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

Запись лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

алгебраические основы кодирования и шифрования

группы 320, 321, 323, 327, 328
осенний семестр 2020/2021 уч. года

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

2020

Вся моя работа должна была свестись к поискам благородной простоты, свободе от показного нагромождения эффектных трудностей в ущерб ясности; введение некоторых новых приемов казалось мне ценным постольку, поскольку оно отвечало ситуации. ... Таковы мои принципы.

Кристоф Виллибальд Глюк.
Предисловие к опере «*Альцеста*»[1)].

Предисловие

В лекциях рассматриваются приложения конечных алгебраических структур к задачам преобразования данных в целях защиты от случайных помех и несанкционированного доступа. Материал лекций частично взят из источников, указанных в списке литературы (и, как правило, так или иначе переработан), частично подготовлен автором.

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

В конспекте же часто повторяются некоторые определения, формулы, важные при изложении материала в данный момент лекции. Этого избегают в учебниках, а повторение, как известно, — одно из

[1)] к слову, написано либреттистом *Раньери де Кальцабиджи*, а Глюком только подписано

главных условий запоминания и усвоения материала. По той же причине некоторые моменты рассуждений и доказательств излагаются часто подробнее, чем это принято в учебниках. И наоборот, результаты, обозначения и др., считающиеся известными, не поясняются и их использование не специфицируется, чтобы не отвлекаться от хода рассуждений.

В данном конспекте неформальные «квазиопределения» выделяются *курсивом*, а моменты, на которые следует обратить внимание — *наклонным шрифтом*. Естественно, опущены некоторые факультативные сведения, сообщаемые лектором при изложении той или иной темы (а неопущенные даны уменьшенным шрифтом). При этом оставлен некоторый материал, обычно не используемый на лекциях, но полезный при самостоятельной проработке материала. В связи со спецификой преподавания курса, в текст конспекта включено некоторое количество примеров и задач 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, *носитель*, $e \in G$ — *нейтральный элемент*, а $\circ$ — такая бинарная операция на носителе, что для любых его элементов x, y, z выполняются следующие *законы* или *аксиомы группы*:

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

1) $(x \circ y) \circ z = x \circ (y \circ z)$ — *ассоциативность*;

2) $e \circ x = x \circ e = x$ — *свойство нейтрального элемента*;

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

Легко показываются единственность нейтрального элемента группы и единственность обратного элемента. 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.

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

Степень элемента при мультипликативной записи:

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

при которой справедливы обычные свойства степени:

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

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

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

Пример 1.2. 1. *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.
- *Ненулевые* элементы множеств $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — абелевы группы относительно *умножения*.

2. *Симметрическая группа* S_n — группа всех перестановок n-элементного множества относительно операции композиции их $(*)$. Нейтральный элемент S_n — единичная перестановка. Ясно, что $|S_n| = n!$. 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 — абелева группа.

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

$$a^n = e.$$

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

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

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

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

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

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

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

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 $\big[\, G : H \,\big]$ называется *индексом подгруппы H по группе G.*

Следствие. *Порядок любого элемента конечной группы делит порядок группы.*

Для абелевых групп имеется усиление.

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

Как пример — см. равенства **??**.

Определение левого xH и правого Hx *смежных классов 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 $G = \langle \{0,1,2,3,4,5\}, +_6 \rangle$ и её подгруппу $H = \langle \{0,3\}, +_6 \rangle$. Тогда индекс $[\, G : H \,] = 6 : 2 = 3$, 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*. 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 группы называют *изоморфными*, символически $G \cong G'$.

Теорема 1.9. *Любая группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.*

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

Утверждение 1.10. *Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма.*

Циклические группы. Будем рассматривать группы с записью групповой операции в мультипликативной форме. Тогда 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*).

Ясно, что циклическая группа абелева (идуцируется коммутативностью сложения целых чисел), 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

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

то есть она изоморфна группе $\langle\, \mathbb{Z},\ +,\ 0\,\rangle$ целых чисел *по сложению*. Она имеет два порождающих элемента: -1 и $+1$.

2. *Порождающий элемент a имеет конченый 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

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

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

Справедливость последнего соотношения вытекает из утверждения 1.10.

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

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

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

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

Свойства функции Эйлера (p — простое):

- $\varphi(p) = p - 1$;

- $\varphi(n^k) = n^{k-1}\varphi(n)$, откуда $\varphi(p^k) = p^{k-1}(p-1)$;
- если m и n *взаимно просты*, то

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

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

Иллюстрация свойств:

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

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

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

1.2 Кольца и поля

Кольца: определение, основные свойства

Определение 1.11. Абелева группа $\langle\, R,\, +,\, 0\,\rangle$ называется *кольцом*, символически $\langle\, R,\, +,\, \cdot,\, 0\,\rangle$, если на ней

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

Рис. 1.1. Первые 99 значений функции Эйлера

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 одновременно нулём по умножению: для любого элемента x кольца справедливо $x \cdot 0 = 0$. Поэтому любую аддитивную группу G можно 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) $\mathbb{Z}_n = \{\, 0,\ 1,\ \ldots,\ n-1 \,\}$, $n \geqslant 2$ — его называют *кольцом классов вычетов*[1)], рассматривая

[1)] Вычет (лат. residum) — остаток. Интуитивно, это кольцо получается

его элементы как остатки от деления целых на n, и результаты обычных операций сложения и умножения берутся по $\bmod\ n$.

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 $a, b \in R$ из $a \cdot b = 0$ следует, что хотя бы один из сомножителей a и b равен 0.

  Кольцо квадратных матриц имеет делители нуля:

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

Определение 1.12. Нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля называется *целостным*.

Пример 1.13. 1. Кольцо $\mathbb{Z}$ целостно.

2. Чётные $2\mathbb{Z}$ — ассоциативно–коммутативное кольцо без единицы и делителей нуля.

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

3. Кольцо $\mathbb{Z}_n$ ассоциативно–коммутативно, унитально, но нецелостно при составном n: например в $\mathbb{Z}_6$ имеем $3 \cdot 2 = 0$.

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

Определение 1.14. Необратимый элемент p *целостного* кольца называется *неприводимым* или *неразложимым*, если из равенства $p = a \cdot b$ следует, что либо a, либо b обратимы.

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

Определение 1.15. 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*, или *кольцом с однозначным разложением на множители*.

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

Кольцо $\left\{ m + n\sqrt{-3} \mid m, n \in \mathbb{Z} \right\}$ 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 $\mathbb{Z}$.

Легко видеть, что всякое подкольцо содержит 0 наследует такие свойства, как ассоциативность и/или коммутативность.

Подкольцо *собственное*, если оно не совпадает со всем кольцом[2)].

Идеалы колец и факторкóльца. Важнейшими подкольцами являются идеалы.

Определение 1.16. Подкольцо I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$ называется его *(двусторонним) идеалом*, если

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

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

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

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

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

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

Пример правого неглавного идеала в кольце квадратных матриц: совокупность матриц, у которых все столбцы, кроме первого — нулевые.

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

Все КГИ факториальны.

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

Определение 1.18. *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 1.19. 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 1.20. *Максимальные идеалы в* $\mathbb{Z}$ *имеют вид* (p), *где* p — *простое число.*

Доказательство. Пусть p — простое, но идеал (p) не максимальный. Тогда в $\mathbb{Z}$ существует собственный идеал I, строго содержащий (p).

Поскольку $\mathbb{Z}$ — КГИ, то найдётся такое число i, $0 < i < p$, что $I = (i)$. Поскольку $(p) \subset (i)$, то $i \mid p$. Но натуральными делителями p являются только само p и 1. Первый случай невозможен, а второй означает, что идеал $I = (1) = \mathbb{Z}$ несобственный. □

Определение 1.21. *Классом вычетов по модулю идеала* I *коммутативного кольца* $\langle R, +, \cdot, 0 \rangle$ *с представителем* r, называют множество

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

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

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

В качестве представителя класса может быть выбран *любой* элемент класса. Например, элементы класса вычетов $\mathbb{Z}/(n)$ кольца $\mathbb{Z}$ по идеалу (n) суть классы

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

где представитель r класса — остаток от деления некоторого целого на n, $0 \leqslant r < n$.

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. 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 1.22. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$ называется *евклидовым*, если для каждого его *ненулевого* элемента a определена *норма* $N(a) \in \mathbb{N}_0$ такая, что для любого элемента $b \neq 0$ существуют такие элементы q и r, что

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

В большинстве пособий на норму накладывается ещё одно требование — $N(a) \leqslant N(ab)$. Однако 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.

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

Пример 1.23.

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

части целые) евклидово с нормой $N(a+ib) = a^2+b^2$.

Можно показать, что КГИ $\left\{ m \pm n\frac{1+\sqrt{-19}}{2} \mid m,n \in \mathbb{Z} \right\}$ неевклидово.

Все евклидовы кольца — КГИ.

Поля

Определение 1.24. Целостное кольцо, в котором все ненулевые элементы обратимы, называется *полем*[3].

Поле также можно определить как такую пятёрку $\langle K, +, \cdot, 0, 1 \rangle$, что два её *редукта* — абелевы группы: $\langle K, +, 0 \rangle$ по сложению, а $\langle \{K \setminus \{0\}, \cdot, 1 \rangle = K^*$ — по умножению, причём эти группы связаны дистрибутивным законом $x \cdot (y+z) = x \cdot y + x \cdot z$ для всех $x, y, z \in K$.

Для нас важны следующие свойства поля:

1) ненулевые элементы поля K образуют абелеву группу K^* относительно *умножения*, её называют *мультипликативной группой* данного поля;
2) факторкольцо R/I является полем если и только если идеал I кольца R — *максимальный*.

Ясно, что произвольное поле K

— можно рассматривать как евклидово кольцо с нормой, равной 1 для всех ненулевых элементов;

[3] первоначально у Р. Дедекинда — Korper, *корпус*, что подчёркивает замкнутость объекта

— имеет только два (*тривиальных*) идеала: (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

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

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

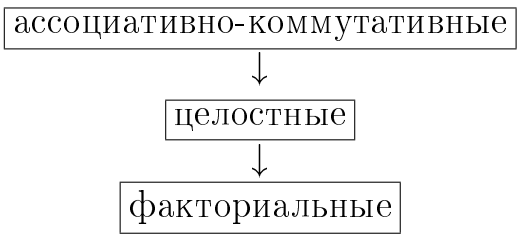
Поле, не обладающее собственным подполем, называется *простым*.

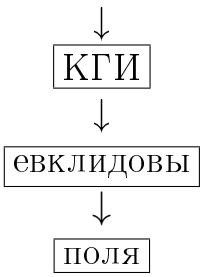
Утверждение 1.25. *В каждом поле содержится только одно простое подполе, которое изморфно либо* $\mathbb{Q}$, *либо* $\mathbb{Z}_p$, p — *простое.*

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

Иерархия колец (от общих к частным):





1.3 Векторные пространства, гомоморфизмы, сравнения

Абстрактные векторные пространства

Определение 1.26. *Абстрактным векторным пространством* над полем $K = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\langle V, K; +, \cdot \rangle$, где

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

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 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 используют *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 $\boldsymbol{x} \in V$ есть (единственная) линейная комбинация базисных векторов:

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

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

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

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

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

Гомоморфизмами называют 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

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

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

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

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

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

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

$$a = b \pmod m, \quad \text{или} \quad a \equiv_m b, \tag{1.1}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4 Задачи

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

1) целые числа, кратные данному натуральному числу n, относительно сложения?
2) неотрицательные целые числа относительно сложения?
3) нечетные целые числа относительно сложения?
4) 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 взаимнооднозначные отображения этого множества на себя, относительно композиции отображений?
14) элементы n-мерного векторного пространства $\mathbb{R}^n$ относительно сложения?

15) параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений?

16) повороты трехмерного пространства $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений?

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

1.3. Вычислите функцию Эйлера для:

а) 375; б) 720; в) 988.

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

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

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

1) квадратные матрицы данного порядка с *действительными* элементами относительно сложения и умножения матриц?

2) многочлены одного неизвестного с целыми коэффициентами относительно обычных операций сложения и умножения?

3) многочлены одного неизвестного с действительными коэффициентами относительно обычных операций?

1.6. Покажите, что для любого элемента r кольца $\langle R, +, \cdot, 0, 1 \rangle$ справедливо $0 \cdot r = r \cdot 0 = 0$.

1.7. Является ли отображение

$$f : \mathbb{Z} \to 2\mathbb{Z},\ f(x) = 2x$$

гомоморфизмом колец?

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

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

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

Глава 2

Конечные кольца и поля

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, телекоммуникационных приложениях.

2.1 Поля Галуа

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

$$(p) = \{ \pm p, \pm 2p, \pm 3p, \ldots, \} \text{ — идеал, и}$$
$$\mathbb{Z}/(p) = \{ \overline{0}, \overline{1}, \ldots, \overline{p-1} \}$$

— кольцо вычетов по модулю идеала (p), то есть классы остатков от деления целых чисел на p:

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

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

Если p — простое, то идеал (p) — максимальный и $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ — *поле*. Его называют *простым полем Галуа* и обозначают $\mathbb{F}_p$ или $GF(p)$[1]. Вообще *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); первым обозначением обычно пользуются математики, а вторым — специалисты по информатике.

[2] 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 наименьшее p такое, что

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

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

Значение $\operatorname{char} K$ может быть только простым числом: иначе, если $\operatorname{char} K = u \cdot v$ при $u, v > 1$, то 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 ∞). Числовые поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — нулевой характеристики.

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

Существуют и бесконечные поля положительной характеристики. Таким будет, например, *поле $K(x)$ рациональных функций* над конечном полем K, элементами которого являются "дроби" $\frac{P}{Q}$, 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 положительной характеристики p.*

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

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

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

Доказательство. В любом коммутативном кольце верна формула степени бинома

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

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

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

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

Мультипликативная группа и примитивный элемент конечного поля. В соответствии с введенным на с. 16 обозначением, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ — мультипликативная группа q-элементного поля Галуа $\mathbb{F}_q$, $q = p^n$, p — простое, n — натуральное.

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

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

Поскольку $|\mathbb{F}_q^*| = q-1$ и порядок любого элемента x конечной группы делит порядок группы, что означает

$$x^{q-1} \;=\; 1,$$

то все её элементы удовлетворяют уравнению

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

Один из них есть 1, но так как $\varphi(q) \geqslant 2$, то в $\mathbb{F}_q^*$ существует ещё хотя бы один элемент такой, что его порядок совпадает с порядком группы. Он и будет элементом, порождающим группу. □

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.

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

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

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 3 — не примитивный.

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), $p - 1 = 10 = 2{\cdot}5$, 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: $\alpha^{12} = 1$ и $\alpha^{18} = 1$.
Например, $3^{18} = 387420489 = 10\,470\,824 \cdot 37 + 1$, и поэтому элемент 3 — не примитивный для поля $GF(37)$.

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

Однако, если найден один примитивный элемент α поля $\mathbb{F}_p$, то любой другой его примитивный элемент может быть получен как степень α^k, где k — взаимно просто с $p - 1 = |\mathbb{F}_p^*|$. В нашем примере $p = 11$ и 2 — примитивный элемент $\mathbb{F}_{11}$, взаимно простые с 10 значения суть 1, 3, 7, 9. В результате получим

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

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

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

Кольца многочленов: деление, корни. Легко видеть, что множество всех многочленов от формальной переменной с коэффициентами из некоторого поля K образует евклидово кольцо; его обозначают $K[x]$.

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

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

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

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.

Неприводимые многочлены

Определение 2.3. Многочлен над некотором полем называется *неприводимым* или *неразложимым*, если он

не является произведением двух многочленов ненулевой степени.

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

В кольце многочленов над

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

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

$\mathbb{C}$ — неприводимы только линейные многочлены.

Далее нас будут интересовать нормированные неприводимые многочлены в кольцах $\mathbb{F}_p[x]$, то есть вида

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

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

Вторая степень: $x^2 + ax + b$.

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

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

$$x^2 + x + 1.$$

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

Исключая, как сделано ранее, делимость на $x+1$, получаем условие

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

Проверкой устанавливаем, что оба эти варианта подходят и дают неприводимые многочлены

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

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

Исключение делимости на $x+1$ приводит к условию

$$a + b + c = 1,$$

то есть остаются к рассмотрению 4 варианта, которые дают 3 неприводимых многочлена:

a	b	c	многочлен
0	0	1	$x^4 + x + 1$
0	1	0	$x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$ — *приводим*
1	0	0	$x^4 + x^3 + 1$
1	1	1	$x^4 + x^3 + x^2 + x + 1$

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

Исключение делимости на $x+1$ приводит к условию

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

— получаем 8 вариантов. Далее исключая делимость на неприводимые многочлены 2 и 3-й степеней (их один и два соответственно) 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. 65).

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

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

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

Для этого в кольце многочленов $\mathbb{F}_p[x]$ выберем некоторый неприводимый многочлен $a(x)$. В этом случае идеал $(a(x))$ будет максимальным в $\mathbb{F}_p[x]$: доказательство проводится аналогично доказательству максимальности идеала (p) в $\mathbb{Z}$ при простом p (см. утверждение 1.20).

Тогда факторкольцо $\mathbb{F}_p[x]/(a(x))$ по модулю рассматриваемого идеала *будет являться полем* относительно сложения и умножения вычетов по модулю $a(x)$. Его элементы суть совокупности $\overline{r(x)}$ многочленов, кратных остатку $r(x)$ при делении многочленов из $\mathbb{F}_p[x]$ на $a(x)$. Иногда говорят, что элементы f, g *сравнимы по двойному модулю* — p и $a(x)$:

$$f(x), g(x) \in \overline{r(x)}, \quad f(x) \equiv_{a(x)} g(x).$$

Если $\deg a(x) = n$, то степени всех многочленов-остатков не выше $n-1$, то есть их всего p^n штук.

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

Может возникнуть вопрос: *почему в обозначении поля $\mathbb{F}_p^n$ не используется многочлен $a(x)$, с помощью которого оно построено?* Ответ даёт следующая

Теорема 2.5. *Любые два поля, содержащие одинаковое число элементов, изоморфны.*

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

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

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

В этом поле сложение коэффициентов многочленов производится по $\bmod 3$, а умножение — с учётом $x^2 = -1 \equiv_3 2$. Например:

$$\overline{2x+1} + \overline{x+2} = \overline{0}, \qquad \overline{x} \cdot \overline{2x} = \overline{1},$$
$$\overline{2x+1} + \overline{x} = \overline{1}, \qquad \big(\overline{2x+1}\big) \cdot \overline{x} = \overline{x+1}, \quad \text{и т. д.}$$

Черту над элементами поля $\mathbb{F}_p[x]/(a(x))$ обычно не ставят и называют их просто «многочленами», считая их *представителями класса* — многочленами наименьшей степени из всего класса.

Пример 2.7. В кольце $\mathbb{R}[x]$ многочленов с действительными коэффициентами возьмём неприводимый многочлен x^2+1 и построим поле

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

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

Расширения простых полей впервые появились в статье Э. Галуа «Из теории чисел» в 1830 г.

Американский математик *Э. Г. Мур* (E. H. Moore) в 1893 г. сообщил о доказательстве теоремы: «Любое конечное поле есть поле Галуа».

2.2 Вычисления в конечных кольцах и полях

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

Поскольку общий делитель пары чисел (a,b) остаётся им и для пары $(a-kb,b)$, то вместо $a-kb$ можно взять остаток r, $0 \leqslant r < b$ от деления нацело a на b, и затем, переставив числа в паре, повторить процедуру; она закончится, т. к. числа в паре уменьшаются, но остаются неотрицательными. В результате образуется пара $(r,0)$, и ясно, что НОД $(a,b) = r$.

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

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

Пример 2.8. 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 2.9 (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 $r = u + (-q)v$. Это справедливо для каждого шага алгоритма Евклида, откуда следует указанное представление. □

[3] дважды описан в «Началах» Евклида, но не был им открыт: 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. 47). Онлайн-калькулятор коэффициентов соотношения Безу доступен по адресу *http://wims.unice.fr/wims/wims.cgi*.

Замечание. Коэффициенты Безу могут быть выбраны неоднозначно, например

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

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

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

0. Зададим матрицу $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ и $r = b$.
1. Перевычислим r как остаток от деления чисел a на b: $a = bq + r$, $0 \leqslant r < b$.

   Если $r = 0$, то второй столбец матрицы E дает вектор $[\,x,\, y\,]^T$ решений заданного соотношения, а d есть последнее ненулевое значение r.
2. Иначе заменим матрицу E матрицей
$$E \times \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix}.$$
3. Заменим пару чисел (a, b) парой (b, r) и перейдем к шагу 1.

Пример 2.10. Обобщённым алгоритмом Евклида найдём натуральное d и целые x и y такие, что

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

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

1. Перевычисляем $r = 252 - 105 \cdot 2 = 42 \neq 0$.
2. Заменяем матрицу E матрицей
$$E \times \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}.$$
3. Заменяем пару чисел $(252, 105)$ парой $(105, 42)$ и перейдем к шагу 1..
4. Вычисляем $r = 105 - 42 \cdot 2 = 21 \neq 0$.
5. Заменяем матрицу E матрицей
$$\begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}.$$
6. Заменям пару чисел $(252, 105)$ парой $(42, 21)$ и перейдём к шагу 1..
7. Вычисляем $r = 42 - 21 \cdot 2 = 0$. Значения $x = -2$ и $y = 5$ найдены, как и $d = 21$.

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

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

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

1. Запишем исходные данные в виде двухстрочной таблицы
$$\begin{matrix} m & 0 \\ c & 1 \end{matrix}$$

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 2.11. Решим в кольце (поле) $\mathbb{Z}/(101)$ сравнение

$$4y \;=\; 1.$$

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

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

Найдено $y^{-1} \;=\; -25 \;\equiv_{101}\; 76$.
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 GE-InvP нахождения в кольце $\mathbb{F}_p[x]/(a(x))$ элемента $y(x)$, обратного к $b(x)$, $\deg a(x) \geqslant \deg b(x)$, НОД $(a(x), b(x)) = 1$.

