y_2^1 и y_2^2 при y_1 (синих рёбер — 0, 1, 2)

$$\boxed{=} \frac{1}{8}\,[\,4\cdot 7 + 4\cdot 3\,] = \frac{4\cdot 10}{8} = 5.$$

4.16. Присоединяя к свободным связям углерода бензольного кольца атомы водорода H или метил CH_3, можно получить молекулы разных веществ (ксилол, бензол и др.).



1) Сколько химически разных молекул можно получить таким путём?

2) Сколько из них молекул с присоединёнными $0, \ldots, 6$ атомами водорода?

Решение. Самодействие группы диэдра D_6.
1) Имеем $D_6 = \langle\, t,\, f,\, s \,\rangle$, $t^4 = f^2 = s^2 = e$, $|D_6| = 12$ — группа диэдра порядка 6, где

t — вращение на 60° вокруг центра квадрата;

f — симметрия относительное прямой, проходящей через середины противоположных сторон (3 оси);

s — симметрия относительное прямой, проходящей через противоположные вершин (3 оси).

Пронумеруем последовательно вершины правильного 6-угольника $1, \ldots, 6$.

Перестановки ниже указаны для случая, когда ось f проходит через середины сторон (2-3) и (5-6), а ось s — через вершины 1 и 4.

$g \in D_6$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\ldots(6)$	$\langle 6, 0, \ldots 0 \rangle$	x_1^6	1
t, t^5	(123456)	$\langle 0, \ldots, 0, 1 \rangle$	x_6^1	2
t^2, t^4	$(135)(246)$	$\langle 0, 0, 2, \ldots 0 \rangle$	x_3^2	2
t^3	$(14)(25)(36)$	$\langle 0, 3, 0, \ldots 0 \rangle$	x_2^3	1
f	$(14)(23)(56)$	$\langle 0, 3, 0, \ldots 0 \rangle$	x_3^2	3
s	$(1)(4)(26)(35)$	$\langle 2, 2, 0, \ldots \rangle$	$x_1^2 x_2^2$	3
Всего				12

$$Z(D_6) = \frac{1}{12}\left[\, x_1^6 + 2x_6 + 2x_3^2 + 4x_2^3 + 3x_1^2 x_2^2 \,\right].$$

Всего молекул — подстановка $x_1 = \ldots = x_6 = 2$ (водород H и метил CH_3):

$$M = \frac{64 + 4 + 8 + 32 + 3 \cdot 16}{3 \cdot 4} = \frac{39}{3} = 13.$$

2) *Число молекул с* $0, \ldots, 6$ *атомами водорода* — обозначение $y_1 = \mathrm{H}$, $y_2 = 1$ и подстановка $x_k = \mathrm{H}^k + 1$, $k = \overline{1,6}$ в P.

$$W = \frac{1}{12}\left[\, (\mathrm{H}+1)^6 + 3(\mathrm{H}+1)^2(\mathrm{H}^2+1)^2 + 4(\mathrm{H}^2+1)^3 + \right.$$
$$\left. +2(\mathrm{H}^3+1)^2 + 2(\mathrm{H}^6+1) \,\right] =$$
$$= \mathrm{H}^6 + \mathrm{H}^5 + 3 \cdot \mathrm{H}^4 + 3 \cdot \mathrm{H}^3 + 3 \cdot \mathrm{H}^2 + \mathrm{H} + 1\,.$$

Итого: молекул с числом атомов водорода (как радикала) — H = 0, 1, 5 и 6 — по 1 шт., H = 2, 3 и 4 — по 3 шт., всего — 13.

4.17. Найти число раскрасок куба в красный и синий цвета с 5 красными рёбрами.