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

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

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

полагаем $y_0(x) = -q_0(x)$.
При $\deg r_0(x) > 0$ переходим к следующему шагу; иначе — к Шагу $n + 1$.

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

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

вычисляем

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

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

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

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

вычисляем

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

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

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

Пример 2.12. Найдём $\left(x^2 + x + 3\right)^{-1}$ в поле

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

Для этого обобщённым алгоритмом Евклида решим соотношение Безу

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

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

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

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

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

2.3 Поля Галуа как векторные пространства

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

$GF(p^n) \,=$

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

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

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

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

Базисом этого пространства являются векторы

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

или же, переходя к многочленам —

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

Теорема 2.13. *Для каждых простого p и натурального n существует с точностью до изоморфизма ровно одно поле Галуа.*

Действительно, свяжем нули двух таких полей F_1 и F_2 отображением изоморфизма, тогда их мультипликативные группы также изоморфны как конечные циклические группы одинакового порядка.

Пусть $\varphi : F_1 \to F_2$ — отображение некоторого порождающего элемента мультипликативной группы F_1 в некоторый порождающей элемент мультипликативной группы F_1, и нуля F_1 в нуль F_2. Тогда $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Однако не любое такое отображение будет изоморфизмом полей: необходимо также, чтобы $\varphi(a + b) =$

$\varphi(a) + \varphi(b)$, а это обеспечивается не любым отображением указанного вида.

Действительно, рассмотрим два поля:

$$\mathbb{F}_1 = \mathbb{F}_2[x]/(x^3 + x + 1) \text{ и } \mathbb{F}_2 = \mathbb{F}_2[x]/(x^3 + x^2 + 1).$$

Оба многочлена $x^3 + x + 1$ и $x^3 + x^2 + 1$, с помощью которых построены эти поля, примитивны, т. е. формальная переменная x будет порождающим элементом рассматриваемых полей. Отображение $\varphi(x) = x$ будет изоморфизмом мультипликативных групп $\mathbb{F}_1^*$ и $\mathbb{F}_2^*$, при этом оно не будет изоморфизмом самих полей $\mathbb{F}_1$ и $\mathbb{F}_2$.

Проверим, например, выполнение

$$\varphi(x + x^2) = \varphi(x) + \varphi(x^2). \tag{2.3}$$

Построив таблицы таблицы степенного представления элементов этих полей, получим:

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

и равенство (2.3) не выполнено.

Однако можно показать, что среди отображений описанного вида всегда найдётся согласованное не только с операцией умножения, но и операцией сложения.

Для данного примера таким будет, например, $\phi(\alpha) = \beta^3$.

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

степень α $\quad \alpha^4 = \alpha + 1$	1	x	x^2	x^3
α	0	1	0	0
α^2	0	0	1	0
α^3	0	0	0	1
$\alpha^4 = 1 + \alpha$	1	1	0	0
$\alpha^5 = \alpha + \alpha^2$	0	1	1	0
$\alpha^6 = \alpha^2 + \alpha^3$	0	0	1	1
$\alpha^7 = \alpha^3 + \alpha^4 = \alpha^3 + \alpha + 1$	1	1	0	1
$\alpha^8 = 1 + \alpha^2 = 1 + \alpha^2$	1	0	1	0
$\alpha^9 = \alpha + \alpha^3$	0	1	0	1
$\alpha^{10} = \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2$	1	1	1	0
$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$	0	1	1	1
$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$	1	1	1	1
$\alpha^{13} = 1 + \alpha^2 + \alpha^3$	1	0	1	1
$\alpha^{14} = 1 + \alpha^3$	1	0	0	1
$\alpha^{15} = 1$	1	0	0	0

Пусть теперь требуется перемножить x^3+x+1 на x^2+x+1. Используя таблицу это сделать значительно легче, чем прямым перемножением многочленов:

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

Теорема 2.14. *Поле $\mathbb{F}_p^m$ есть подполе $\mathbb{F}_p^n$, если и только если $m \mid n$.*

Доказательство. Пусть поле $K_1 = \mathbb{F}_p^m$ — подполе поля $K_2 = \mathbb{F}_p^n$. K_2 можно рассматривать, как векторное пространство некоторой размерности d над полем K_1.

А это значит, что K_2 имеет $|K_1|^d = p^n$ элементов, то есть $p^n = (p^m)^d$, что и означает $m \mid n$.

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

2.4 Корни многочленов над конечным полем

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

Определение 2.15. *Минимальным многочленом (м. м.)* элемента $\beta \in \mathbb{F}_p^n$ называется нормированный многочлен $m_\beta(x) \in \mathbb{F}_p[x]$ наименьшей степени, для которого β является корнем.

Сразу заметим, что минимальный многочлен для x можно получить из порождающего поле неприводимого. Для этого рассмотрим поле $F = \mathbb{F}_p[x]/(a(x)) \cong \mathbb{F}_p^n$, порождаемое неприводимым многочленом

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

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

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

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

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

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

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

Теорема 2.16. *Для каждого элемента β поля $\mathbb{F}_p^n$ существует м. м., и его степень не превосходит n.*

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

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

Поэтому β — корень многочлена

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

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

Теорема 2.17. *Минимальные многочлены неразложимы.*

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

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

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

$$m_\beta(\beta) = 0$$

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

Теорема 2.18. *Пусть $m_\beta(x)$ — м. м. для элемента β в некоторого поля Галуа, а $f(x)$ — многочлен имеющий β своим корнем. Тогда $m_\beta(x) \mid f(x)$.*

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

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

Подставляя в это равенство β вместо x, получаем

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

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

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

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

Определение 2.19. Минимальный многочлен примитивного элемента поля называется *примитивным многочленом.*

Ясно, что данный 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 2.20. 1. Многочлен

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

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

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

2. Для своего корня x многочлен

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

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

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

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

Теорема 2.21. *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 $(\mathbb{F}_p^n)^*$.

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

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

Теорема 2.22 (о делимости биномов). *В любом кольце многочленов*

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

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

- Если $m \vdots n$, то $m = kn$ и имеем
$$x^m - 1 = y^k - 1 = (y-1)\cdot(y^{k-1} + y^{k-2} + \ldots + y + 1).$$

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

□

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

Пример 2.23. 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 2.24. *Все неприводимые многочлены n-й степени над $\mathbb{F}_p$ делят бином $x^{p^n} - x$.*

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

$\underline{n > 1}$. 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 и $f(x)$, и, по теореме 2.21, бинома $x^{p^n-1} - 1$.

По свойствам м. м. (утверждение 2.18) бином $x^{p^n-1} - 1$ делится на $f(x) = m_x(x)$. □

Пример 2.25. Возвращаемся к разложению бинома $x^{15} + 1 \in \mathbb{F}_2[x]$.

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

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

Таким образом,

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

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

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

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

Теорема 2.26. *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. Из тождества Фробениуса (см. теорему 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 $n \geqslant k$. □

Корни неприводимого многочлена

Теорема 2.27 (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 $n > 1$.

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

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

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

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

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

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

Будем пользоваться далее свойствами сравнения.

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

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

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

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

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

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

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

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

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

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

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

Действительно, если в поле $\mathbb{F}_p^k \cong \mathbb{F}_p[x]/(\varphi(x))$, $\deg\varphi(x) = k < n$ многочлен $f(x)$ имеет корень β, то $\varphi(x) \mid f(x)$. Поэтому многочлен $f(x)$ имеет своим полем разложением поле $\mathbb{F}_p[x]/(f(x))$. Далее применяем теорему 2.27.

Пример 2.28. 1. Найдём корни неприводимого над $\mathbb{F}_2$ многочлена

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

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

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

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

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

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

1) $\beta^{p^d} = \beta$, и тогда
$$m_\beta(x) = (x-\beta)\cdot(x-\beta^p)\cdot\ldots\cdot\left(x-\beta^{p^{d-1}}\right).$$
2) $\beta^{p^d} = x$, и тогда $m_\beta(x)$ есть многочлен $a(x)$ после нормировки, как и для случая $\beta = x$.

Пример 2.29. Найдём минимальные многочлены для элементов
$$\beta_1 = x^2 + x \quad \text{и} \quad \beta_1 = x + 1$$
поля $\mathbb{F}_2[x]/\left(x^4 + x + 1\right)$.

В этом поле $x^4 = x + 1$.

1. $\underline{\beta = \beta_1 = x^2 + x}$. Вычисляем элементы, сопряжённые с β:
$$\beta^2 = \left(x^2+x\right)^2 = x^4 + x^2 = x^2 + x + 1,$$
$$\beta^4 = \left(x^2+x+1\right)^2 = x^4 + x^2 + 1 = x + \cancel{1} + x^2 + \cancel{1} = x^2 + x = \beta.$$

Таким образом $m_\beta(x)$ — квадратный многочлен и
$$m_\beta(x) = (x-\beta)(x-\beta^2) = x^2 + \left(\beta^2+\beta\right)x + \beta^3.$$
Вычисляем коэффициенты этого многочлена:
$$\beta^2 + \beta = \left(x^2+x+1\right) + \left(x^2+x\right) = 1,$$
$$\beta^3 = \left(x^2+x+1\right)\cdot\left(x^2+x\right) = \ldots = (x+1) + x = 1.$$

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

2. $\underline{\beta = \beta_2 = x + 1}$. Элементы, сопряжённые с β:
$$\beta^2 = x^2 + 1, \quad \beta^4 = x^4 + 1 = x + 1 + 1 = x,$$
поэтому $m_\beta(x) = x^4 + x + 1$.

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

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

Теорема 2.30 (Гаусс). $$\sum_{d|n} d \cdot I_p^d = p^n.$$

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 линейных над $\mathbb{F}_2$ многочлена: x и $x+1$. Отсюда $I_2^7 = (128-2)/7 = 18$.

Из формулы Гаусса имеются важные

Следствия.

1. Простая оценка ($p \geqslant 2$, $n \geqslant 2$)

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

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

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 $n>1$ —

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

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

Теорема 2.31.

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

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

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

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

2.5 Циклические подпространства колец вычетов

Идеалы в кольцах классов вычетов. 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 2.32. *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. 18).

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 2.33. 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 $\mathcal{R} = \mathbb{F}_p[x]/(x^n - 1)$. 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:

$$\begin{aligned}\left(a_0 + a_1 x + \ldots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}\right) \cdot x \;&= \\ = a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{=1} \;&= \\ = a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1}.&\end{aligned}$$

Поэтому $\mathcal{R}$ называют *циклическим полиномиальным кольцом.*

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

Теорема 2.34. *Подпространство I кольца $R = \mathbb{F}_p[x]/(x^n - 1)$ является циклическим если и только если оно идеал.*

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

Обратно, пусть I — циклическое подпространство кольца 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. □

Пример 2.35. 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 $R = \mathbb{F}_2[x]/\big(x^4 - 1\big)$ все кратные φ многочлены имеют вид

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

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

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

Пусть $n = t \cdot p$. Поскольку тогда $x^{tp} - 1 = (x^t - 1)^p$, то корнями бинома $x^n - 1$ будут все корни $x^t - 1$ 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 неприводимых многочленов:

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

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

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 d, то β^p, β^{p^2}, $\ldots$ $\beta^{p^{d-1}}$ — также его корни. Отсюда следует, что величины k и $d_1, \ldots, d_k$ можно найти, разбив элементы $\mathbb{Z}_n$ на *орбиты* отображения $\ell \mapsto p\ell \pmod{n}$.

Пример 2.36. 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. Конкретно разложение было найдено ранее (см. с. 59).

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 многочленов: одного линейного (очевидно, это $x + 1$), одного квадратного (очевидно, это $x^2 + x + 1$) и некоторого неприводимого 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 $x^{23}-1$ разлагается в произведение одного линейного многочлена и двух неприводимых многочленов 11-й степени.

2.6 Задачи

2.1. Построить все изоморфизмы между мультипликативной группой поля $\mathbb{F}_7$ и аддитивной группой $\mathbb{Z}_6$.

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*) $a = 20989$, $b = 2573$.

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

2.4. Решите сравнение

а) $7x = 11 \pmod{25}$;

б) $9x = 3 \pmod{10}$;

в) $6x + 2 = 3 \pmod{7}$;

г) $6x + 2 = 3 \pmod{9}$;

д) $6x + 2 = 4 \pmod{9}$;

е) $6x + 1 = 4 \pmod{9}$.

2.5. 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.

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

2.7 (Теорема Вильсона). Доказать, что

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

2.8. Построить поле из 4-х элементов.

2.9. В кольце $\mathbb{Z}_2[x]$ найти

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

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

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

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

5) найти минимальные многочлены всех элементов поля.

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

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

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

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

2.15. Многочлен

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

разложить на неприводимые множители.

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

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

2.18. Определить, является ли:

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

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

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

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

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

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

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

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

2.22. Найти количество нормированных неприводимых многочленов

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

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

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

С её помощью вычислить выражение

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

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

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

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

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

2.27. Разложить на неприводимые множители многочлен

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

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

2.29. Найти м. м. для всех элементов β поля

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

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

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

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

2.32. Примитивен ли элемент x в полях

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

2.33. Найти корни многочлена

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

2.34. Является ли многочлен

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

примитивным?

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

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

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

2.37. Найти корни многочлена

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

2.38. Найти корни многочлена

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

2.39. Найти корень многочлена

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

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

Глава 3

Коды, исправляющие ошибки

3.1 Блоковое кодирование

Задача помехоустойчивого кодирования. 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 случайно, независимо и с равными вероятностями могут оказаться инвертированными, но вставок или выпадения битов нет (*двоичный симметричный канал*).

Задача: обеспечить автоматическое исправление ошибок, построив *помехозащищённый код*, и имеющий, по возможности, простые алгоритмы кодирования и декодирования.

Началом теории корректирующих кодов считается 1948 г., когда была опубликована статья Клода Шеннона «Математическая теория связи». В ней і. а. Шеннон установил, что по каналу связи информация может передаваться безошибочно в том случае, если скорость передачи не превышает пропускной способности канала. Однако теорема Шеннона является теоремой чистого существования и не дает конкретных методов построения кодов.

Подход к решению (один из возможных!):

1. Весь поток информации разбить на *сообщения* — последовательные непересекающиеся блоки фиксированной длины k.
2. Каждый блок *кодировать* (модифицировать) —

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

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

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

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

[1)] иногда именно это отображение и называют кодом

Кодирование, при котором биты сообщения переходят в заранее фиксированные позиции кодового слова, называют *разделимым*. 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, m/n — его *избыточность*.

Впервые конструктивный метод построения кодов с избыточностью, способных корректировать одиночные ошибки и простым декодированием, предложил Ричард Хэмминг (R. W. Hamming, 1915–1998) в 1950 г.

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

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

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

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

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

Увеличение m при данном k ведёт к увеличению кодового расстояния (как конкретно — очень трудный 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 одному биту, то есть пространство сообщений есть $S=\{0,1\}$.

Код с повторением $a \mapsto \overbrace{a\ldots a}^{2r+1 \text{ раз}}$, очевидно, исправит до r ошибок. Простейший его вариант — *утраивание*: $0 \mapsto 000$, $1 \mapsto 111$.

Ясно, что код с повторением содержит $m=2r$

проверочных символов, и с точки зрения минимизации m крайне неэффективен.

2. *Код с одной проверкой на чётность*, содержащий только один проверочный символ, являющийся суммой по модулю 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 слово не декодируется. Таким образом, любое нечётное число ошибок приводит к отказу от декодирования, и тем самым ошибки обнаруживаются.

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

Рассмотренные коды представляют собой в некотором смысле «предельные случаи» двоичного кодирования. Коды с повторением имеют огромную корректирующую способность, но каждый блок содержит только один информационный символ. Коды с одной проверкой на чётность обладают очень высокой скоростью, но способны только обнаруживать и только нечётное число ошибок.

Кодирование. Все векторы далее мы будем считать вектор-строками, как принято в литературе о кодировании. Обозначения:

- сообщение — вектор

$$\boldsymbol{u} = [u_1, \ldots, u_k] \in \{0,1\}^k = S;$$

- кодовое слово — вектор $\boldsymbol{v} \in \{0,1\}^n = B^n$;

- совокупность C всех кодовых слов — $[n,k]$-*код*, или, с кодовым расстоянием — $[n,k,d]$-*код*[2)].

Пример 3.2. Избыточный код $[5,2]$-код мощности $Q=4$:
$C=\{\,\boldsymbol{c}_1=[\,00000\,],\ \boldsymbol{c}_2=[\,10101\,],\ \boldsymbol{c}_3=[\,01110\,],\ \boldsymbol{c}_4=[\,11011\,]\,\}$.

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 ошибочных битах и 0 в остальных.

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

1-й этап. Определение кодового слова $\widehat{\boldsymbol{v}}$ как *ближайшего* в метрике Хэмминга слову к $\boldsymbol{w}$, то есть нахождение центра соответствующего шара — *декодирование по максимуму правдоподобия* (MLD, maximum likelihood decoding, задача NCP, nearest code problem).
Если произошло не более $r=\lfloor\,(d-1)/2\,\rfloor$, ошибок, где d — известное кодовое расстояние, то $\widehat{\boldsymbol{v}}=\boldsymbol{v}$.

2-й 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.

[2)] В общем случае не все векторы дины k включаются в код и он имеет мощность $Q<2^k$. Для таких кодов используют обозначение (n,Q,d). Обозначения $(n,Q,d)_q$ и $[n,k,d]_q$ используют для q-ичных кодов.

Ясно, что 1-й этап может быть выполнен по таблице декодирования. Кодовые слова образуют первую строку этой таблицы. Если получено некоторое кодовое слово, естественно предположить, что было передано именно оно. Под каждым кодовым словом задан перечень возможных принятых слов, которые могут декодироваться в это кодовое слово. При этом каждое возможное принятое слово появляется в таблице только один раз.

Понятно, что таблица декодирования имеет размер порядка $2^{n-k} \times 2^k$. 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 значения n и k могут достигать *сотен тысяч*.

Приняв некоторые ограничения на множество кодовых слов, можно сократить объёмы вычислений при кодировании/декодировании. Эти ограничения приводят к использованию кодов специального вида: *линейных*, а из линейных — *циклических*.

Плотная упаковка шаров в единичный куб

Теорема 3.3 (Хэмминг). *Максимальная мощность Q 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*.

Нижнюю границу для Q установил в 1952 г. американский математик *Э. Гильберт* (E. N. Gilbert, 1923–2013, не путать со знаменитым немецким математиком Д. Гильбертом), а верхняя граница впервые была приведена в работе 1947 г. индийского математика и статистика *К. Р. Рао* (C. R. Raj, 1920) и лишь в 1950 г. — в работе *Р. Хэмминга*.

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

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

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

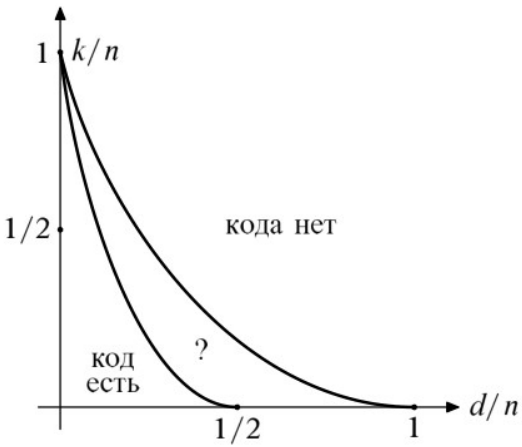


Рис. 3.1. Границы Гильберта (левая) и Хэмминга (правая) для $n \gg 1$.

Чтобы построить блоковый $[n, k]$-код, исправляю-

щий 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 коды, такое удаётся только в следующих случаях, когда получаются *совершенные* или *экстремальные коды*:

1) $n = 2^m - 1$, $r = 1$ — *коды Хэмминга*; у них $k = 2^m - 1 - m$, $m = 2, 3, \ldots$;
2) $n = 23$, $r = 3$ — *код Голея* (см. с. 97), у него $k = 12$ и $m = 11$;
3) $[n, n-1, 2]$ — коды с проверкой на чётность.

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 $Q = 4 < \frac{2^5}{1+5} = 5\frac{1}{3}$.

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

Образуем сначала единичную матрицу порядка

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

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

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

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

Просуммировав по $\mathrm{mod}\ 2$ все совокупности строк таблицы и добавив нулевую строку, получим мощность кода

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

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

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 $3 = d$.

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

Данный код содержит $Q = 2^4 = 16$ кодовых слов построенного $[7, 4, 3]$-кода Хэмминга.

3.2 Линейные коды

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

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 называется *линейным*, если он образует линейное векторное подпространство V размерности k координатного пространства W всех потенциально возможных принятых слов, символически $V \leqslant \{0, 1\}^n = W$.

Линейный код обладает следующими свойствами.

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

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

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

2. Кодовое расстояние d группового 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 двоичных разделимых линейных $[n, k, d]$-кодов легко получить оценку Синглтона: $d \leqslant n - k + 1$. Действительно, кодовое слово, соответствующее сообщению веса 1, содержит не

более $n-k+1$ единиц: одну в информационных разрядах и максимально — во всех $n-k$ проверочных (возможность преобразования произвольного линейного кода к систематическому виду показана ниже).

К сожалению, не существует двоичных нетривиальных систематических кодов, для которых *граница Синглтона* (равенство в приведённом неравенстве) достигается.

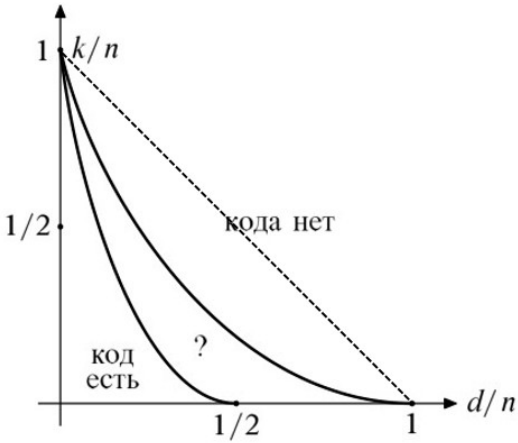


Рис. 3.2. Границы Гильберта, Хэмминга и Синглтона (пунктир) для $n \gg 1$.

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

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

Порождающая матрица. Составим из векторов некоторого базиса кода матрицу

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

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

$$\boldsymbol{v} = \boldsymbol{u}G. \tag{3.1}$$

Пример 3.9. Линейный код из примера 3.2 порождается матрицей

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

Некоторые операции над строками порождающей матрицы G не изменяют всего подпространства

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

кодовых слов. Таковыми, очевидно, являются любая перестановка строк и сложение любой линейной комбинации некоторых строк с произвольной строкой. Эти операции называют *элементарными*.

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

$$G = [\ I_k\ P_{k\times m}\ ],$$

где I_k — единичная матрицы порядка k. Такую формы порождающей матрицы называют *канонической* (*или приведённо–ступенчатой*). При кодировании такой матрицей первые k бит сообщения перейдут

в первые биты кодового слова, обеспечивая систематическое кодирование.

Если к элементарным операциям добавить возможность перестановки столбцов матрицы, то эта операция изменит не только базис, но и порождаемый код. Однако новое подпространство будет обладать теми же метрическими свойствами, что и исходное: все попарные расстояния между его векторами останутся прежними. Коды, полученные комбинациями таких преобразований называют *эквивалентными*.

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

Пример 3.10. Код из примеров 3.2 и 3.9 порождается также матрицей G', получающейся из G перестановкой первых двух столбцов.

Пример 3.11. В примере 3.5 была получена таблица, сложением различных совокупностей строк которой получаются все кодовые слова некоторого кода Хэмминга. Она и является порождающей матрицей $G_{4\times 7}$ данного кода.

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

Напомним, что для того, чтобы узнать кодовое

расстояние линейного кода, в общем случае необходимо *перебрать все кодовые слова*. Для этого можно умножить по (3.1) все, кроме нулевого, векторы сообщений $\boldsymbol{u}$ на порождающую матрицу и определить минимальный вес полученных кодовых слов.

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

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

У данного кода $\dim C = k$ и $\dim C^\perp = n-k = m$. При этом $W = \{0,1\}^n$ *не есть прямая сумма* подпространств C и $C^\perp$: произвольный вектор из W может либо не разлагаться, либо разлагаться неоднозначно в сумму векторов из C и $C^\perp$. Причиной этих «странностей» является то, что из ортогональности системы векторов $\{0,1\}^n$ не следует их линейной независимости, как это имеет место в евклидовом пространстве.

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

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

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

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

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

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

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

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

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

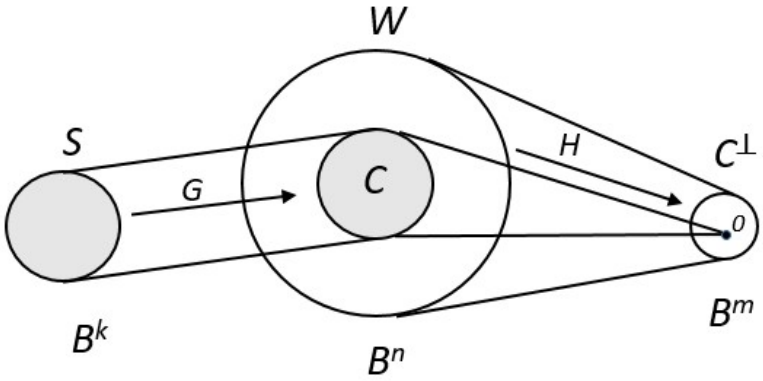


Рис. 3.3. Преобразования: G — сообщений в линейный код C и H — принятых слов в $C^{\perp}$.

ведливо

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

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

Рассмотрим линейный $[n, k]$-код. Пусть его порождающая матрица $G_{k\times n}$ имеет каноническую форму $G = [\ I_k\ P_{k\times m}\ ]$. Тогда проверочной матрицей этого кода будет

$$H = [\ P^T_{m\times k}\ I_m\ ],$$

где I_m — единичная матрицы порядка m.

Действительно, в этом случае

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

— нулевая $k \times m$-матрица.

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

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

Пример 3.12. Для построенной в примере 3.11 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 C 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 3.13. 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* с помощью элементарных преобразований *строк* выделим в матрице G единичную подматрицу порядка 3 (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 биты 1, 2, 3 сообщения последовательно 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 $P_{3\times3}$ из столбцов G', *отличных от столбцов единичной подматрицы* —

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

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

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

3. Найдем кодовое расстояние d. Для этого закодируем все ненулевые сообщения $\boldsymbol{u}_1$, …, $\boldsymbol{u}_7$ и найдем минимальный хэммингов вес полученных 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[3] в 1949 г. обнаружил, что

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

Это позволило предположить, что существует совершенный $[23, 12, 7]$-код 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 выполняется только для кодов Хэмминга, Голея и тривиальных.

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

3.3 Декодирование линейных кодов

Конечная цель 1-го, наиболее сложного этапа декодирования — определить, какое кодовое слово передавалось. Однако оказывается легче ответить сначала на промежуточный вопрос: «Каков вектор $\boldsymbol{e}$ ошибок, произошедших в канале?»

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

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

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

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

(очевидно, $\boldsymbol{s}$ — вектор-столбец).

Определение 3.14. *Синдром слова* $\boldsymbol{w}$, принятого при передаче сообщения, закодированного линейным кодом с проверочной матрицей H и, возможно, содержащего ошибки, называют вектор $\boldsymbol{s} = H\boldsymbol{w}^T$.

Синдром в общем смысле — совокупность явлений, вызванных отклонением от нормы.

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, как видно из (3.3), вектор ошибок $\boldsymbol{e}$ удовлетворяет неоднородной недоопределенной СЛАУ

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

а кодовые слова являются решениями соответствующей однородной системы (3.2).

Таким образом, вектор $\boldsymbol{e}$ может быть представлен как частное решение неоднородной системы (3.4) и общее решение однородной (3.2).

Определение ошибок по синдрому. 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 возможным синдромам $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{2^m}$, а каждая строка содержит *наиболее вероятный вектор ошибок*, данному синдрому соответствующий. Этот вектор должен иметь наименьший вес среди возможных решений системы (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 3.15. 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	$[00]^T$
Другие	1000	0010	1111	0101	$[10]^T$
смежные	0100	1110	0011	1001	$[11]^T$
классы	0001	1011	0110	1100	$[10]^T$
	лидеры				*синдромы*

Первый столбец содержит лидеры смежных классов, последний — синдромы.

Пусть исходное сообщение есть $\boldsymbol{u} = [10]$. Тогда соответствующее ему кодовое слово есть $\boldsymbol{v} = [1010]$.

Пусть ошибка произошла во 2-м разряде и получено слово $\boldsymbol{w} = [1110]$. Его синдром: $\boldsymbol{s} = H\boldsymbol{w}^T = [11]^T$.

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

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

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 $r = \left\lfloor \frac{d-1}{2} \right\rfloor$ 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, пусть необходимо передать сообщение $\boldsymbol{u} = [\,00\,]$, и тогда по каналу связи будет передаваться кодовое слово $\boldsymbol{v} = [\,0000\,]$.

Пусть при передаче произошла ошибка в 3-м разряде и принято слова $\boldsymbol{w} = [\,0010\,]$. Соответствующий ему синдром есть $\boldsymbol{s} = [\,10\,]^T$. По таблице будет установлен вектор ошибки $\boldsymbol{e} = [\,1000\,]$ как лидер смежного класса, имеющий этот синдром. Тогда передаваемое кодовое слово будет восстановлено неверно:

$$\widehat{\boldsymbol{v}} = \boldsymbol{w}+\boldsymbol{e} = [\,0010\,]+[\,1000\,] = [\,1010\,] \neq \boldsymbol{v} = [\,0000\,].$$

В результате получатель информации ошибочно посчитает, что было передано сообщение $[\,10\,]$.

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 большими параметрами становится практически невозможным найти лидеров смежных классов. Так, например, линейный

$[50, 20]$-код над 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* 3.12 получена матрица

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

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

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

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

Пример 3.16. 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

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

указывает позицию ошибки.

Для кода Хэмминга решить задачу декодирования несложно. Для линейного кода общего вида нужно решать задачу MLD: по данному вектору с ошибкой найти ближайшее кодовое слово. Декодировать произвольный линейный код, что является NP-сложной задачей.

Дуальные коды. Заметим, что 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, кода $H = G$. Такие коды называют *самодуальными*. Все самодуальные коды — чётной длины.

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

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

самодуален.

3.4 Циклические коды

Определение и построение циклических кодов

Определение 3.17. Блоковый код называется *циклическим*, если он инвариантен относительно циклических сдвигов своих кодовых слов.

Впервые их в 1957–58 годах построил американский учёный *Е. Прейндж* (Eugene August Prange, 1917–2006).

Заметим, что циклические коды не обязательно линейные. Далее будем рассматривать только линейные циклические коды.

Теорема 2.34 утверждает, что циклическое пространство образуют элементы идеала I в кольце классов вычетов по модулю многочлена $x^n - 1$. Такой идеал в кольце $\mathbb{F}_p[x]/(x^n - 1)$ задаётся делителем $g(x)$ бинома $x^n - 1$: элементы I суть многочлены из $\mathbb{F}_p[x]$, кратные $g(x) \pmod{x^n - 1}$.

Имеется биективное соответствие векторов и полиномов, введённое на с. 50. Например, соотношение, описывающее элементы образованного циклического пространства есть

$$\boldsymbol{v} = [\ v_0\ v_1\ \ldots\ v_{n-1}\ ] \leftrightarrow$$
$$\leftrightarrow\ v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}.$$

Поэтому построить двоичный циклический $[n, k]$-код[4)] можно следующим образом.

1. Задаёмся нечётным значением n и выбираем *любой* делитель $g(x)$ бинома $x^n - 1$; понятно,

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

что $\deg g(x) = m < n$.
Многочлен $g(x)$ полностью задаёт циклический код, его называют *порождающим* данный код или его *генератором*.

2. Идеал $(g(x))$ кольца $R = \mathbb{F}_2[x]/(x^n - 1)$ состоит из всех многочленов вида
$$f(x) \cdot g(x), \quad 0 \leqslant \deg f(x) < n - m = k.$$
Многочлены из этого идеала задаются *векторами своих коэффициентов, которые и будут кодовыми словами*.

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

Пример 3.18. Построим циклический код длины $n = 23$. В п. 2 примера 2.36 найдены число и степени неприводимых многочленов, факторизующих бином $x^{23} - 1$. Конкретно это разложение таково:
$$f(x) = (x+1)(\underbrace{x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1}_{g_1(x)}) \times \\ \times (\underbrace{x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1}_{g_2(x)}).$$

Поскольку степени полиномов $g_1(x)$ и $g_2(x)$ оказались равными $m = 11$, для построения $(23, 12)$-кода может быть выбран любой из них. Можно показать, что в обоих случаях кодовое расстояние оказывается равным 7. Ясно, что построен код Голея, либо двойственный к нему.

Коды Хэмминга могут быть циклическими. Построенная в примере 3.5 таблица 4×7 для кода Хэмминга *не порождает циклического кода.* Однако если переставить 3-элементные окончания некоторых строк, то полученная таблица (см. ниже)

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

уже порождает циклический код.

Кодирование циклическими кодами. Пусть циклический $[n, k]$-код C задаётся порождающим полиномом $g(x)$, делящим бином $x^n - 1$, и $\deg g(x) = m = n - k$.

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий:

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

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

Действительно, умножение $u(x)$ на x^m поместит сообщение в старшие в k разрядов n-битного кодового 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 3.19. 1. Построим циклический код длины $n = 7$.

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени его неприводимых делителей, для чего применим способ разбиения $\mathbb{Z}_7$ на орбиты относительно умножения на 2 (см. с. 69):

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

С учётом теорем 2.21 и 2.27, заключаем, что все 7 ненулевых элементов $\alpha^0 = 1, \alpha, \ldots, \alpha^6$ поля разложения бинома $x^7 - 1$, или, что то же, его корни, разбиваются на классы сопряжённых корней

$$C_0 = \left\{\alpha^0\right\},\ C_1 = \left\{\alpha, \alpha^2, \alpha^4\right\},\ C_2 = \left\{\alpha^3, \alpha^6, \alpha^5\right\}. \tag{3.5}$$

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

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

В качестве порождающего полинома $g(x)$ выберем

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

Тогда $m = 3$, $k = 4$, и будет построен циклический $(7, 4)$-код.

Заметим, что при выборе $g(x) = x + 1$ получаем код с проверкой на чётность; при выборе, например

$g(x) = (x+1)\left(x^3+x+1\right)$ — расширенный код Хэмминга; при выборе $g(x) = x^7 - 1$ — тривиальный код $(k = 0)$.

2. Закодируем несистематическим и систематическим кодированием сообщение

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

Несистематическое кодирование.

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

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

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

то есть $r(x) = x$ и поэтому

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

Декодирование циклических кодов

Определение 3.20. *Синдромом $s(x)$ слова $w(x)$*, принятого при передаче сообщения, закодированного циклическим кодом, называют остаток от деления $w(x)$ на многочлен $g(x)$, порождающий код.

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

3.5 Коды БЧХ. Кодирование

Коды Боуза-Чоудхури-Хоквингема (BCH, БЧХ) — подкласс циклических кодов, исправляющих *не менее заранее заданного* числа ошибок[5)].

Циклотомические классы

Определение 3.21. Ненулевые элементы поля $\mathbb{F}_p^t$, имеющие общий минимальный многочлен, называют *сопряженными*.

Все сопряжённые элементы составляют *циклотомический класс*.

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

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* $\mathbb{F}_p$.

Поскольку в поле характеристики p значения любого полинома в точках α и α^p одинаковы, то циклотомические классы можно получать возведением в степень p какого-то одного его элемента. Это совпадает с построением орбиты отображения (см. с. 70)

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

элементов мультипликативной группы $\mathbb{Z}_{p^t-1}$. Нас интересует случай $p = 2$.

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

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

Пример 3.22. Пусть $t = 4$ и α — примитивный элемент поля $F = \mathbb{F}_2^4$. Тогда мультипликативная группа

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

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

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

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

Если требуется исправлять не менее r ошибок, зададимся *конструктивным расстоянием*

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

Степени α, α^2, α^3, ..., α^{2r} примитивного элемента α поля $\mathbb{F}_2^t$ называют *нулями кода*.

Код БЧХ есть циклический $[n, k, d]$-код, в котором порождающий многочлен $g(x)$ *является полиномом минимальной степени, имеющим корнями все нули кода*. Как и у всех циклических кодов, для него $\deg g(x) = m = n - k$, 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 суть также корни любого кодового слова.

Определение 3.23. *Синдромами* s_1, ..., s_{2r} принятого полинома $w(x)$ при кодировании БЧХ-кодом с нулями α, ..., α^{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 $i = 1$, ..., $\delta - 1$ 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 $x^n - 1$, $k = n - \deg g(x)$.

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 α, α^2, …, α^{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 3.24. Выберем $t = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

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

Поскольку многочлен $a(x)$ — примитивный, и, согласно (3.5), F^* разбивается на следующие циклотомические классы ($\alpha = x$):

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

Для построения кодов, исправляющих заданное количество ошибок, необходимо определить соответствующий порождающий полином. Ясно также, что при вычислениях в этом поле имеем $\alpha^3 = \alpha + 1$.

1. *Код БЧХ длины $n = 7$, исправляющий $r = 1$ ошибку.* В этом случае $2r = 2$ и нули кода α, α^2 попадают в один циклотомический класс C_1.

Минимальный многочлен элементов этого класса — $a(x)$, поэтому порождающий полином $g(x) = g_1(x) = a(x)$, $m = 3$, и в результате получаем уже известный $[7, 4, 3]$-код Хэмминга (см. пример 3.19).

2. *Код БЧХ длины $n = 7$, исправляющий не менее $r = 2$ ошибок.* Теперь $2r = 4$. Нули строящегося кода α, α^2, α^3, α^4 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 $g_2(x)$:

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

Таким образом $g_2(x)=x^3+x^2+1$[6] и

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

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

Пример 3.25. Попытаемся построить лучшие коды, взяв бóльшие их длины: выберем $t=4$ и тогда длина кода $n=2^4-1=15$.

Рассмотрим поле $F=\mathbb{F}_2[x]/(a(x))\cong\mathbb{F}_2^4$, образованное некоторым неприводимым многочленом $a(x)$ степени $t=4$. Тогда F^* относительно своего примитивного элемента α, как показано в примере 3.22, разобьётся на 5 циклотомических классов над $\mathbb{F}_2$:

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

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

В качестве многочлена 4-й степени, определяющего конкретное поле F, возьмём примитивный многочлен

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

который одновременно является м. м. для порождающего элемента $\alpha = x$ и всего класса C_1. В данном поле $\alpha^4 = \alpha + 1$.

1. *Код БЧХ длины $n = 15$, исправляющий не менее 2 ошибок.* В этом случае $2r = 4$, и нули α, α^2, α^3, α^4 конструируемого кода располагаются в циклотомических классах C_1 и C_2.

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

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

Тогда порождающий полином кода есть

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

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

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

Минимальные многочлены для C_1 и C_2 уже найдены. Далее, очевидно $g_3(x) = x^2 + x + 1$, поскольку это

единственный неприводимый квадратный многочлен над $\mathbb{F}_2$. Тогда порождающий полином есть

$$g(x) = g_1(x) \cdot g_2(x) \cdot g_3(x) = \\ = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1. \quad (3.6)$$

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 3.26. Рассматриваем $[7, 4]$-код Хэмминга, построенный в примере 3.19 для циклических кодов, где был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [\,0\,0\,1\,1\,]$:

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

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:

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

Определим значение j, для которого $\alpha^j = s$:

$$\begin{aligned} \alpha^0 &= 1, & \alpha^3 &= \alpha + 1, \\ \alpha^1 &= \alpha, & \alpha^4 &= \alpha(\alpha+1) = \alpha^2 + \alpha, \\ \alpha^2 &= \alpha^2, & \alpha^5 &= \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 = s \end{aligned}$$

и 5-я позиция ошибки определена верно.

Декодирование кодов БЧХ: общий случай. Рассмотрим $[n, k, d]$-код БЧХ длины $n = 2^t - 1$, при построении которого для определения порождающего полинома использовалось поле

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

с примитивным элементом (нулём кода) α.

Пусть при передаче кодового слова произошло

$$\nu \leqslant r = \lfloor (d-1)/2 \rfloor \ \text{ ошибок в позициях } \ j_1, \ldots, j_\nu,$$

которые и нужно определить.

Тогда *полином ошибок* есть

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

Вычислим синдромы принятого полинома $w(x)$:

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

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

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

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

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

Перепишем полученную систему как зависимости с введёнными переменными:

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

Определим *полином локаторов ошибок*

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

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

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

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

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

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

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

Данные равенства представляют собой СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$.

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

Например, декодер PGZ (Peterson-Gorenstein-Zierler) состоит в последовательных попытках решения данных соотношений для $\nu = r, r-1, \ldots$ до тех пор, пока матрица очередной СЛАУ не окажется невырожденной.

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

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

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

Алгоритм декодирования $[n, k, d]$-кода БЧХ

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

1. Найти все синдромы $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$; если все они равны 0, то считаем, что ошибок нет, $v(x) = w(x)$, и переходим к пункту 6.

2. Используя тот или иной декодер, найти полином локаторов ошибок $\sigma(x)$; число ν произошедших ошибок равно его степени.

3. Найти все корни $\sigma(x)$, например, перебором всех элементов F^*; пусть эти корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.

4. Найти позиции ошибок $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.

5. Найти полином ошибок $e(x) = x^{j_1} + \ldots + x^{j_\nu}$ и восстановить кодовое слово $v(x) = w(x) + e(x)$.

6. По $v(x)$ восстановить переданное сообщение $u(x)$.

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

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

где s_i — синдромы, $i = \overline{1, 2r}$ и, формально, $s_0 = 1$ и $s_i = 0$ при $i > 2r$.

Перемножив введённые полиномы, получим *полином значений ошибок*:

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

Его коэффициенты определяются соотношением для произведения многочленов —

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

Замечаем, что значения λ_i по данной формуле для $i = \nu + 1, \ldots, 2r$ суть левые части соотношений Ньютона-Жирара $(*)$, то есть все они равны 0. Значит полином значений ошибок имеет нулевую «среднюю часть».

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

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

Это означает, что

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

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

Ключевое уравнение имеет вид (2.1). Это позволяет записать его в виде соотношения Безу

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

которое может быть решено обобщённым алгоритмом Евклида в кольце $\mathbb{F}_2[x]/(x^{2r+1})$ с условием останова «*степень очередного остатка не более* r» и опусканием заключительного шага нормировки (см. с. 47).

Пример 3.27. Рассматриваем $[15, 5, 7]$-код БЧХ с полем разложения $\mathbb{F}_2[x]/\big(x^4 + x + 1\big) \;=\; F$, построенный в п. 2 примера 3.25. При вычислениях будем пользоваться таблицей со с. 52.