Решение. Ранее был найден цикловой индекс действия группы O на рёбра куба:

$$Z(O \underset{\alpha}{:} R) = \frac{1}{24}\left[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \,\right].$$

$y_k = x^k + 1$,

$$\begin{aligned} W &= \frac{1}{24}\left[\, (y+1)^{12} + 6(y^4+1)^3 + 3(y^2+1)^6 + \right. \\ &\quad \left. +6(y+1)^2(y^2+1)^5 + 8(y^3+1)^4 \,\right] = \\ &= \frac{1}{24}\left[\, \ldots + \left(C_{12}^5 + 6C_2^1C_5^2\right)\, y^5 \,\right] = \\ &= \frac{1}{24}\left[\, \ldots + (792 + 6\cdot 2\cdot 10)\, y^5 \,\right] = \ldots + \frac{792+120}{24} y^5 = \\ &= \ldots + (33+5)\, y^5 = \ldots + 38\, y^5. \end{aligned}$$

Ответ: 38.

5. Алгебраические основы криптографии

5.1. 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.

Решение.

Теорема 5.1 (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 если a не делится на p, то $(a^{p-1} - 1) \vdots p$, то есть $a^{p-1} \equiv_p 1$.

5.2. В системе шифрования RSA по данным модулю $n = 91$ и экспоненте $e = 29$ найти ключ расшифрования d.

Решение. 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 $d = 5$.

5.3. 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.

Решение. Организатор выбрал $n = 21 = 3 \cdot 7$, поэтому $\varphi(21) = 2 \cdot 6 = 12$. Для определения d по алгоритму GE-InvZm решается сравнение

$$d \cdot 11 \;=\; 1 \pmod{12}.$$

1	12	0	
2	11	1	$q = 1$
3	1	$\mathbf{-1}$	$q = 11$
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:

$$\begin{aligned} x_1 &= 01^{11} = 1 \equiv_{21} 1, \\ x_2 &= 11^{11} = 285311670611 \equiv_{21} 2, \\ x_3 &= 12^{11} = 743008370688 \equiv_{21} 3. \end{aligned}$$

5.4. Используя алгоритм согласования, решить сравнения

а) $6^x \equiv_{11} 2$; б) $8^x \equiv_{11} 3$; в) $2^x \equiv_{13} 3$.

Решение. (а) $6^x \equiv_{11} 2$. 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 ответ: $x = Hu - v = 4 \cdot 3 - 3 \equiv_{10} 9$.

(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: $x = 4$.

5.5. 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}.

Решение. $X_A = 2^5 = 32 \equiv_{23} 9$;

$X_B = 2^{17} = 131\,072 \equiv_{23} 18$;

$X_C = 2^{12} = 4\,096 \equiv_{23} 2$;

$K_{AB} = X_A^{17} = 9^{17} = 16\,677\,181\,699\,666\,569 \equiv_{23} 3$;

$K_{AC} = X_A^{12} = 9^{12} = 282\,429\,536\,481 \equiv_{23} 9$;

$K_{BC} = X_B^{12} = 18^{12} = 1\,156\,831\,381\,426\,176 \equiv_{23} 18$.

5.6. 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 $y_2 = 03$.

Решение. 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. *Воронин В. П.* Дополнительные главы дискретной математики. — М.: ф-т ВМК МГУ, 2002. [http://padabum.com/d.php?id=10281].
2. *Авдошин С. М., Набебин А. А.* Дискретная математика. Модулярная алгебра, криптография, кодирование. — М.: ДМК Пресс, 2017.
3. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. — М.: КомКнига, 2006.
4. *Берлекэмп М.* Алгебраическая теория кодирования. — М: Мир, 1971.
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. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

10. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.

11. *Нефёдов В. Н., Осипова В. А.* Курс дискретной математики. — М.: Изд-во МАИ, 1992.

12. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

13. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.

14. *Сагалович Ю. Л.* Введение в алгебраические коды: Учебное пособие. — М.: ИППИ РАН, 2010.

15. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.

16. *Ведение* в криптографию. — Под общ. ред. В. В. Ященко. — М. МЦНМО, 2012.