Пусть передаётся сообщение

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

При систематическом кодировании порождающим полиномом (3.6) кодовым словом (опустим этот этап) будет

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

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

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

1. Найдём все $2r = 6$ синдромов:

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

Таким образом, синдромный полином есть

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

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

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

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

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

$$
\begin{aligned}
\text{Шаг 2.}\quad & r_{-1}(x) = r_0(x)q_1(x) + r_1(x),\\
& q_1(x) = \alpha^8 x + \alpha^2,\\
& r_1(x) = \alpha^{14}x^4 + \alpha^3 x^3 + \alpha^2 x^2 + \alpha^{11}x,\\
& \qquad \deg r_1(x) = 4 > 3 = r,\\
& \sigma_1(x) = \sigma_{-1}(x) + \sigma_0(x)q_1(x) =\\
& \qquad = \alpha^7 x^2 + \alpha^{11}x.\\
\text{Шаг 3.}\quad & r_0(x) = r_1(x)q_2(x) + r_2(x),\\
& q_2(x) = \alpha^9 x,\\
& r_2(x) = \alpha^5 x + \alpha^{13},\\
& \qquad \deg r_2(x) = 1 \leqslant 3 = r,\\
& \sigma_2(x) = \sigma_0(x) + \sigma_1(x)q_2(x) =\\
& \qquad = \alpha x^3 + \alpha^5 x^2 + \alpha^{14}x + \alpha^{13}.
\end{aligned}
$$

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

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

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

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

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

Первый корень 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

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

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

Коды БЧХ: общий взгляд. Коды БЧХ получили широкое распространение. Это обусловлено следующими основными причинами.

1. Среди кодов БЧХ существуют коды с хорошими корректирующими свойствами и низкой избыточностью.
2. Известны достаточно эффективные методы их кодирования и декодирования.

   При этом никаких более эффективных способов вычисления корней многочлена локаторов ошибок, кроме полного перебора (т. н. *процедура Ченя*) до сих пор не найдено.
3. В методическом плане коды БЧХ обладают относительно простой и понятной конструкцией, а понимание их структуры облегчает понимание многих других видов циклических кодов.

Перечисленные выше достоинства кодов БЦХ могли бы раз и навсегда поставить точку в выборе помехоустойчивых кодов для широкого круга задач. Однако коды БЧХ являются *асимптотически плохими*: с увеличением длины n кодового слова скорость кода и отношение d/n стремится к нулю.

Известный учёный в области кодирования *Элвин Берлекемп* 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 реализуемого 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*».

3.7 Коды Гоппы

Быстрое введение. Рассмотрим коды, предложенные в 1970 г. советским исследователем В. Д. Гоп-

пой[7]. Он ввёл в рассмотрение очень широкий класс линейных кодов, включающий и все БЧХ-коды [3]. Коды Гоппы вообще говоря, не циклические (а единственные из них циклические — коды БЧХ). При их рассмотрении ограничимся случаем двоичных кодов.

При построении циклических кодов кодовые слова были элементами идеала, задаваемого порождающим многочленом $g(x)$. Для построения кодов Гоппы также используется некоторый многочлен $G(z)$, и сам автор предложил, по аналогии с циклическими кодами, также называть *порождающим*. Коды Гоппы задаются многочленами Однако если по порождающему многочлену циклического кода трудно определить его кодовое расстояние d, то коды Гоппы обладают тем свойством, что для них $d \geqslant \deg G(z) + 1$.

Матрицы, у которых положительны все миноры любого порядка, называют *вполне положительными*. Самой известной вполне положительной матрицей является матрица Вандермонда, и на её основе построены БЧХ-коды. Матрицы вида $\|(x_i - y_i)^{-1}\|$ также являются вполне положительными. Они и лежит в основе кодов Гоппы.

1. Зафиксируем число m; на практике это обычно это 10, 11 или 12.

2. Выберем число $n \leqslant 2^m$. Оно будет длиной кода: все кодовые слова будут принадлежать n-мерному координатному пространство W над $GF(2)$. Это пространство традиционно обозначают V_n, но мы будем использовать привычное нам обозначение.

Часто берут $n = 2^m$.

[7] *Валерий Денисович Гоппа* (1939). Работал в ЦЭМИ, ИППИ и ВЦ РАН. Д. ф.-м. н., лауреат премии IEEE.

3. Рассмотрим расширение m-й степени простого поля Галуа $\mathbb{F}_2$, то есть поле $\mathbb{F}_2^m$. В этом поле выберем конечную последовательность L из n элементов[8)]

$$L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{2^m}.$$

Если $n = 2^m$, то это просто все элементы $GF(2^m)$, которые удобно взять в лесикографическом порядке:

$$L = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\right\},$$

где α — примитивный элемент поля $GF(2^m)$.

4. Определим многочлен

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{F}_2^m[x].$$

5. Выберем число $t \in \left[2, \frac{2^m-1}{m}\right]$ и зафиксируем неприводимый многочлен $G(z)$ степени t. Его называют многочленом Гоппы.

6. Код Гоппы $\Gamma(L, G)$ составляют множество кодовых слов $\boldsymbol{v}$ из W таких, что

$$\Gamma = \Gamma(L, G) = \\ = \left\{ \boldsymbol{v} \in \{0,1\}^n \;\middle|\; \sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \equiv 0 \pmod{G(x)} \right\}.$$

Иначе говоря, Γ — это ядро отображения–«синдрома» $\mathbb{F}_2^n \to (\mathbb{F}_2^m)^t$

[8)] Если все эти элементы различны, получаемый тогда код называют *сепарабельным*.

$$\boldsymbol{w} \leftrightarrow [\, w_0, \ldots, w_{n-1} \,] \mapsto$$

$$\mapsto\ b_0 + b_1 x + \ldots + b_{t-1} x^{t-1} \equiv \sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \pmod{G(x)}.$$

Отсюда следует, что построенный код линейный и число его информационных размер не менее $n - mt$.

Определение. Дадим более подробное и формальное описание построения кодов Гоппы, которое даст возможность описать и проверочную матрицу для них.

Многочлен Гоппы $G(z)$ строят следующим образом. Зададимся длиной n строящегося кода и выберем значение m такое, что $n \leqslant 2^m$. Рассмотрим расширение m-й степени простого поля Галуа $GF(2)$, то есть поле $GF(2^m)$. Заметим, такое обозначение традиционно, и здесь m не есть число избыточных символов кода. В этом поле выберем n элементов[9)], обозначив их совокупность через L:

$$L = \{\, \alpha_1, \ldots, \alpha_n \,\} \subseteq GF(2^m).$$

L называют множеством *нумераторов позиций* кодового слова.

Выберем многочлен $G(z)$ степени t с коэффициентам из $GF(2^m)$ такой, что *среди корней которого нет элементов из* L:

$$G(\alpha_i) \neq 0, \quad i = \overline{1, n}.$$

[9)] Если все эти элементы различны, получаемый тогда код называют *сепарабельным*.

Многочлен $G(z)$ называют *многочленом Гоппы*. Обратите внимание, что коэффициенты многочлена Гоппы есть элементы расширенного, а не простого поля Галуа, как рассматривалось до сих пор.

Определение 3.28. *Код Гоппы* $\Gamma(L, G)$, или просто Γ, состоит из всех векторов $\boldsymbol{v} \in W$ таких, что

$$\sum_{i=1}^{n} \frac{v_i}{x - \alpha_i} \equiv 0 \pmod{G(z)}. \tag{3.7}$$

Ясно, что данное сравнение в кольце $\mathbb{F}_2^m[z]/G(z)$ эквивалентно

$$R_{\boldsymbol{v}}(z) = \sum_{i=1}^{n} \frac{v_i}{z - \alpha_i} = 0. \tag{3.8}$$

$$R_{\boldsymbol{v}}(z) = 0 \text{ в кольце } \mathbb{F}_2^m[z]/G(z).$$

Задавая различным образом многочлен $G(z)$, можно получать коды с различными свойствами. Если $G(z)$ неприводим, то Γ называют *неприводимым кодом Гоппы*.

Коды Гоппы, определённые в (3.7), обладают следующими свойствами:

- Γ — линейный код;
- $n = |L|$ — длина кода;
- число информационных символов $k \geqslant n - mt$;
- кодовое расстояние $d(\Gamma) \geqslant t + 1$.

Проверочная матрица. Сравнение (3.7) эквивалентно

$$\sum_{i=1}^{n} v_i \left\{(z-\alpha_i)^{-1}\right\}_m = 0,$$

где $\left\{(z-\alpha_i)^{-1}\right\}_m$ — элемент, обратный к $z-\alpha_i$ в кольце многочленов по $\bmod G(z)$. Этот обратный элемент существует, поскольку $z-\alpha_i$ не делит $G(z)$ (поскольку $G(\alpha_i) \neq 0$), и находится следующим образом:

$$\left\{(z-\alpha_i)^{-1}\right\}_m = \frac{G(z)-G(\alpha_i)}{z-\alpha_i} G^{-1}(\alpha_i). \qquad (3.9)$$

Действительно,

$$-(z-\alpha_i) \cdot \frac{G(z)-G(\alpha_i)}{z-\alpha_i} G^{-1}(\alpha_i) \equiv 1 \pmod{G(z)}.$$

Следовательно, вектор $\boldsymbol{v}$ лежит в коде $\Gamma(L,G)$, если и только если

$$\sum_{i=1}^{n} v_1 \cdot \frac{G(z)-G(\alpha_i)}{z-\alpha_i} \cdot G^{-1}(\alpha_i) = 0 \qquad (3.10)$$

как многочлен, а не по модулю $G(z)$.

Выполнив деление и проведя некоторые упрощения, равенство (3.10) можно переписать в следующем виде:

$$x^{t-1} \sum_{i=1}^{n} v_i \frac{1}{G(\alpha_i)} + x^{t-2} \sum_{i=1}^{n} v_i \frac{\alpha_i}{G(\alpha_i)} + \ldots$$
$$\ldots + x \sum_{i=1}^{n} v_i \frac{\alpha_i^{t-2}}{G(\alpha_i)} + \sum_{i=1}^{n} v_i \frac{\alpha_i^{t-1}}{G(\alpha_i)} = 0.$$

Отсюда непосредственно получаем проверочную матрицу кода:

$$H_{t\times n} = \begin{bmatrix} \frac{1}{G(\alpha_1)} & \frac{1}{G(\alpha_2)} & \cdots & \frac{1}{G(\alpha_n)} \\ \frac{\alpha_1}{G(\alpha_1)} & \frac{\alpha_2}{G(\alpha_2)} & \cdots & \frac{\alpha_n}{G(\alpha_n)} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\alpha_1^{t-1}}{G(\alpha_1)} & \frac{\alpha_2^{t-1}}{G(\alpha_2)} & \cdots & \frac{\alpha_n^{t-1}}{G(\alpha_n)} \end{bmatrix}. \qquad (3.11)$$

Легко заметить, что всякая квадратная подматрица H^* порядка t (составленная из любых t различных столбцов матрицы) представима произведением матрицы Вандермонда на диагональную невырожденную матрицу:

$$H^*_{t\times t} = \begin{bmatrix} \frac{1}{G(\alpha_{i_1})} & \frac{1}{G(\alpha_{i_2})} & \cdots & \frac{1}{G(\alpha_{i_t})} \\ \frac{\alpha_1}{G(\alpha_{i_1})} & \frac{\alpha_{i_2}}{G(\alpha_2)} & \cdots & \frac{\alpha_n}{G(\alpha_{i_t})} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\alpha_{i_1}^{t-1}}{G(\alpha_{i_1})} & \frac{\alpha_{i_2}^{t-1}}{G(\alpha_{i_2})} & \cdots & \frac{\alpha_{i_t}^{t-1}}{G(\alpha_{i_t})} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_{i_1} & \alpha_{i_2} & \ldots & \alpha_{i_t} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{i_1}^{t-1} & \alpha_{i_2}^{t-1} & \ldots & \alpha_{i_t}^{t-1} \end{bmatrix} \times \begin{bmatrix} \frac{1}{G(\alpha_{i_1})} & 0 & \ldots & 0 \\ 0 & \frac{1}{G(\alpha_{i_2})} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \frac{1}{G(\alpha_{i_t})} \end{bmatrix}.$$

Поскольку все элементы α_{i_j} из L различны, определитель такой матрицы будет отличен от нуля.

Можно показать, что $\Gamma(L, G)$-код длины $n \leqslant 2^m$, у которого $\deg G(x) = t$ имеет

- не более $n - k = mt$ проверочных символов;
- кодовое расстояние $d \geqslant 2t + 1$.

Пример 3.29. Выберем $n = 8$, $m = 3$ $(n = 2^m)$ и в качестве нумераторов позиций L — все элементы поля $GF(2^3)$:

$$L = \{ 0,\ 1,\ \alpha,\ \ldots,\ \alpha^6 \},$$

α — примитивный элемент поля. Выберем и порождающий многочлен Гоппы:

$$G(z) = z^2 + x + 1$$

Легко видеть, что ни один элемент поля $GF(2^3)$ не является корнем многочлена $G(z)$: все его корни лежат в полях $GF(2^2)$, $GF(2^4)$, $GF(2^6)$, ..., и не лежат в поле $GF(2^3)$.

Таким образом, получен неприводимый код Гоппы длины $n = 8$, количеством информационных символов $k \geqslant 8 - 2 \cdot 3 = 2$ и с кодовым расстоянием $d \geqslant 5$. Согласно (3.11) проверочная матрица этого кода равна

$$H = \begin{bmatrix} \frac{1}{G(0)} & \frac{1}{G(1)} & \frac{1}{G(\alpha)} & \cdots & \frac{1}{G(\alpha^6)} \\ \frac{0}{G(0)} & \frac{1}{G(1)} & \frac{\alpha}{G(\alpha)} & \cdots & \frac{\alpha^6}{G(\alpha^6)} \end{bmatrix}.$$

После вычислений в поле $F_2[z]/(G(z))$ получим

$$H = \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix} =$$

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

Кодовыми словами являются

$$\left\{\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right\},$$

они образуют $[8, 2, 5]$-код Гоппы.

Декодирование. Двоичного кода Гоппы производится алгоритмом Паттерсона, который достаточно прост в реализации и быстр в использовании.

Алгоритм Паттерсона преобразует синдром в вектор ошибок. Синдром двоичного слова $\boldsymbol{w} = (w_0, \ldots, w_{n-1})$ есть

$$s(x) \equiv \sum_{i=1}^{n} \frac{w_i}{x - \alpha_i} \equiv 0 \pmod{G(z)},$$

что эквивалентно

$$s(x) = H\boldsymbol{w}^T.$$

Если $s(x) \equiv 0$, то ошибок нет. Иначе вычисляется величина

$$c(x) \equiv \sqrt{s(x)^{-1} - x} \pmod{G(x)}$$

и используя расширенный алгоритм Евклида находят полиномы $a(x)$ и $b(x)$:

$$a(x) \equiv b(x) \cdot c(x) \pmod{G(x)},$$

при этом $\deg(a) \leqslant \lfloor t/2 \rfloor$ и $\deg(b) \leqslant \lfloor (t-1)/2 \rfloor$.

Наконец, полином локаторов ошибок вычисляется как

$$\sigma(x) = a(x)^2 + x \cdot b(x)^2.$$

Далее стандартным способом определяются позиции ошибок (см. пункты 3–4 алгоритма на с. 120).

3.8 Задачи

3.1. Построить порождающую G и проверочную H матрицы для

1) тривиального кода утраивания;
2) кода проверки на чётность.

3.2. Для кода Хемминга, заданного своей проверочной матрицей

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

требуется

1) построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;
2) найти такое кодирование для сообщений

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

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

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

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

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,
3) $w_3(x) = x^6 + x^3 + x^2 + x$.

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

3.6. Пусть α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\left(x^4 + x + 1\right)$. Для кода БЧХ с нулями α, α^2, α^3 и α^4 и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

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

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок есть

$$\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить *позиции ошибок* в $w(x)$.

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

3.9. Рассмотрим БЧХ-код, нули которого есть степени примитивного элемента α поля

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

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить позиции ошибок в данном слове.

Глава 4

Алгебраические основы криптографии

4.1 Основные понятия

Термины. Для всех нижеприведённых терминов имеются различные определения разной степени строгости и точности. Нам будут достаточны указанные.

Криптография (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 человека-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 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) — 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, его сменная часть.

Зашифрование (encryption) — процесс преобразования открытого текста в шифрованный с помощью шифра и ключа.

Расшифрование (decryption) — процесс, обратный к зашифрованию, осуществляемый при известном значении ключа.

Дешифрование — процесс раскрытия криптограммы (злоумышленником или *криптоаналитиком*) без знания секретного ключа.

Определения шифра и его ключа соответствуют принятому в современной криптографии прави-

лу стойкости О. Керкгоффса[1)], согласно которому *в секрете держится только ключ, а сам алгоритм шифрования открыт.*

Таким образом, *надёжность зашифрования определяется исключительно значением его секретного ключа*, известному только легальным пользователям. Алгоритм шифрования тщательно разрабатывается и меняется в редких случаях. А ключ при необходимости легко меняется: 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 криптосистема ключ задается двоичным числом длиной не менее 128 и до 4096 бит.

Шифры подразделяются на:

блочные — сообщение разбивается на блоки фиксированной длины, которые зашифровываются независимо друг от друга (обычно блоки имеют длину 64 или 128 бит);

поточные — сообщение шифруется последовательно посимвольно (символом может быть бит, байт, ...), и каждый символ шифруется в зависимости от его расположения в тексте.

[1)] *Огюст Керкгоффс* (Auguste Kerckhoffs, 1835–1903) — нидерландский криптограф, лингвист, историк, математик, автор фундаментального труда «Военная криптография» (1883), в котором сформулированы общие требования к криптосистемам. Является одним из создателей и популяризаторов искусственного языка Волапюк.

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*. Основная проблема симметрической криптографии — обеспечение секретности при передаче ключей.

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, 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*[2)], если ключ не содержит

[2)] Под «абсолютной» понимается стойкость к дешифрованию, обеспеченная фундаментальными законами природы, а не имеющимися технологическими возможностями.

Использование данной и аналогичных криптосистем с *одноразовым шифрблокнотом* (содержащим наборы ключей $\widetilde{\gamma}_1$, $\widetilde{\gamma}_2$, ...) требует выработки длинных последовательностей двоичных ключей нужного качества, решения проблем их хранения, передачи и уничтожения. На каждом

длинных повторяющихся последовательностей бит и используется однократно.

Утверждённая в России с 1.06.2019 в качестве стандарта криптосистема «Кузнечик» реализует симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит.

Объявленная в США с 26.05.2002 стандартом криптосистема AES (Advanced Encryption Standard) реализует симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 128/192/256 бит.

При асимметрическом шифровании ключ расшифрования k_d остаётся секретным (private key), а ключ зашифрования k_e делается общедоступным (public key). Поэтому асимметрические системы называют ещё *криптосистемами с открытым ключом* или *двуключевыми*. Расшифровать криптограмму может 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) возможных секретных ключей. *Экс-*

из этих этапов жизненного цикла ключей имеется угроза их раскрытия. Все это делает данные системы непрактичными, дорогостоящими, и они применяется в исключительных случаях.

поненциальные 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.

На практике используют гибридные криптографические системы, когда обмен ключами производится с использованием асимметричной криптографии, а шифрование/расшифрование данных — более быстрыми симметричными алгоритмами.

Алгоритм быстрого возведения в степень. При возведении в натуральную степень x некоторого числа используют двоичную запись степени:

$$x = x_k 2^k + x_{k-1} 2^{k-1} + \ldots + x_0 2^0,\ x_i \in \{0,1\},\ i = \overline{0,k}.$$

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 $5 + 3 = 8$ умножений, а не 52.

При вычислении степени некоторого элемента по модулю n возводят в квадрат не само число, а его остаток от деления на n, что существенно проще. Поэтому вычисляют вектор

$$[\ x_0\ \ldots\ x_k\ ]$$

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 $a_{i+1} \equiv_n a_i^2$, $i = 0, \ldots, k-1$.

Пример 4.1. 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, $i = 0, 1, 2, 3$:

$$\begin{aligned} a_0 &= 3 \equiv_5 3,\\ a_1 &= 3^2 = 9 \equiv_5 4,\\ a_2 &= 4^2 = 16 \equiv_5 1,\\ a_3 &= 1^2 \equiv_5 1. \end{aligned}$$

3. Окончательно $3^{11} \equiv_5 3 \cdot 4 = 12 \equiv_5 2$.

Теоремы Ферма и Эйлера

Теорема 4.2 (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 2.21 (см. с. 57). Дадим ещё одно

Доказательство. Требуемое сравнение выполняется для $a \equiv_p 1$ и всегда для $p = 2$ (тогда a нечётно).

Для остальных случаев оно доказывается для данного $p > 2$ индукцией по a, $a + 1 \not\equiv_p 0$. По тождеству Фробениуса и индуктивному предположению $a^p \equiv_p a$ имеем

$$(a+1)^{p-1} = (a+1)^p(a+1)^{-1} \equiv_p (a^p+1)(a+1)^{-1} = \\ = (a+1)(a+1)^{-1} \equiv_p 1.$$

□

Обобщением малой теоремы Ферма является следующая

Теорема 4.3 (*Эйлер*). *Если* $n > 1$ *и* $(a, n) = 1$, *то*

$$a^{\varphi(n)} \equiv_n 1. \tag{4.1}$$

Задача о рюкзаке: выбрать такие элементы вектор-строки $\boldsymbol{a} = [\ a_1\ \ldots\ a_n\ ]$ различных целых, чтобы их сумма равнялась данному z («размер рюкзака»)[3)].

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: $\boldsymbol{a} \times \boldsymbol{x} = z$. Неизвестны полиномиальные алгоритмы решения задачи о рюкзаке.

[3)] Предполагается, что решение существует и единственно; другое название задачи — *проблема подмножества суммы*

Односторонняя функция — центральное понятие криптографии.

Определение 4.4. Дадим его неформальное определение. *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.*

Для формализации данного понятия вспомним, что такое *вероятностный алгоритм.* Это алгоритм, предусматривающий на определённых этапах своей работы обращение к генератору случайных чисел. В результате этого сокращается время получения результата, однако достоверность последнего становится не абсолютной и носит вероятностный характер.

Напомним также, что $\{0,1\}^*$ обозначает множество всевозможных, включая пустую, $(0,1)$-последовательностей.

Определение 4.5. Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется *односторонней*, если

(1) она полиномиально вычислима;
(2) существует полином p такой, что $|x| \leqslant p(|f(x)|)$ для всех $x \in \{0,1\}^*$;

(3) для любого полиномиального вероятностного алгоритма $\mathcal{A}$ величина

$$\Pr\left[A(f(x)) \in f^{-1}(f(x))\right],\ x \in \{0,1\}^n,$$

пренебрежимо мала как функция от $n \in \mathbb{N}$.

Заметим, что f^{-1} есть многозначное отношение («один ко многим»). Условие (2) означает, что функция f *честная*, то есть, говоря неформально, не сильно уменьшает длину своего аргумента. Без этого условия полиномиальному алгоритму может не хватить времени на выписывание какого либо прообраза x входного значения $f(x)$. Условие (3) означает, что для любого полинома p неравенство $f(\widetilde{x}) \leqslant 1/p(|\widetilde{x}|)$ выполняется при всех $\widetilde{x} \in \{0,1\}^*$ достаточно большой длины, то есть функция f убывает быстрее, чем $1/p(|\widetilde{x}|)$ для любого полинома p.

До сих пор не доказано, что однонаправленные функции вообще существуют (проблема их существования эквивалентна проблеме $P \stackrel{?}{=} NP$). Однако было предложено много функций, претендующие на односторонность. Они использует 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 значение x, что $a^x = b \pmod n$ — задача нахождения *дискретного логарифма*, DLP (Discrete Logarithm Problem[4)]).
- Решить задачу о рюкзаке для общего случая.
- Декодировать исправляющий ошибки линейный код общего вида.

[4)] не путать с технологиями предотвращения утечек конфиденциальной информации Data Leak Prevention

Односторонняя функция с секретом (с лазейкой; trapdoor one-way function) — функция $f_k(x) : X \to Y$ 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.

Это неформальное и недостаточное определение[5)] для нс будет достаточно. Для точного определения требуется вводить ряд новых понятий.

Также заметим, что в приведённом общепринятом названии слово прилагательное "односторонняя" просто лишний: 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: вычисление y производится методом быстрого возведения в степень, а эффективный алгоритм обратного преобразования $f^{-1}(y)$ требует знания примарного разложения n. Эта информация может считаться лазейкой.

Применение односторонних функций с секретом позволяет организовать обмен шифрованными сооб-

[5)] см. http://cryptography.ru/100/

щениями по открытым каналов связи, снабдить документ электронной подписью и др.

4.2 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 этого

1. Автор документа a вычисляет значение y хэш-функции преобразования a в битовую строку установленной длины[6)].
2. Используя свой секретный ключ k к односторонней функции с секретом f_k, автор вычисляет значение $x = f_k^{-1}(y)$ и посылает документ a, его хэш y и вычисленное значение x адресатам.
3. Проверку авторства документа a легко проводит любой адресат, вычисляя без знания k значение $f_k(x)$ и сравнивая результат с y.

[6)] Понятно, что хэш-функции осуществляют необратимые преобразование информации. *Хэш* (или *дайджест*) y выступает как компактный представитель (паспорт) документа a. К хэш-функциям предъявляются специфические требования, которые мы не будем здесь обсуждать.

Ясно, что снабдить ЭЦП данного автора какой-либо документ без знания секрета k трудновыполнимо, а проверка подписи проводится быстрее, чем её создание.

В России федеральным законом определяются три вида электронных подписей: простая, усиленная неквалифицированная и усиленная квалифицированная. Отличия заключаются в степени защищенности и юридически предоставляемых возможностях.

Выработка общего секретного ключа по открытому каналу связи — покажем, как это можно сделать на примере протокола DH Диффи–Хеллмана[7)].

Два лица — традиционно A (Алиса) и B (Боб) — обмениваются сообщениями по открытому каналу. Чтобы обеспечить секретность переписки, A и B должны выработать общий секретный ключ.

Для этого они выбирают простое число p, а в поле Галуа $GF(p)$ — некоторый элемент α; эти значения открыты. 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:

$$A:\ X = \alpha^x, \qquad B:\ Y = \alpha^y, \qquad (*)$$

[7)] Предложен в 1976 г. сотрудниками MTI *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 криптографии с открытым ключом.

которыми они обмениваются по открытому каналу.

Абонент A, получив Y, вычисляет ключ:

$$K = Y^x = \alpha^{xy} \pmod{p},$$

и аналогично поступает абонент B:

$$K = X^y = \alpha^{xy} \pmod{p}.$$

Тем самым у Алисы и Боба появился общий секретный ключ $K \in GF(p)$, который в дальнейшем используется в алгоритмах симметричного шифрования.

Пассивный злоумышленник, перехватывающий, но не изменяющий сообщений (традиционно E, Ева, от англ. eavesdropper, подслушивающий) не может определить ключ K: его определение 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.

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 собеседник. Действительно, если к каналу связи имеет доступ *активный злоумышленник* (традиционно M, Меллори от англ. 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 каналу связи* (защищённому от подмены, но не от прослушивания.

[8)] Вспоминаем Сказку о царе Салтане *А. С. Пушкина*: «...И в суму его пустую // Суют грамоту другую».

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 $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^n$. Умножая $\boldsymbol{a}$ на эти векторы-столбцы, получим шифртекст $\boldsymbol{y} = [\, y_1 \ \ldots \ y_n \,]$. Таким образом, шифрование осуществляется элементарно.

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 $\boldsymbol{a}$ меньше 916. 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. Это даст возможность далее определить элемент $v = u^{-1} \pmod{m}$.

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 значения m и u.

Пример 4.6. 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:

$$\boldsymbol{b} \times X = \begin{bmatrix} 3 & 6 & 12 & 24 & 11 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \\ = \begin{bmatrix} 39 & 29 & 14 \end{bmatrix} = \boldsymbol{y}.$$

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 $\boldsymbol{x}^1$, $\boldsymbol{x}^2$, $\boldsymbol{x}^3$.

4.3 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
$$y = x^e \pmod{n}. \tag{4.2}$$

Для расшифрования криптограммы y нужно решить сравнение (4.2) относительно x.

Искомое решение может быть представлено в виде
$$x = y^d \pmod{n}, \tag{4.3}$$
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 4.3 Эйлера имеем

$$x^{\varphi(n)} \equiv_n 1, \quad \text{то} \quad x^{k\cdot\varphi(n)} \equiv_n 1$$

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

$$d \cdot e = 1 \pmod{\varphi(n)}. \tag{4.4}$$

Решить это сравнение можно было бы, например, с помощью обобщённого алгоритма Евклида 2.2 со с. 45. 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 RSA основана на сложности задачи FACT*. Также как и DLP, эта задача принадлежит классу NP, но её NP-полнота не доказана.

Система RSA опубликована в 1978 г., и её название есть аббревиатура от фамилий авторов Рональда Линна Ривéста (Ronald Linn Rivest, 1947), *Ади Шамира* (Adi Shamir, 1952) и Леонарда Макса Áдлемана (Leonard M. Adleman, 1945) из MTI[9)].

[9)] Однако согласно рассекреченным британским правительством в 1997 г. сведениям, идея основных принципов криптографии с открытым

Алгоритм RSA используется в большом числе криптографических приложений.

Конкретно, авторы этой схемы предложили выбирать число n в виде произведения двух больших простых множителей p и q, $p \neq q$. Тогда

$$\varphi(n) = \varphi(pq) = (p-1)(q-1), \qquad (4.5)$$

и условием на выбор экспоненты e будет её взаимная простота с $p-1$ и $q-1$. Отметим, что число, представимое в виде произведения двух простых чисел, называют *полупростым*.

Утверждение 4.7. *Пусть $n = pq$, где p, q — простые числа. 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.

ключём принадлежит сотруднику Главного управления связи Великобритании (GCHQ) Джеймсу Х. Эллису, который высказал её в 1970 г., но не смог найти для неё практической реализации. Первооткрывателем алгоритма RSA в 1973 г. стал Клиффорд Кокс, а впервые реализовал то, что известно как протокол Диффи–Хеллмана — в следующем году Малкольм Дж. Уильямсон (все из GCHQ).

1. Организатор системы выбирает два 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 (4.4) — определяет d.
3. Числа n и e публикуются, числа d и $\varphi(n)$ остаются секретными.
4. Теперь любой абонент может отправлять зашифрованные с помощью (4.2) сообщения организатору этой системы, который легко расшифровывает их с помощью (4.3).

Заметим, что

- большие простые p и q должны быть такими, чтобы значение $|p-q|$ было также не мало, иначе их несложно подобрать;
- 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;
- нахождение ключа расшифрования d без знания $\varphi(n)$ (факторизация большого значения n) вычислительно неосуществимо;
- алгоритм расшифрования в системе RSA намного медленнее, чем для симметрических криптоалгоритмов.

Пример 4.8. 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	$q = 9$ (117 9)
3	3	-9	$q = 4$ (12 $-$ 36)
4	1	**37**	$q = 3$
5	0		

и получим $d = 37$.

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 [4].

Для иллюстрации своего метода Ривест, Шамир и 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 (4.2) при модуле n, содержащим 129 знаков (система 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 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 и в результате дешифровки получилась фраза «*The magic words are squeamish ossifrage*» (*Волшебные слова — привередливая скопа*; по-видимому, нарочито бессмысленная фраза).

Выполнение вычислений потребовало огромных по тем временам ресурсов: в работе, возглавлявшейся четырьмя авторами 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 фразу считалось подтверждением стойкости системы RSA-129. Однако в последние десятилетия были найдены эффективные алгоритмы факторизации, 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.

Также отметим, что побуквенное шифрование крайне нестойко: в достаточно длинной криптограмме легко выделяются пробелы, затем 1- и 2-буквенные слова, что позволит простым подбором по смыслу восстановить открытый текст без подбора ключа.

4.4 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

Выбирается случайное число a из интервала $[\ 2,\ N-1\ ]$, символически $a \xleftarrow{\$} [\ 2,\ N-1\ ]$.

N — составное, если окажется, что либо $a \mid N$, либо сравнение

$$a^{N-1} \equiv_N 1 \tag{4.6}$$

не выполняется.

Иначе вопрос остаётся открытым, и N испытывается при другом значении a.

Имеется, однако, бесконечно много составных чисел, для которых сравнение (4.6) выполняется при всех a, взаимно простых с N, то есть они не будут выявлены данной проверкой. Эти числа называют *псевдопростыми* или *числами Кармайкла*[10]; $561 = 3 \cdot 11 \cdot 17$ — наименьшее такое число. По мере возрастания чи́сла Кармайкла становятся всё более редкими.

Отметим, что

[10] *Роберт Дэниэл Кармайкл* (R. D. Carmichael, 1879–1967) — американский математик.

- 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, основанные на эллиптических кривых.

Генерация ключей. Линейный конгруэнтный метод. Один из виртуальных способов получения ключа шифрования — использовать генератор псевдослучайных чисел. Хорошие по статистическим свойствам последовательности псевдослучайных чисел получаются по формуле *линейного конгруэнтного метода* (linear congruential):

$$r_{i+1} \equiv_m a \cdot r_i + b, \quad i = 1, \ldots, N,$$

где a, b, m — некоторые целые взаимно простые числа, от которых и зависит качество такой последовательности.

Очевидно, рассматриваемая последовательность будет периодической, и показано, что её период может достигать значения m. Часто 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 N. Отсюда следует вывод: линейный конгруэнтный метод *не обладает криптографической стойкостью.*

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. Различные методы типа вычисления адреса памяти или номера сектора на диске с извлечением данных оттуда, использование интервалов между последовательными 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 большое 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 возможно, что N — простое. Тогда следует попытаться доказать

[11] Это согласуется с естественнонаучной точкой зрения, что природа любой случайности — квантовая. «*Любой, кто рассматривает арифметические методы получения случайных чисел, безусловно заблудшая душа*» (Дж. фон Нейман).

это с помощью более мощных и трудоёмких тестов[12)].

Для вычислений с большими числами созданы специальные языки программирования, например PARI и UBASIC.

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 многих криптосистем основывается на трудности решения задачи FACT. Отметим, что на существующих компьютерах распознавание простоты целого числа с 125-ю десятичными цифрами может быть выполнено за несколько минут, в то время как его факторизация потребует миллионы лет компьютерных вычислений.

Сплиттингом натурального числа n называют представление его в виде

$$n = a \cdot b, \quad a, b \in [\, 2,\ \lfloor n/2 \rfloor\,],$$

а числа a и b — *нетривиальными факторами* 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

$$a := f(a),\ b := f(f(b)) \pmod{n}.$$

[12)] см. теорему 4 на с. 102 книги *Введение в криптографию / Под общ. ред. В. В. Ященко. — М.: МЦНМО, 2012.*

3. Вычисляем $d = \text{НОД}\,(a - b, n)$.

4. Если $d \in [\ 2,\ n-1\ ]$, то d — делитель n.
   Если $d = 1$, то переход к шагу 2.
   Если $d = n$, то алгоритм заканчивает работу, и вопрос о нетривиальных факторах в n остается открытым.

ρ-алгоритм Полларда[13)] для сплиттинга числа n требует $O\left(n^{1/4}\right)$ модулярных умножений и эффективен при поиске малых делителей.

Пример 4.9. 1. Разложим на нетривиальные сомножители число $n = 163\,829$.

1. $a = 5,\ b = 26$.

2. $a - b = 5 - 26 = -21 \equiv_{163\,829} = 163\,808$ и
   $d = \text{НОД}\,(163\,808, 163\,829) = 23$.

3. Поскольку $d \in [\ 1,\ n-1\ ]$, 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

[13)] Предложен в 1975 г. британским математиком *Джоном Полларом* (John M. Pollard, 1941). Название связано с тем, что алгоритм строит числовую последовательность, элементы которой, начиная с некоторого элемента образуют цикл, что иллюстрируется расположением чисел в виде греческой буквы ρ.

	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 455 459.

4.5 Дискретное логарифмирование

DLP и криптосистема ЭльГамаля. 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 асимметричных шифрсистем с отрытым ключом, в частности рассмотренная ранее система Диффи–Хелмана DH и система Elgamal, разработанная Т. Эльджимали[14)].

[14)] *Та́хер А. Эльджимали́* (англ. Taher Elgamal, 1955) — американский криптограф египетского происхождения; на русском языке утвердилось написание его фамилии Эль-Гамаль.

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 ключом*, вычисляет по $\bmod p$ пару чисел

$$a = \alpha^s \quad \text{и} \quad b = m \cdot (d_B)^s,$$

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 4.10. 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

$$s = 1520 \in [\,1,\, p-2\,];$$

4) вычисляет по mod 2 357 числа $a = \alpha^s = 1\,430$ и
$$b = m \cdot (d_B)^s \equiv 2035 \cdot 1\,185^{1520} \equiv 697;$$
5) посылает шифртекст (1 430, 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 группе по умножению кольца $\mathbb{F}_p^*$, 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 машинной памяти.

Так же ясно, что найти такой элемент x в группе $\mathbb{Z}_m$, что $a^x = b$ можно лишь если b принадлежит подгруппе, порожденной элементом a. Понятно, если группа G циклическая и a — её порождающий элемент группы, то вопрос снимается.

Алгоритм согласования. Рассмотрим сравнение

$$a^x \equiv_p b \tag{4.7}$$

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 (4.7) 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 (4.7)

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

$$\begin{aligned} &H,\ H-1,\ H-2,\ \ldots,\ H-H \\ &\qquad 2H,\ 2H-1,\ \ldots,\ 2H-H,\ \ldots, \\ &\qquad\qquad H^2,\ H^2-1,\ \ldots,\ H^2-H \end{aligned}$$

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 4.11. 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. $u = 1, 2, 3, 4$

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. $v = 0, 1, \ldots, 4$

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 4.12. 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 достаточно быстрые (субэкспоненциальные) алгоритмы дискретного логарифмирования, основанные на различных идеях.

4.6 Криптосистемы МакЭлиса и Ниддеррайтера

Криптосистема МакЭлиса. 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 *рандомизацию* — внесение случайностей в данные. Кратко опишем её простейший вариант.

Для получения секретных сообщений от Боба, Алиса выбирает исправляющий r ошибок линейный $[n, k, 2r+1]$-код C, для которого известен эффективный декодирующий алгоритм. Пусть код C задающийся порождающей матрицей $G_{k\times n}$.

[15)] Эта задача декодирования множества данных (Information set decoding Problem, ISD Problem) и состоит указании вероятностной стратегии, которая по пытается определить позиции $\leqslant \lfloor d/2 \rfloor$ ошибок в принятом, возможно искажённом слове $[k, n, d]$-кода.

Далее Алиса генерирует случайные квадратные матрицы:

S порядка k — невырожденную;
P порядка n — перестановочную.

Вычисляя $k \times n$-матрицу

$$G' = S \times G \times P,$$

Алиса «маскирует» матрицу G.

Секретным ключом является тройка матриц (S, G, P), а открытым — пара (G', r), которая передаётся Бобу.

Алиса, желая зашифровать своё сообщение $\boldsymbol{u}$ длины k

1) выбирает случайный n-вектор $\boldsymbol{e}$ с не более чем r единицами;
2) вычисляет вектор $\boldsymbol{w} = \boldsymbol{u}G' + \boldsymbol{e}$ и пересылает её Бобу.

Для расшифрования крипторгаммы $\boldsymbol{w}$ Боб

1) вычисляет вектор $\boldsymbol{w}' = \boldsymbol{w}P^{-1}$;
2) используя какой-либо алгоритм декодирования кода C, порождённого матрицей G, получает из $\boldsymbol{w}'$ вектор $\boldsymbol{u}'$.
3) вычисляет $\boldsymbol{u} = \boldsymbol{u}'S^{-1}$.

Покажем, что описанная схемы расшифрования действительно восстанавливает исходное сообщение $\boldsymbol{u}$. Имеем:

$$\boldsymbol{w}' = \boldsymbol{w}P^{-1} = [\boldsymbol{u}G' + \boldsymbol{e}]\,P^{-1} = \\ = [\boldsymbol{u}SGP + \boldsymbol{e}]\,P^{-1} = (\boldsymbol{u}S)G + \boldsymbol{e}P^{-1}.$$

Поскольку вектор $\boldsymbol{e}P^{-1}$ содержит не более r единиц, алгоритм декодирования кода C корректирует $\boldsymbol{w}'$ до $\boldsymbol{u}' = \boldsymbol{u}S$. Преобразование $\boldsymbol{u}'S^{-1} = \boldsymbol{u}$ завершает расшифрование.

Шифрсистема МакЭлиса основана на следующих предположениях.

1. Предполагается, что задача NCP поиска кодового слова, ближайшего к принятому, к 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 $\boldsymbol{u}$ на S перед кодированием призвано разрушить внутреннюю структуру сообщения, чтобы трудно было его «угадать».

По сравнению с RSA криптосистема МакЭлиса имеет преимущество в скорости зашифрования и расшифрования, а также более высокую степень защиты при данной длине ключа.

К недостаткам системы относятся большие размеры открытого ключа и криптограммы $\boldsymbol{w}$, которая оказывается значительно длиннее сообщения $\boldsymbol{u}$.

Пример значений реально используемых параметров шифрсистемы МакЭлиса: $n = 6960$, $k = 5413$, $r = 119$, 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 Нидеррайтера 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 МакЭлиса и

[16] *Харальд Нидеррайтер* (Harald G. Niederreiter, 1944) — австрийский математик.

Нидеррайтера взломаны российскими криптоаналитиками, однако они остаются стойкими при условии использовании кодов Гоппы[17].

4.7 Задачи

4.1. 1. Решить комбинаторную задачу.

Пусть p — простое число, большее 2. Сколько существует способов C раскрасить вершины правильного p-угольника в a цветов, если раскраски, получающиеся совмещением при вращении многоугольника вокруг своего центра, считать одинаковыми?

2. На основе полученного решения доказать малую теорему Ферма.

4.2. В системе шифрования RSA по данным модулю $n = 91$ и экспоненте $e = 29$ найти ключ расшифрования d.

4.3. 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.

4.4. Решить сравнения

$$\text{а) } 6^x \equiv_{11} 2; \quad \text{б) } 8^x \equiv_{11} 3; \quad \text{в) } 2^x \equiv_{13} 3.$$

[17] Криптосистема МакЭлиса на кодах Гоппы рассматривается Еврокомиссией как перспективная.

4.5. 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}.

4.6. 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 $y_2 = 03$.

Глава 5

Начала эллиптической криптографии

5.1 Эллиптическая криптография: введение

Почему 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). Наиболее быстрые из них имеют лишь 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. одновременно были предложены в независимых работах американских математиков В. Миллера и Н. Коблица.

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 5.1. *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 5.2. *Всякую неособенную алгебраическую кривую E третьего порядка над произвольным полем можно преобразовать к виду*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (5.1)$$

называемому длинной формой Вейерштрасса.

Определение 5.3. 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

$$(x, y) + \mathcal{O} = \mathcal{O} + (x, y) = (x, y), \quad \mathcal{O} + \mathcal{O} = \mathcal{O},$$

называют *эллиптической кривой E над полем K*, символически $E(K)$.

Ясно, что точки $(x, y) \in K^2$, лежащие на $E(K)$, удовлетворяют уравнению (5.1), 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

$$-P = (x_0, -a_1x - a_3 - y_0) \qquad (5.2)$$

также удовлетворяет (5.1), 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 (5.1) 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

$$y^2 = x^3 + ax + b. \qquad (5.3)$$

В этом случае противоположная к $P = (x_0, y_0)$ точка эллиптической кривой E есть

$$-P = (x_0, -y_0). \tag{5.4}$$

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. 5.1). При параметризации, считая, что x имеет сте-

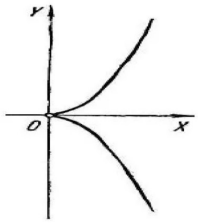


Рис. 5.1. Полукубическая парабола (парабола Нейла)

пень 2, а y — степень 3, индексы i коэффициентов a_i, $i = \overline{1,6}$ (5.1) определяют 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.

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 допускают наглядные графическую интерпретацию как плоских кривых 3-го порядка (*кубик*) и 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*

$$\Delta \stackrel{\text{def}}{=} -16(4a^3 + 27b^2) \neq 0. \tag{5.5}$$

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 $\Delta > 0$ их двух связных компонент, а при $\Delta < 0$ — из одной (см. рис. 5.2).

Далее нашей целью будет задание на E такой операции сложения, чтобы эллиптическая кривая превратилась в аддитивную абелевую группу.

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

[1)] Полукубическая парабола имеет точку возврата $(0, 0)$

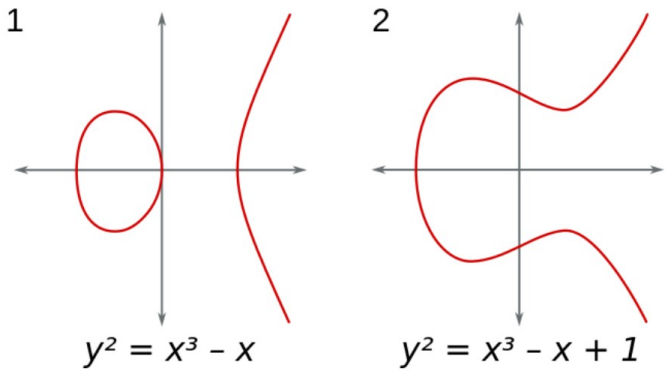


Рис. 5.2. Графики ЭК над $\mathbb{R}$ при (1) $\Delta = 64 > 0$ и (2) $\Delta = -368 < 0$

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:

$$P + Q = -R. \tag{5.6}$$

Проведём через две точки P и Q на кривой E прямую 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 счита-

ем, 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.

Красивая 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.

Пример 5.4. На рис. 5.3 показано нахождение точки $P+Q$ в случае $Q \neq \pm P$ на действительной ЭК $y^2 = x^3 - x$.

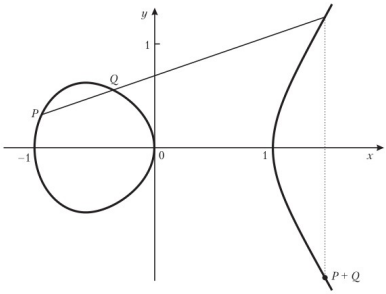


Рис. 5.3

Пусть $P=(x_1,y_1)$ и $Q=(x_2,y_2)$. Тогда можно показать, что координаты (x_3,y_3) точки $-(P+Q)=R$ 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

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \quad (5.7)$$

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

$$\begin{cases} x_3 = \lambda^2 - 2x_1, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{3x_1^2 + a}{2y_1}. \quad (5.8)$$

Геометрическую иллюстрацию формул суммирования и удвоения точек ЭК см. на рис. 5.4. Геометрическую иллюстрацию формул суммирования и удвоения точек ЭК см. на рис. 5.4.

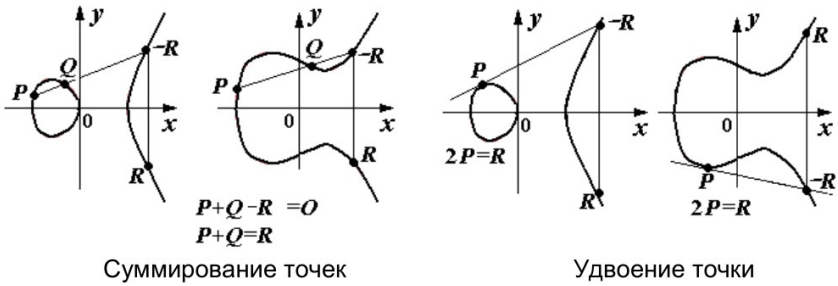


Рис. 5.4. Суммирование и удвоение точек на ЭК

Пример 5.5. 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.

1. Подстановка $x_1 = -3$, $y_1 = 9$, $x_2 = -2$, $y_2 = 8$ в первое из уравнений (5.7) даёт $x_3 = 6$.
2. Тогда второе уравнение даёт $y_3 = 0$ и $P + Q = (6, 0)$.
3. Далее, подставляя $x_1 = -3$, $y_1 = 9$, $a = -36$ в первое уравнение из (5.8) 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 (5.3), то есть если $\operatorname{char} K \neq 2, 3$.

Теорема 5.6 (*Пуанкаре*, 1901). *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 точках на кубической кривой*). □

Приведённая теорема А. Пуанкаре справедлива для ЭК над любым полем K при определении сложения в общем виде (5.6).

Умножение точки P на целое положительное k, называемое *скалярным умножением*, определяется как сумма k точек P:

$$kP \;=\; P + \ldots + P \quad (k \text{ раз}).$$

5.2 Эллиптические кривые в конечных полях

Порядок эллиптической кривой. Приведём вначале «графики» ЭК $y^2 = x^3 - 7x + 10 \pmod p$ для $p = 19, 97, 127, 487$. Видно, что они имеют симметрию относительно $y = p/2$.

Множества точек эллиптической кривой над конечным полем, естественно, конечно. Порядок этой

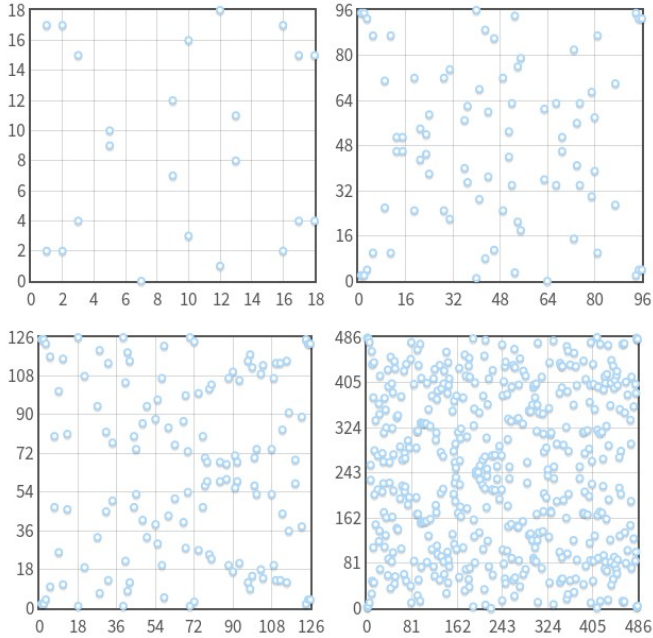


Рис. 5.5. ЭК $y^2 = x^3 - 7x + 10 \pmod{p}$ для $p = 19, 97, 127, 487$

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 корни, следует сразу ожидать, что порядок эллиптической кривой примерно q.

Сильным результатам является

Теорема 5.7 (*Хассе*, 1934). *Пусть* N — *порядок эллиптической кривой* $E(GF(q))$. *Тогда*

$$|\, N - (q+1)\,| \leqslant 2\sqrt{q}.$$

Утверждение 5.8. *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 5.9. 1. При $a = 1$, $b = 0$ короткая форма Вейерштраса (5.3) 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 (5.3) 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 kP для заданной точки $P = (x, y)$, эту операцию выполняют с использованием операций сложения, вычитания и удвоения точки.

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 5.10. 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 стойки к взлому. Факторизация порядка таких ЭК не должна содержать малых простых множителей, что сильно затрудняет решение задачи дискретного логарифмирования. 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 $m = \lceil N_1 \rceil$.
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 5.11. 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.

Удобно, если n — простое число.

По теореме Лагранжа

$$N = n \cdot h.$$

Значение h (индекс подгруппы группы точек ЭК) называют *кофактором.*

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 название 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

$$n = 2^{252} + 27742317777372353535851937790883648493$$

индекса $h = 8$. Умножение точек проходит за фиксированное время. Размеры секретного и открытого ключей на практике составляют всего 32, 64 или 128 бита.

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 (5.5), то есть $\Delta \neq 0$ по $\bmod(\operatorname{char} K)$.

Далее будем для точек

$$P = (x_1, y_1), \quad Q = (x_2, y_2)$$

данной ЭК находить точки

$$-P, \quad P + Q \quad \text{и} \quad 2P,$$

этой же кривой, координаты которых будем обозначать (x_3, y_3).

$\underline{\operatorname{char} K > 3}$. 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. 184 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 5.12. В п. 3 примера 5.9 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 5.13. *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 5.14. *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.*

$\underline{\text{char } K = 3}$. В этом случае уравнение (5.1) при подходящей замене переменных принимает вид

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in GF(3^n). \qquad (5.9)$$

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 (5.7) для координат точки $P + Q = 2P$ остаются справедливыми.

4. При $x_1 = x_2$ точка $P + Q = 2P$ имеет координаты

$$\begin{cases} x_3 = \lambda^2 - a + x_1, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{ax_1 - b}{y_1}. \qquad (5.10)$$

Пример 5.15. 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:

$$\{\,(0,\pm 1),\ (\pm 1,\pm 1),\ (t,0),\ (t^3,0),\ (t^9,0),(-t^2,\pm t^7),$$
$$(-t^4,\pm t^{11}),\ (t^5,\pm t^{11}),\ (-t^6,\pm t^8),\ (-t^7,\pm t^{11}),$$
$$(t^8,\pm t^7),\ (-t^{10},\pm t^8),\ (-t^{11},\pm t^8),\ (-t^{12},\pm t^7),\ \mathcal{O}\,\}\,.$$

char $K = 2$. В этом случае кривая (5.1) 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 5.16. 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 $\gamma^3 = \gamma + 1$.

5.3 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. 5.6.

Тогда задача ECDLP принимает вид нахождения целого числа m из соотношения

$$m \cdot P = Q \tag{5.11}$$

для точек P и Q ЭК.

Использование группы точек ЭК при построении криптосистем позволило уменьшить параметры криптосистем при сохранении их стойкости.

Криптологическая устойчивость систем на ЭК основана на сложности определения m из равенства (5.11) при заданных известных Q и P, если m велико.

Это связано 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

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. 5.6. «Перевод» криптоалгоритма над конечным полем в аналогичный над эллиптической кривой

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 (5.11) — 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 гораздо сложнее, и потому для криптостойкости число это порядок группы G можно брать меньше, на практике его длина от 150 до 350 бит.

Рассмотрим алгоритм работы данной системы EC-ElGamal.

Системные параметры — выбираются и вычисляются организатором шифрсистемы. Ему необходимо:

1) описать конечное поле F;
2) задать уравнение ЭК E над полем F, найти порядок группы точек кривой E;
3) найти в E циклическую подгруппу G большого порядка N 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 5.17. 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 2972.

3. Порядок подгруппы некоторой группы есть делитель порядка группы.

   Собственные делители 2972 суть 2, 4, 743, 1486.

   На E выбирается циклическая подгруппа G наибольшего порядка $N = 1486$ 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 (5.4) и (5.7) 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

$$\begin{aligned} d &= r \cdot Y \;=\; 1325 \cdot (589, 1045) \;=\; (2047, 1793), \\ g &= r \cdot P \;=\; 1325 \cdot (8, 2123) \;=\; (192, 742), \\ h &= M + d \;=\; (1634, 2494) + (2047, 1793) \;= \\ &= (351, 33). \end{aligned}$$

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 $t = \mathrm{FA}$.

Срок действия	Шифр с секретным ключом	RSA	Криптография на эллиптических кривых
дни/часы	50	512	100
5 лет	73	1024	146
10–20 лет	103	2048	206
30–50 лет	141	4096	282

Рис. 5.7. Длины ключей, достаточные для конфиденциальности (шифр с секретным ключом — шифр Вернама)

Решения задач

1. Группы, кольца, поля

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

1) целые числа, кратные данному натуральному числу n, относительно сложения?
2) неотрицательные целые числа относительно сложения?
3) нечетные целые числа относительно сложения?
4) 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 взаимнооднозначные отображения этого множества на себя, относительно композиции отображений?

14) элементы n-мерного векторного пространства $\mathbb{R}^n$ относительно сложения?

15) параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений?

16) повороты трехмерного пространства $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку O относительно композиции движений?

(1) Да, (2) нет (противоположного элемента), (3) нет (устойчивости), (4) нет (ассоциативности), (5) нет (обратного у 0), (6) да, (7) да, (8) нет (ассоциативности), (9) да, (10) нет (обратных у всех), (11)–(16) да.

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

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

1. Все подгруппы циклической группы — циклические. Порождающими элементами *подгрупп* $\mathbb{Z}_{24}$ будут делители m порядка группы 24: то есть $m = 1, 2, 3, 4, 6, 8, 12, 24 \equiv 0$.
Порядок соответствующей подгруппы — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle \cong \mathbb{Z}_{24}$;
$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;
$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_{8}$;
$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_{6}$;
$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_{4}$;
$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_{3}$;
$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_{2}$;
$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — 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:

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

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

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

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

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) = \\
&= p_1^{\alpha_1 - 1}\varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_k) = \\
&= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_1) \cdot \ldots \cdot \varphi(p_k) = \\
&= \frac{n}{p_1 \cdot \ldots \cdot p_k} \cdot (p_1 - 1) \cdot \ldots \cdot (p_k - 1) = \\
&= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

1.5. 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?

Все — кольца: (1) обратной матрицы может не быть; (2), (3) многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы).

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

По дистрибутивности

$$x{\cdot}(y{+}z) = x{\cdot}y{+}x{\cdot}z \;\Rightarrow\; x{\cdot}(0{+}0) = x{\cdot}0 = x{\cdot}0{+}x{\cdot}0 \;\Rightarrow$$
$$\Rightarrow\; x \cdot 0 = 0.$$

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

Нет! Хотя $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$.

1.8. Показать, что множество векторов пространства с операциями сложения и векторного умножения является кольцом.

Является ли оно ассоциативным? коммутативным?

Множество векторов V содержит нулевой вектор $\mathbf{0}$ и является, очевидно, абелевой группой по сложению, а операция $\times$ векторного умножения связана со сложением дистрибутивными законами

$$\boldsymbol{x} \times (\boldsymbol{y} + \boldsymbol{z}) = \boldsymbol{x} \times \boldsymbol{y} + \boldsymbol{x} \times \boldsymbol{z},$$
$$(\boldsymbol{y} + \boldsymbol{z}) \times \boldsymbol{x} = \boldsymbol{y} \times \boldsymbol{x} + \boldsymbol{z} \times \boldsymbol{x}.$$

Кольцо $\langle V, +, \times, \mathbf{0} \rangle$ некоммутативно: $\boldsymbol{x} \times \boldsymbol{y} \neq \boldsymbol{y} \times \boldsymbol{x}$ и неассоциативно: $\boldsymbol{x} \times (\boldsymbol{y} \times \boldsymbol{z}) \neq (\boldsymbol{x} \times \boldsymbol{y}) \times \boldsymbol{z}$.

Однако в рассматриваемом кольце выполняются тождества, заменяющие, в некотором смысле коммутативность и ассоциативность:

$$\boldsymbol{x} \times \boldsymbol{y} = -\boldsymbol{y} \times \boldsymbol{x} \;\; (\text{антикоммутативность}),$$

$$(\boldsymbol{x} \times \boldsymbol{y}) \times \boldsymbol{z} + (\boldsymbol{y} \times \boldsymbol{z}) \times \boldsymbol{x} + \\ + (\boldsymbol{z} \times \boldsymbol{x}) \times \boldsymbol{y} = \mathbf{0} \text{ (тождество Якоби).}$$

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

В кольце $\mathbb{Z}_6$ классы вычетов по идеалу $(3) = \{0, 3\}$ суть

$$\begin{aligned} 0 + (3) &= 3 + (3) = (0, 3), \\ 1 + (3) &= 4 + (3) = (1, 4), \\ 2 + (3) &= 5 + (3) = (2, 5). \end{aligned}$$

1.10. Является ли поле $\mathbb{Z}_2$ подполем поля $\mathbb{Z}_5$?

Нет! В $\mathbb{Z}_2 : 1 + 1 = 0$, а в $\mathbb{Z}_5 : 1 + 1 = 2$, то есть операция сложения в $\mathbb{Z}_5$ неустойчива при переходе к своему подмножеству $\{0, 1\}$.

2. Конечные кольца и поля

2.1. Построить все изоморфизмы между мультипликативной группой поля $\mathbb{F}_7$ и аддитивной группой $\mathbb{Z}_6$.

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*) $a = 20989$, $b = 2573$.

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

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.

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

$$\begin{aligned} P = \prod_{i=1}^{3}(x - \beta_i) &= (x+1)(x+\alpha)(x+\alpha+1) = \\ &= (x+1)\left(x^2 + \alpha x + x + \alpha x + \alpha^2 + \alpha\right) = \\ &= (x+1)\left(x^2 + x + \alpha^2 + \alpha\right) = \\ &= \left(x^3 + (\alpha+1)x^2 + (\alpha+1)x^2 + (\alpha^2+\alpha+1)x + \right. \end{aligned}$$

$$+\alpha^2+\alpha\big) \;=\; x^3+1,$$

и по теореме 2.21:

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

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

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.

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.

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 кольце $\mathbb{Z}_2[x]$ найти

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

Воспользуемся алгоритмом Евклида:

$$x^5 + x^2 + x + 1 = \left(x^2 + x\right)\left(x^3 + x^2 + x + 1\right) + \underline{\left(x^2 + 1\right)},$$

$$x^3 + x^2 + x + 1 = (x+1)\underline{\left(x^2+1\right)}.$$

Ответ: $x^2 + 1$.

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

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

1) построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов;
2) построить таблицу умножения элементов;
3) для каждого элемента поля указать обратные;
4) найти порождающие элементы поля;
5) найти минимальные многочлены всех элементов поля.

Поле $F = \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$ содержит 8 элементов: 0 и степени $1, \ldots, 7$ порождающего элемента α. Можно полагать $x = \alpha$, т. к. $a(x)$ — примитивный многочлен.

1. Таблица соответствий между полиномиальным и степенным представлением его ненулевых элементов:

$x^3 = x + 1$ степень x	1	x	x^2
x	0	1	0
x^2	0	0	1
$x^3 = x + 1$	1	1	0
$x^4 = x^2 + x$	0	1	1
$x^5 = x^2 + x + 1$	1	1	1
$x^6 = x^2 + 1$	1	0	1
$x^7 = 1$	1	0	0

2. Таблица умножения:

$\times$	x	x^2	x^3	x^4	x^5	x^6
x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1
x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1	x
x^3	x^2+x	x^2+x+1	x^2+1	1	x	x^2
x^4	x^2+x+1	x^2+1	1	x	x^2	$x+1$
x^5	x^2+1	1	x	x^2	$x+1$	x^2+x
x^6	1	x	x^2	$x+1$	x^2+x	x^2+x+1

3. Обратные элементы:

x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1
x^2+1	x^2+x+1	x^2+x	$x+1$	x^2	x

4. Поле F имеет $\varphi(7) = 6$ порождающих элементов: все кроме 0 и 1.

5. Находим м. м. элементов поля. Ясно, что

   - $m_0(x) = x$;
   - $m_1(x) = x + 1$;

- остальные элементы F суть порождающие его мультипликативной группы, и их м. м. будут совпадать с $a(x)$.

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

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.

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

В поле $\mathbb{F}_2$ имеем $x - 1 = x + 1$.

1. $f(1) = 0 \Rightarrow 1$ — корень f.
2. Делим $f(x)$ на $x + 1$, получаем
$$x^4 + x^3 + x + 1 = f_1(x).$$
3. $f_1(1) = 0 \Rightarrow 1$ — корень f_1; $\frac{f_1}{x+1} = x^3+1 = f_2(x)$.
4. $f_2(1) = 0 \Rightarrow 1$ — корень f_2; $\frac{f_2}{x+1} = x^2 + x + 1$.
5. Многочлен $x^2 + x + 1$ неприводим.

Ответ: $x^5 + x^3 + x^2 + 1 = (x + 1)^3 \left(x^2 + x + 1\right)$.

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

1. $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$,
$(x - 2) \equiv_5 (x + 3)$

2.
$$\begin{array}{rr|r}
x^3+2x^2+4x+1 & & x+3 \\
\cline{3-3}
x^3+3x^2 & & x^2+4x+2 \\
\cline{1-1}
\quad 4x^2+4x & & \\
\quad 4x^2+2x & & \\
\cline{1-1}
\qquad\quad 2x+1 & & \\
\qquad\quad 2x+1 & & \\
\cline{1-1}
\qquad\qquad\quad 0 & &
\end{array}$$

3. Перебором элементов $\mathbb{F}_5$ убеждаемся, что многочлен
x^2+4x+2 неприводим над $\mathbb{F}_5$.

Ответ: $x^3+2x^2+4x+1=(x+3)\left(x^2+4x+2\right)$.

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

1. 0, 1, 2 — не корни $f(x)$ $\Rightarrow$ $f(x)$ линейных делителей не содержит.
2. Неприводимые многочлены над $\mathbb{F}_3$ степени 2:
$$x^2+1,\quad x^2+x+2,\quad x^2+2x+2.$$
3. Подбором получаем
Ответ: $f(x)=x^4+x^3+x+2=$
$=\left(x^2+1\right)\left(x^2+x+2\right)$.

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

1. $f(x) \neq 0$ ни при каком $x = 0, 1, 2, 3, 4$, то есть $f(x)$ не имеет линейных делителей.

2. Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем

Ответ: $f(x) = \left(x^2 + x + 1\right)\left(x^2 + 2x + 4\right)$.

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

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

Перебором коэффициентов $b, c \in \{\,0,\ 1,\ 2\,\}$ в выражении x^2+bx+c, находим подходящие многочлены:

$$\begin{aligned} f_1(x) &= x^2 + 1, \\ f_2(x) &= x^2 + x + 2, \\ f_3(x) &= x^2 + 2x + 2. \end{aligned}$$

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

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

$$\begin{aligned} f_1(x) &= x^3 + 2x + 1, \\ f_2(x) &= x^3 + 2x + 2, \\ f_3(x) &= x^3 + x^2 + 2, \\ f_4(x) &= x^3 + 2x^2 + 1, \\ f_5(x) &= x^3 + x^2 + x + 2, \\ f_6(x) &= x^3 + x^2 + 2x + 1, \\ f_7(x) &= x^3 + 2x^2 + x + 1, \\ f_8(x) &= x^3 + 2x^2 + 2x + 2. \end{aligned}$$

2.18. Определить, является ли:

1. многочлен $a(x) = x^2 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2. элемент $4x^2 + 2$ — корнем $a(x)$ в факторкольце/поле $\mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$?

1. Перебором элементов из $\mathbb{F}_5$ —

$$a(0) = 4,\ a(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1,$$

убеждаемся, что квадратный многочлен $a(x)$ неприводим.

Следовательно, факторкольцо $\mathbb{F}_5[x]/\big(x^2 + 2x + 4\big)$ *является полем*; в нём $x^2 = -2x - 4 = 3x + 1$.

2. $a(4x^2 + 2) = \big(2(2x^2 + 1)\big)^3 + 2 \cdot 2(2x^2 + 1) + 4 =$
$= 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 =$
$= 4(3x + 1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + x + x^2 + 1 = 0$ — да, является.

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

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

1. $a(x) = x^2 + x - 1$, $a(0) = 6$, $a(1) = 1$, $a(2) = 5$, $a(3) = 4$, $a(4) = 6$, $a(5) = 1$, $a(6) = 6$, то есть многочлен $a(x)$ — *неприводим* в $\mathbb{F}_7$ и F — поле ($\cong \mathbb{F}_7^2$).

2. $\mathbb{F}_7^2 = \big\{\, ax + b \mid a, b \in \mathbb{F}_7,\ x^2 = 1 - x = 6x + 1 \,\big\}$

$$(ax + b) \cdot (6x + 1) = \ldots = (2a + 6b)x + (6a + b) = 1$$

$$\begin{cases} 6a+b &= 1 \\ a+3b &= 0 \end{cases} \Rightarrow \begin{cases} a=1 \\ b=2 \end{cases}$$

Ответ: $(1-x)^{-1} = x+2$ в F.

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

1) поля $F_1 = \mathbb{F}_2[x]/\big(x^4+x+1\big)$;
2) поля $F_2 = \mathbb{F}_2[x]/\big(x^4+x^3+1\big)$.

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

Мультипликативная группа указанных полей состоит из $2^4 - 1 = 15$ элементов.

Примарное разложение 15: $15 = 3 \cdot 5$, поэтому равенство $\beta^d = 1$ нужно проверить для $d = 15/5 = 3$ и $d = 15/3 = 5$.

1. $\underline{x^4 = x+1}$

$$\begin{aligned} \beta^2 &= x^2(x+1)^2 = x^4 + x^2 = x^2 + x + 1, \\ \beta^3 &= x(x+1)\left(x^2+x+1\right) = x\left(x^3+1\right) = \\ &= x^4 + x = x + 1 + x = 1. \end{aligned}$$

Ответ: В поле F_1 $\operatorname{ord}\beta = 3$.

2. $\underline{x^4 = x^3+1}$

$$\begin{aligned} \beta^2 &= x^4 + x^2 = x^3 + x^2 + 1, \\ \beta^3 &= x(x+1)\left(x^3+x^2+1\right) = \\ &= x\left(x^4+x^2+x+1\right) = x\left(x^3+x^2+x\right) = \\ &= x^4 + x^3 + x^2 = x^2 + 1 \neq 1, \\ \beta^5 &= x^2x^3 = \left(x^3+x^2+1\right)\left(x^2+1\right) = \end{aligned}$$

$$= \left(x^5 + x^4 + x^2 + x^3 + x^2 + 1\right) = \ldots$$
$$\ldots = \left(x^3 + 1\right) x = x^4 + x = x^3 + x + 1 \neq 1.$$

Ответ: В поле F_2 $\operatorname{ord}\beta = 15$.

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

Мультипликативная группа поля

$$\mathbb{F}_2[x]/\left(x^6 + x^3 + 1\right)$$

состоит из $2^6 - 1 = 63$ элементов.

Простые делители $63 = 3^2 \cdot 7$ суть 3 и 7, поэтому равенство $x^d = 1$ нужно проверить только для $d = 21 = \frac{63}{3}$ и $d = 9 = \frac{63}{7}$.

В рассматриваемом поле $x^6 = x^3 + 1$ и

$$x^9 = x^6 x^3 = \left(x^3 + 1\right) x^3 = x^6 + x^3 = \not{x}^3 + 1 + \not{x}^3 = 1.$$

Т.о. $\operatorname{ord} x = 9 \neq 63$ и многочлен $f(x)$ *не примитивен.*

2.22. Найти количество нормированных неприводимых многочленов

1) степени 7 над полем $\mathbb{F}_2$;
2) степени 6 над полем $\mathbb{F}_5$.

$$\sum_{d|n} d \cdot I_p^d = p^n.$$

1. $\underline{((7))\text{ над }\mathbb{F}_2}$

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

$((1)) = 2$: это x и $x+1$, отсюда $((7)) = \frac{128-2}{7} = 18$.

2. $\underline{((6)) \text{ над } \mathbb{F}_5}$

$$((6)) = \frac{1}{6}\sum_{d|6}\mu(d)\,5^{\frac{6}{d}} = \frac{1}{6}\left[\mu(1)5^6 + \mu(2)5^3 + \right.$$

$$\left. + \mu(3)5^2 + \mu(6)5\right] = \frac{15625 - 125 - 25 + 5}{6} = 2\,580.$$

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

С её помощью вычислить выражение

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

Поскольку $\operatorname{char} F = 3$, то $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

$F = \mathbb{F}_3^2$, F^* содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1,8}$ примитивного элемента α.

Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в $\mathbb{F}_3^2$ проводятся по $\bmod a(x)$, будем иметь

$$x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1.$$

Найдём порядок элемента x: т. к. $8 = 2^3$, $\frac{8}{2} = 4$, проверим равенство $x^4 = 1$:

$$x^4 = \left(x^2\right)^2 = (2x+1)^2 = x^2 + x + 1 =$$

$$= \cancel{2}x + 1 + \cancel{x} + 1 = 2 \neq 1,$$

то есть x — примитивный элемент F:
$\operatorname{ord} x = 8$ и $x^8 = 1$.

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над $\mathbb{F}_3$, иначе примитивный элемент поля F пришлось бы искать.

Теперь вычислим значение заданного выражения. Имеем $2^8 = 256 \equiv_3 1$, $x + 2 = -x^2$, $x^4 = 2$ и далее:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} =$$
$$= x^6 + x^4 = \left(x^2\right)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \not{1} + \not{2} =$$
$$= 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

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

В данном 9-элементном поле

$$x^2 + 1 = 0 \;\Rightarrow\; x^2 = -1 \equiv_3 2.$$

1. Найдём порядок элемента x, для чего проверим равенство $x^4 = 1$ (т. к. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = \left(x^2\right)^2 = 4 \equiv_3 1.$$

Следовательно $\operatorname{ord} x = 4$ и элемент x не является 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:

$$\alpha^1 = x+1, \qquad \alpha^5 = 2(x+1) = 2x+2,$$
$$\alpha^2 = x^2+2x+1 = 2x, \qquad \alpha^6 = \alpha^2 \cdot \alpha^4 = 4x = x,$$
$$\alpha^3 = 2x(x+1) = 2x+1, \qquad \alpha^7 = x(x+1) = x+2,$$
$$\alpha^4 = 4x^2 = x^2 = 2, \qquad \alpha^8 = (\alpha^4)^2 = 4 = 1.$$

Замечание: вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

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

Сначала убедимся, что многочлен $f(x) = x^2+x+2$ неприводим: ни одно из значений $f(x)$, $x \in \mathbb{F}_3$ не равно 0.

Далее проверим, является ли $f(x)$ делителем x^4+1?

$x^4+1 = \left(x^2+x+2\right)\left(x^2+2x+2\right)$ — да, является

Поэтому искомый идеал составят многочлены из R, кратные $f(x)$:

$$\left(x^2+x+2\right) = \left\{ \left(x^2+x+2\right)(ax+b) \mid a,b \in \mathbb{F}_3, x^4 = 1 \right\}.$$

Теперь проведём умножение:

$$\left(x^2+x+2\right)(ax+b) = ax^3+(a+b)x^2+(2a+b)x+2b.$$

Перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $\left(x^2+x+2\right)$:

a	b	$ax^3+(a+b)x^2+(2a+b)x+2b$
0	0	0
0	1	x^2+x+2
0	2	$2x^2+2x+1$
1	0	x^3+x^2+2x
1	1	x^3+2x^2+2
1	2	x^3+x+1
2	0	$2x^3+2x^2+x$
2	1	$2x^3+2x+2$
2	2	$2x^3+x^2+1$

А если бы $f(x) \not| a(x)$? Тогда в R существует идеал, порождённый элементом НОД$\,(f(x),a(x))$.

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

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

Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \;=\; \frac{1}{ad-bc}\cdot\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

1. Сначала вычислим $\det M = ad-bc$ с учётом $x^2=2x+2$:

$$\begin{aligned} \det M \;&=\; (3x+4)(3x+2)-(x+2)(x+3) \;= \\ &=\; 4x^2+3x+3-x^2-1 \;= \\ &=\; 3x^2+3x+2 \;=\; 3(2x+2)+3x+2 \;=\; 4x+3. \end{aligned}$$

2. Найдём обратный к $4x+3$ элемент, решая соотношение Безу

$$\left(x^2+3x+3\right)a(x)+(4x+3)b(x) \;=\; 1$$

с помощью обобщённого алгоритма Евклида:

Шаг 0. // *Инициализация*

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

Шаг 1. // *Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком*

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x)+r_0(x),\\ q_0(x) &= 4x+4,\\ r_0(x) &= 1,\ // \ \deg r_0 = 0 \ \Rightarrow \ \textit{ОСТАНОВ}\\ y_0(x) &= y_{-2}(x)-y_{-1}(x)q_0(x) =\\ &= -q_0(x) = -4x-4 = x+1. \end{aligned}$$

3. Вычислим обратную матрицу

$$M^{-1} \;=\; (x+1)\begin{bmatrix} 3x+2 & 4x+2\\ 4x+3 & 3x+4 \end{bmatrix} \;=\; \begin{bmatrix} x+2 & 1\\ 4x & 3x \end{bmatrix}.$$

2.27. Разложить на неприводимые множители многочлен

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

1. $f(0)=f(1)=1$, и значит $f(x)$ не имеет корней в $\mathbb{F}_2$, то есть не имеет линейных делителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.

Таковых над $\mathbb{F}_2$ только один — x^2+x+1.

При делении $f(x)$ на x^2+x+1, получаем

$$f(x) = \big(x^2+x+1\big)\cdot \big(\underbrace{x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1}_{g(x)}\big).$$

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:

$$x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = \big(x^3+x+1\big)\big(\underbrace{x^6+x^5+x^3+x^2+1}_{h(x)}\big) \quad \text{— делится!}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

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

Поскольку многочлен $h(x)$ 6-й степени не имеет делителей 3-й и меньших степеней, то он является неприводимым.

Ответ: В $\mathbb{F}_2[x]$ справедливо разложение

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = \left(x^2 + x + 1\right)\left(x^3 + x + 1\right)\left(x^6 + x^5 + x^3 + x^2 + 1\right).$$

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

1. Найдём разложение многочлена $f(x)$ на *неприводимые* множители над $\mathbb{F}_3$.

- Ищем корни: $f(0) = 2,\ f(1) = 1,\ f(2) = 0.$
  Поскольку $x - 2 \equiv_3 x + 1$, то
  $f(x) = (x + 1)\left(x^2 + 2x + 2\right)$.
- Многочлен $g(x) = x^2 + 2x + 2$ не имеет корней в $\mathbb{F}_3$, его степень 2, т. е. он неприводим.
- Окончательно: $f(x) = (x + 1)\left(x^2 + 2x + 2\right)$.

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над $\mathbb{F}_p$, то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —
  $$g(x) = (x-\alpha)\cdot(x - \alpha^p)\cdot\left(x - \alpha^{p^2}\right)\cdot\ldots\cdot\left(x - \alpha^{p^{n-1}}\right),$$
  где α – произвольный корень $g(x)$ в F;
- не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$.

В этом поле если α — корень $g(x)$, то и α^3 — тоже его корень. Вычисляем:

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

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 $\mathbb{F}_3[x]/\left(x^2+2x+2\right) = GF(3^2)$.

2.29. Найти м. м. для всех элементов β поля

$$F = \mathbb{F}_2[x]/\left(x^4+x+1\right).$$
$$\beta \in \{0, 1, \alpha, \ldots, \alpha^{14}\} = F, \quad x^4 = x+1.$$

$\beta = 0$: $m_0(x) = x$.

$\beta = 1$: $m_1(x) = x+1$.

$\beta = \alpha$: сопряжённые с α элементы — α^2, α^4, α^8 и

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = \ldots$$
$$\ldots = x^4 + x + 1 = 0.$$

Это означает, что x^4+x+1 — примитивный многочлен и $m_\alpha(x) = x^4 + x + 1$.

$\beta = \alpha^3$: сопряжённые с α^3 элементы суть α^6, α^{12}, $\alpha^{24} = \alpha^9$, их м. м. —

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = \\ = x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 + \\ + \left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2 + \\ + \left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x + \\ + \left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right) = x^4 + \left(\alpha^3 + (\alpha^3+\alpha^2) + (\alpha^3+\alpha) + \right. \\ \left. + (\alpha^3+\alpha^2+\alpha+1)\right)x^3 + (\ldots)\,x^2 + (\ldots)\,x + \alpha^{30} = \\ = x^4+x^3+x^2+x+1.$$

$\beta = \alpha^5$: 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. —

$$m_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) = \\ = x^4+x^3+1.$$

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

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

1. Любой многочлен в поле характеристики 5 вместе с корнем α^3 имеет корнями и все сопряжённые с ним элементы $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т. д.

2. В поле F имеем $\alpha^{5^2-1} = \alpha^{24} = 1$, и сопряжённым с α^3 будет только элемент α^{15}, т. к. $\alpha^{75} = \alpha^3$. Поэтому минимальный многочлен элемента α^3 — квадратный:

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2 - (\alpha^3+\alpha^{15})x + \alpha^{18}.$$

3. Найдём коэффициенты данного многочлена, учитывая $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = \\
&= 4(4\alpha+3) + 3\alpha = 4\alpha + 2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = \\
&= 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\
&= 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3, \\
\alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\
&= 4(4\alpha+3) + 4\alpha + 1 = 3.
\end{aligned}$$

Ответ: $m(x) = x^2 + 3$.

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

1. По одной формуле

$$\sum_{d|6} d\cdot I_2^d = 1\cdot I_2^1 + 2\cdot I_2^2 + 3\cdot I_2^3 + 3\cdot I_2^6 = 2^6 = 64.$$

Поскольку $I_2^1 = I_2^3 = 2$ и $I_2^2 = 1$, то

$$(64 - (2+2+6)/6) = 54/6 = 9.$$

2. По другой формуле

$$I_2^6 = \frac{1}{6}\sum_{d|6}\mu(d)\cdot 2^{\frac{6}{d}} =$$

$$= \frac{1}{6}\left[\,\mu(1)\cdot 2^6+\mu(2)\cdot 2^3+\mu(3)\cdot 2^2+\mu(6)\cdot 2^1\,\right] =$$

$$= \frac{1}{6}\left[\,64-8-4+2\,\right] = 54/6 = 9.$$

2.32. Примитивен ли элемент x в полях

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

1) Поскольку $|F_1^*| = 2^3-1 = 7$ — простое число, то каждый неединичный элемент мультипликативной группы F^* — примитивный, в т. ч. и x. Это означает, что x — *примитивный элемент* поля F и м.м. многочлен $a(x)$ примитивен.
2) Поскольку $|F_2^*| = 2^4-1 = 15 = 3\cdot 5$, то для определения значения $\operatorname{ord} x$ нужно проверить на равенства $x^3 = 1$ и $x^5 = 1$.

   Первое равенство явно не имеет места, поэтому вычисляем с учётом $x^4 = x^3+x^2+x+1$:

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

   Это означает, что $\operatorname{ord} x = 5 \neq 15$, x — *не есть примитивный элемент* F, а м.м. $a(x)$ не примитивен.

2.33. Найти корни многочлена

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

Вычисление значений $f(x)$ для $x = 0, 1, \ldots, 4$, показывает, что $f(3) = 0$, т. е. $x = 3$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 3 = x + 2$, получим $x^3 + 3x^2 + 4x + 4 = (x - 3) \cdot \big(x^2 + x + 2\big)$.

Перебором элементов $x \in GF(5)$ убеждаемся, что $f_2(x) = x^2 + x + 2$ — неприводимый многочлен.

В поле $\mathbb{F}_5[x]/\big(x^2 + x + 2\big)$ корни многочлена $f_2(x)$ суть $\{\, x,\, x^5 \,\}$ и $x^2 = -x - 2 = 4x + 3$.

Вычисляем:

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

Ответ: $\{\, 3,\, x,\, 4x + 4 \,\}$.

2.34. Является ли многочлен

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

примитивным?

Подстановкой в $f(x)$ всех элементов $0, \ldots, 4$ поля $\mathbb{F}_5$ убеждаемся, что данный многочлен 2-й степени не имеет линейных делителей и, следовательно, *неприводим*.

Порядок мультипликативной группы $GF(5^2)$ есть $24 = 2^3 \cdot 3$. Определим порядок элемента её x, для которого $x^2 = -x - 2 = 4x + 3$.

Поскольку простые делители 24 суть 2 и 3, проверим равенство $x^d = 1$ для $d = 24/2 = 12$, $24/3 = 8$. Вычисляем:

$$
\begin{aligned}
x^4 &= \left(x^2\right)^2 = (4x+3)^2 = x^2+4x+4 = \ldots \\
&\ldots = 3x+2 \neq 1, \\
x^8 &= \left(x^4\right)^2 = (3x+2)^2 = -x^2+2x+4 = \ldots \\
&\ldots = 3x+1 \neq 1. \\
x^{12} &= x^8 x^4 = (3x+1)(3x+2) = -x^2+4x+2 = \ldots \\
&\ldots = 4 \neq 1.
\end{aligned}
$$

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\left(x^2+x+2\right)$.

2.35. Для бинома $x^{40}-1 \in \mathbb{F}_5[x]$ определить количество и степени неприводимых сомножителей.

В каком минимальном поле расширения $\mathbb{F}_5[x]$ данный бином раскладывается на линейные множители?

Поскольку $n = 40 = 5 \cdot 8$, то корни бинома $x^{40}-1$ суть все корни x^8-1 (они все различны), но 5-й кратности.

Рассмотрим разложение многочлена x^8-1 над $\mathbb{F}_5$. Относительно умножения на 5 вычеты по модулю 8 $\{\overline{0}, \overline{1}, \ldots, \overline{7}\}$ разбиваются на орбиты:

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

Пояснение: $5 \cdot 5 = 25 \equiv_8 1$, $2 \cdot 5 = 10 \equiv_8 2$ и т. д.

Поэтому:

- бином $x^8-1 \in \mathbb{F}_5[x]$ разлагается в произведение четырёх линейных и двух неприводимых квадратных многочленов;

- бином $x^{40}-1=\left(x^8-1\right)^5$ разлагается в произведение двадцати многочленов степени 1 (четырёх кратности 5 каждый) и десяти неприводимых многочленов степени 2 (двух кратности 5 каждый);
- максимальная степень неприводимых делителей-многочленов есть 2, следовательно полем расширения данного бинома будет $\mathbb{F}_5^2$.

Замечание. В данном случае разложение бинома $x^8-1\in\mathbb{F}_5[x]$ на неприводимые множители легко находится (первые три равенства справедливы в любом кольце):

$$\begin{aligned}
x^8-1 &= \left(x^4-1\right)\left(x^4+1\right),\\
x^4-1 &= \left(x^2-1\right)\left(x^2+1\right),\\
x^2-1 &= (x-1)(x+1),\\
x^2+1 &\equiv_5 x^2-4=(x-2)(x+2),\\
x^4+1 &\equiv_5 x^4-4=\left(x^2-2\right)\left(x^2+2\right).
\end{aligned}$$

Итого в $\mathbb{F}_5[x]$:

$$x^8-1=(x+1)(x-1)(x+2)(x-2)\cdot\left(x^2+2\right)\left(x^2-2\right).$$

И далее

$$x^{40}-1=(x+1)^5(x-1)^5(x+2)^5(x-2)^5\cdot\left(x^2+2\right)^5\left(x^2-2\right)^5.$$

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

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

$\deg f(x) = 2$ и поэтому $f(x)$ имеет 2 корня.

(1) Полином $f(x)$ неприводим над $\mathbb{F}_2 \Rightarrow$ его корни суть x и x^2.

(2) Полином $f(x)$ приводим над $\mathbb{F}_3$:

$$x^2 + x + 1 \;=\; x^2 - 2x + 1 \;=\; (x-1)^2,$$

поэтому $f(x)$ над $\mathbb{F}_3$ имеет корень 1 степени 2.

(3) Полином $f(x)$ неприводим над $\mathbb{F}_5 \Rightarrow$ его корни x и x^5.

2.37. Найти корни многочлена

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

Вычисляем значения $f(x)$ для всех x из $\mathbb{F}_5 = \{\,0,\,1,\,2,\,3,\,4\,\}$: $f(0) = 4$, $f(1) = 1$, $f(2) = 0$ и, таким образом, $x = 2$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 2 = x + 3$, получим $\quad 2x^4 + x^3 + 4x^2 + 4 = (x+3)\cdot(2x^3 + 4x + 3)$.

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[2)].

[2)] а если бы это был многочлен 4-й степени?

В поле $\mathbb{F}_5[x]/\big(x^3+2x+4\big)$ корнями многочлена $f_2(x)=0$ будут $x,\ x^5,\ x^{25}$.

Вычисляем — с учётом $x^3=-2x-4=3x+1$:

$$\begin{aligned} x^5 &= x^2(3x+1) = 3x^3+x^2 = 4x+3+x^2 = \\ &= x^2+4x+3; \\ x^{25} &= \big(x^5\big)^5 = \big(x^2+4x+3\big)^5 = x^{10}+4^5x^5+3^5 = \\ &= x^{10}+4\big(x^2+4x+3\big)+3 = x^{10}+4x^2+x. \end{aligned}$$

(поскольку $4^5=2^{10}=1024$ и $3^5=81\cdot 3=243$).

Найдём отдельно x^{10}:

$$\begin{aligned} x^{10} &= \big(x^5\big)^2 = \big(x^2+4x+3\big)^2 = \\ &= x^4+x^2+3^2+3x^3+4x+x^2 = \\ &= x^4+3x^3+2x^2+4x+4 = \\ &= 3x^2+x+4x+3+2x^2+4x+4 = 4x+2. \end{aligned}$$

Продолжаем:

$$x^{25} = x^{10}+4x^2+x = 4x+2+4x^2+x = 4x^2+2.$$

Ответ: уравнение $f(x)=2x^4+x^3+4x^2+4=0$, где $f(x)\in\mathbb{F}_5[x]$ имеет корни 2, x, x^2+4x+3, $4x^2+2$ в поле $F=\mathbb{F}_5[x]/\big(x^3+2x+4\big)$ (поскольку корень $2\in F$).

2.38. Найти корни многочлена

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

В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{\left(x^4+x^3+1\right)}_{f_1(x)}\underbrace{\left(x^4+x^3+x^2+x+1\right)}_{f_2(x)}.$$

Уравнения $f_1(x)=0$ и $f_2(x)=0$ ранее были решены: их корни соответственно суть

$$x,\ x^2,\ x^3+1,\ x^3+x^2+x$$
$$\text{в поле } F_1 = \mathbb{F}_2[x]/\left(x^4+x^3+1\right)$$

$$\text{и}\quad x,\ x^2,\ x^3,\ x^3+x^2+x+1$$
$$\text{в поле } F_2 = \mathbb{F}_2[x]/\left(x^4+x^3+x^2+x+1\right).$$

Степени обоих расширений поля $GF(2)$ совпадают и поля F_1 и F_2 изморфны, т. о. все 8 корней уравнения $f(x)=0$ лежат в поле $GF(2^4)$.

Для записи данных корней выберем представление F_1 поля $GF(2^4)$. Тогда запись корней $f_1(x)$ останется без изменений, а корни $f_2(x)$ надо представить как элементы F_1.

Приравнивая многочлены, порождающие данные поля, получим

$$x^4+x^3+1 = x^4+x^3+x^2+x+1 \ \Rightarrow\ x^2+x = x(x+1) = 0.$$

Ясно, что при подстановке $x \mapsto x+1$ полученное равенство останется справедливым. Применим данную

подстановку для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле F_1:

$$\begin{gathered} x \mapsto x+1, \\ x^2 \mapsto (x+1)^2 = x^2+1, \\ x^3 \mapsto (x+1)^3 = x^3+x^2+x+1, \\ x^3+x^2+x+1 \mapsto \left(x^3+x^2+x+1\right)+\left(x^2+1\right)+ \\ +(x+1)+1 = x^3. \end{gathered}$$

Проверим, что, например, x^2+1 — корень $f(x)$:

$$\begin{aligned} f\left(x^2+1\right) &= \left(x^2+1\right)^8+\left(x^2+1\right)^4+\left(x^2+1\right)^2+ \\ &+\left(x^2+1\right)+1 = \\ &= \left(x^{16}+1\right)+\left(x^8+1\right)+\left(x^4+1\right)+x^2. \end{aligned}$$

Очевидно $x^{16} = x$, $x^4 = x^3+1$ и
$x^8 = \left(x^3+1\right)^2 = x^6+1$.
Поскольку $x^5 = x^4+x = x^3+x+1$, то
$x^6 = x^4+x^2+x = x^3+x^2+x+1$ и $x^8 = x^3+x^2+x$.

Подставляя в выражение для $f\left(x^2+1\right)$ полученные полиномиальные представления степеней x, получим

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

Ответ: многочлен $f(x) = x^8+x^4+x^2+x+1 \in \mathbb{F}_2[x]$ имеет в поле $\mathbb{F}_2[x]/\left(x^4+x^3+1\right)$ корни x, x^2, x^2+1, x^3, x^3+1, x^3+x^2+x, $x+1$, x^3+x^2+x+1.

2.39. Найти корень многочлена

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

Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных:

$$f(x) = x^4+2x+2 = \left(x^2+ax+b\right)\left(x^2+cx+d\right) = \\ = x^4+cx^3+dx^2x+ax^3+acx^2+adx+bx^2+bcx+bd = \\ = x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd.$$

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.

Т.о. полином $f(x)$ над $\mathbb{F}_3$ *неприводим*.

Теперь рассмотрим поле $\mathbb{F}_3[x]/\left(x^4+2x+2\right)$.

В нём $f(x)=x^4+2x+2=0$, то есть $x^4=x+1=0$, и корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3}.

Вычислим x^9 и x^{27}:

$$x^9 = \left(x^4\right)^2 x = (x+1)^2x = x^3+2x^2+x;$$
$$x^{27} = \left(x^9\right)^3 = \left(x^3+2x^2+x\right)^3 = x^9+2x^6+x^3 = \\ = \ldots = x^3+x^2+x.$$

Ответ: полином $f(x)=x^4+2x+2$ имеет корни x, x^3, x^3+2x^2+x, x^3+x^2+x в поле $\mathbb{F}_3[x]/(f)$.

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

Поскольку $f(0) = f(1) = 1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

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

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\left(x^5 + x^2 + 1\right)$. В нём $f(x) = x^5 + x^2 + 1 = 0$, то есть $x^5 = x^2 + 1 = 0$ и его корни суть x, x^2, x^{2^2}, x^{2^3}, x^{2^4}.

Вычислим x^8 и x^{16}:

$$\begin{aligned} x^8 &= x^5x^3 = \left(x^2+1\right)x^3 = x^5 + x^3 = x^3 + x^2 + 1; \\ x^{16} &= \left(x^8\right)^2 = \left(x^3 + x^2 + 1\right)^2 = x^6 + x^4 + 1 = \\ &= x^5x + x^4 + 1 = (x^3 + x) + x^4 + 1 = \\ &= x^4 + x^3 + x + 1. \end{aligned}$$

Ответ: в поле $\mathbb{F}_2[x]/\left(x^5 + x^2 + 1\right)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

имеет корни x, x^2, x^4, $x^3 + x^2 + 1$, $x^4 + x^3 + x + 1$.

3. Коды, исправляющие ошибки

3.1. Построить порождающую G и проверочную H матрицы для

1) тривиального кода утраивания;

2) кода проверки на чётность.

1. Код утраивания является линейным $(3,1)$-кодом, у которого

$$G_{1,3} = \begin{bmatrix} 1\ 1\ 1 \end{bmatrix},\ I_1 = \begin{bmatrix} 1 \end{bmatrix},\ P_{1,2} = \begin{bmatrix} 1\ 1 \end{bmatrix},$$
$$P^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix},\ I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ H_{2,3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

2. Код проверки задаётся порождающей матрицей

$$G = \begin{bmatrix} 100\ldots1 \\ 010\ldots1 \\ \ldots \\ 00\ldots11 \end{bmatrix}$$

или проверочной матрицей

$$H = \begin{bmatrix} 1\ldots1\ I \end{bmatrix} = \begin{bmatrix} 11\ldots1 \end{bmatrix}.$$

3.2. Для кода Хемминга, заданного своей проверочной матрицей

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

требуется

1) построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;

2) найти такое кодирование для сообщений

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

Проверочная матрица H имеет размерность 3×7, и код при длине $n = 7$ содержит $m = 3$ проверочных и $k = 7 - 3 = 4$ информационных бит.

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P & I_4 \end{bmatrix}$.

Матрицу P можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P^T \end{bmatrix}$, 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.

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

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

кода.

3.3. Циклический $[9, 3]$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние d, а также осуществить систематическое кодирование полинома

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

Для определения кодового расстояния найдём все кодовые слова:

$$\begin{aligned} v(x) &= g(x)(ax^2 + bx + c) = \\ &= \left(x^6 + x^3 + 1\right)\left(ax^2 + bx + c\right) = \\ &= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c. \end{aligned}$$

В векторном виде все кодовые слова представляются как

$$[\,a,\,b,\,c,\,a,\,b,\,c,\,a,\,b,\,c\,].$$

Это код трёхкратного повторения, и $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$u(x) \mapsto v(x) = x^6 u(x) + r(x).$$

1) Вычисляем $x^6 u(x) = x^6\left(x^2 + x\right) = x^8 + x^7$.

2) Находим остаток $r(x)$ от деления $x^6 u(x)$ на $g(x)$:

$$\begin{array}{l|l} x^8 + x^7 & x^6 + x^3 + 1 \\ \cline{2-2} x^8 \quad + x^5 \quad + x^2 & x^2 + x \\ \cline{1-1} \quad x^7 + x^5 \quad + x^2 & \\ \quad x^7 \quad + x^4 \quad + x & \\ \cline{1-1} \quad x^5 + x^4 + x^2 + x & \end{array}$$

Т. о. $r(x) = x^5 + x^4 + x^2 + x$ и

$$v(x) = x^8 + x^7 + x^5 + x^4 + x^2 + x \leftrightarrow [0\,1\,1\,0\,1\,1\,\underline{0\,1\,1}]^T.$$

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

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,
3) $w_3(x) = x^6 + x^3 + x^2 + x$.

Декодирование систематического кода Хэмминга можно провести делением принятого полинома на порождающий: остаток от деления определяет синдром s с учётом таблицы соответствий между полиномиальным и степенным представлением элементов рассматриваемого поля со с. 221):

Находим позицию j ошибки.

1. $x^6 + x^2 + x = \left(x^3 + x + 1\right)^2 + \underline{x + 1}$, $j = 3$.

   Действительно,

$$w(\alpha) = \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1.$$

2. $x^6 + x^5 + x^3 + x^2 + x = \\ = \left(x^3 + x^2 + x + 1\right)\left(x^3 + x + 1\right) + \\ + \underline{x^2 + x + 1}$, $j = 5$;

   Действительно,

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

3. $x^6 + x^3 + x^2 + x \;=\; \bigl(x^3 + x\bigr)\bigl(x^3 + x + 1\bigr) + \underline{0}$, т. е. ошибки не произошло.

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

Имеем $\alpha^{31} = 1$ и разложение F^* над $\mathbb{F}_2$ есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8\, \alpha^{16}\},$$
$$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}, \{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\},$$
$$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}, \{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\},$$
$$\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}.$$

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

Будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов данного поля со с. 52.

С её помощью вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\
&= (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\
&= \alpha^3 + \alpha + 1 = \alpha^7, \\
s_2 &= w(\alpha^2) = \bigl(w(\alpha)\bigr)^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \bigl(w(\alpha^2)\bigr)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1.$$

Решим соотношение Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) \;=\; \lambda(x), \quad \deg\lambda(x) \leqslant 2.$$

с помощью обобщённого алгоритма Евклида:

Шаг 0. $r_{-2}(x) \;=\; x^5,$
$r_{-1}(x) \;=\; s(x),$
$\sigma_{-2}(x) \;=\; 0,$
$\sigma_{-1}(x) \;=\; 1.$

Шаг 1. $r_{-2}(x) \;=\; r_{-1}(x)q_0(x) + r_0(x),$
$q_0(x) \;=\; \alpha^2 x,$
$r_0(x) \;=\; s(x),$
$\sigma_0(x) \;=\; -q_0(x) \;=\; \alpha^2 x.$

Шаг 2. $r_{-1}(x) \;=\; r_0(x)q_1(x) + r_1(x),$
$q_1(x) \;=\; \alpha^{12}x + \alpha^5,$
$r_1(x) \;=\; \alpha^{14}x^2 + 1,$
$\deg r_1(x) = 2 \leqslant r,$
$\sigma_1(x) \;=\; \sigma_{-1}(x) - \sigma_0(x)q_1(x) \;=$
$= \; 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) \;=$
$= \quad \underbrace{\alpha^{14}x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} \quad = \sigma(x).$

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

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок есть

$$\sigma(x) \;=\; \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить *позиции ошибок* в $w(x)$.

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.

Имеем $n = 31 = 2^5 - 1$, $t = 5$, $\delta - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни α, α^2, α^3, α^4, α^5, α^6, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $C_1 = \{\, \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16} \,\}$.

При решении задачи 3.5 на с. 253 о разложение F^* на классы было установлено, что эти классы также будут пятиэлементными:

$$C_2 = \left\{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17} \right\};$$
$$C_3 = \left\{ \alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18} \right\}.$$

На с. 39 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[3)] 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 —

[3)] например, [8], Том 1, Таблица С.

$$\left(x^5+x^4+x^3+x+1\right)\Big|_{x=\alpha^5} = \alpha^{25}+\alpha^{20}+\alpha^{15}+\alpha^5+1 =$$
$$= (\alpha^3+1)^5+(\alpha^3+1)^4+(\alpha^3+1)^3+\alpha^5+1 = \ldots = 0.$$

Таким образом,
$g_2(x) = x^5+x^3+x^2+x+1,\ g_{\alpha^5}(x) = x^5+x^4+x^3+x+1$
и порождающий многочлен для $(31, 16, 7)$-кода БЧХ есть

$$g(x) = g_1(x)\cdot g_2(x)\cdot g_3(x) =$$
$$= x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1,$$
$$\deg g(x) = m = 15,\ k = n-m = 16.$$

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

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить позиции ошибок в данном слове.

Для вычислений в поле F нам понадобится таблица, уже построенная на с. 52.

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x + \alpha^{15} = \alpha^6 x + 1 = (\alpha^3+\alpha^2)\,x + 1:$$
$$\sigma(\alpha) = \alpha^4+\alpha^3+1 = \alpha+\alpha^3 \neq 0;$$
$$\sigma(\alpha^2) = \alpha^5+\alpha^4+1 = \alpha^2+\alpha+\alpha+1+1 = \alpha^2 \neq 0;$$
$$\ldots\ldots$$
$$\sigma(\alpha^9) = \alpha^{12}+\alpha^{11}+1 =$$
$$= (\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+1 = \mathbf{0}.$$

Замечание. Рассмотрен общий подход к определению корня полинома локаторов ошибок. Но в данном

случае всё сильно упрощается: полином $\sigma(x)$ линеен и поэтому имеет лишь один корень

$$x = \alpha^{-6} = \alpha^9.$$

Находим позицию единственной ошибки:

$$-9 \equiv_{15} 6.$$

4. Алгебраические основы криптографии

4.1. 1. Решить комбинаторную задачу.

Пусть p — простое число, большее 2. Сколько существует способов C раскрасить вершины правильного p-угольника в a цветов, если раскраски, получающиеся совмещением при вращении многоугольника вокруг своего центра, считать одинаковыми?

2. На основе полученного решения доказать малую теорему Ферма.

Теорема 4.18 (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 $a^{p-1} \equiv_p 1$.

4.2. В системе шифрования RSA по данным модулю $n = 91$ и экспоненте $e = 29$ найти ключ расшифрования d.

Заметим сначала, что значения $n = 91$ и $e = 29$ взаимно просты.

Найдём разложение $n = pq$ и значение функции Эйлера модуля:

$$91 = 7 \cdot 13; \quad \varphi(91) = 6 \cdot 12 = 72.$$

Число $e = 29$ не имеет общих делителей ни с $n = 91$, ни с $\varphi(n) = 72$, и значит годится в качестве ключа зашифрования.

Найдём d из условия $d \cdot 29 \equiv_{72} 1$ по алгоритму GE-InvZm:

1	72	0		
2	29	1	$q = 2$	(58 2)
3	14	-2	$q = 2$	(28 -4)
4	1	**5**	$q = 14$	
5	0			

Откуда $d = 5$.

4.3. 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.

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:

$$\begin{aligned} x_1 &= 01^{11} = 1 \equiv_{21} 1, \\ x_2 &= 11^{11} = 285311670611 \equiv_{21} 2, \\ x_3 &= 12^{11} = 743008370688 \equiv_{21} 3. \end{aligned}$$

4.4. Решить сравнения

а) $6^x \equiv_{11} 2$; б) $8^x \equiv_{11} 3$; в) $2^x \equiv_{13} 3$.

Используем алгоритм согласования (см. с. 169).

(а) $\underline{6^x \equiv_{11} 2}$. Имеем $p = 11$, $a = 6$, $b = 2$.

1. $H = \lceil \sqrt{11} \rceil = 4$.
2. $6^4 = 1\,296 \equiv_{11} 9 = c$ $(1296 = 117 \cdot 11 + 9)$.
3. $u = 1, 2, 3, 4$

u	1	2	3	4
9^u	9	$9 \cdot 9 = 81$	$4 \cdot 9 = 36$	$3 \cdot 9 = 27$
$9^u \pmod{11}$	9	4	3	5

4. $v = 0, \ldots, 4$

v	0	1	2	3	4
6^v	1	6	36	216	1296
$2 \cdot 6^v$	2	12	72	432	2592
$2 \cdot 6^v \pmod{11}$	9	1	6	3	7

5. Совпал элемент 3 таблиц при $u = 3$ и $v = 3$. Отсюда $Hu - v = 4 \cdot 3 - 3 \equiv_{10} 9$.

Ответ: $x = 9$.

(б) $\underline{8^x \equiv_{11} 3}$. Имеем $p = 11$, $a = 8$, $b = 3$.

1. $H = 4$.
2. $8^4 = 4\,096 \equiv_{11} 4 = c$.

u	1	2	3	4
3. 4^u	4	$4 \cdot 4 = 16$	$5 \cdot 4 = 20$	$9 \cdot 4 = 36$
$4^u \pmod{11}$	4	5	9	3

4.

v	0	1	2	3	4
8^v	1	8	64	512	4096
$3 \cdot 8^v$	3				
$3 \cdot 8^v \pmod{11}$	3				

5. Совпал элемент 4 таблиц при $u = 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 4 = 16 \equiv_{10} 6$.

Ответ: $x = 6$.

(в) $2^x \equiv_{13} 3$. Имеем $p = 13$, $a = 2$, $b = 3$.

1. $H = 4$.

2. $2^4 = 16 \equiv_{13} 3 = c$.

3.

u	1	2	3	4
c^u	3	9	27	3
$c^u \pmod{13}$	**3**	9	1	3

4.

v	0	1	2	3	4
2^v	1				
$3 \cdot 2^v$	3				
$3 \cdot 2^v \pmod{11}$	**3**				

5. Совпал элемент 3 таблиц при $u = 1, 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 1 = 4$, или $4 \cdot 4 \equiv_{12} 4$.

Ответ: $x = 4$.

4.5. 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}.

$$X_A = 2^5 = 32 \equiv_{23} 9;$$

$$X_B = 2^{17} = 131\,072 \equiv_{23} 18;$$

$$X_C = 2^{12} = 4\,096 \equiv_{23} 2;$$

$$K_{AB} = X_A^{17} = 9^{17} = 16\,677\,181\,699\,666\,569 \equiv_{23} 3;$$

$$K_{AC} = X_A^{12} = 9^{12} = 282\,429\,536\,481 \equiv_{23} 9;$$

$$K_{BC} = X_B^{12} = 18^{12} = 1\,156\,831\,381\,426\,176 \equiv_{23} 18.$$

4.6. 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 $y_2 = 03$.

Определим модуль $n = pq = 11 \cdot 17 = 187$. При этом экспонента $e = 13$ взаимно проста с $p - 1 = 10$ и $q - 1 = 16$. Открытый ключ есть пара $(187, 13)$.

Определим ключ расшифрования d. Вычислив $\varphi(n) = (p-1)(q-1) = 160$, решим сравнение

$$d \cdot 13 \equiv_{160} 1.$$

1	160	0		
2	13	1	$q = 12$	$(\ 156\ 12\ )$
3	4	-12	$q = 3$	$(\ 12\ \ -36)$
4	1	**37**	$q = 4$	
5	0			

Получаем $d = 37$.

Расшифровываем криптограммы 02 и 03:

$$x_1 = 2^{37} = 137\,438\,953\,472 \equiv_{187} 117,$$
$$x_2 = 3^{37} = 450\,283\,905\,890\,997\,363 \equiv_{187} 141.$$

Список литературы

1. *Авдошин С. М., Набебин А. А.* Дискретная математика. Модулярная алгебра, криптография, кодирование. — М.: ДМК Пресс, 2017.

2. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. — М.: КомКнига, 2006.

3. *Гоппа В. Д.* Новый класс линейных корректирующих кодов // Проблемы передачи информации. — Том VI, вып. 3, 1970, с. 24–30.

4. *Введение* в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.

5. *Вернер М.* Основы кодирования. Учебник для ВУЗов. — М: Техносфера, 2004.

6. *Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н.* Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.

7. *Касами Т., Токура Н., Ивадари Ё., Инагаки Я.* Теория кодирования. — М.: Мир, 1978.

8. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. — М.: Мир, 1988.

9. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.

10. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

11. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.

12. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.