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

Конспект лекций по курсу

ПРИКЛАДНАЯ АЛГЕБРА

алгебраические основы кодирования и шифрования

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

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

2019

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. И, наконец, нет такого правила, которое бы я не нарушил ради достижения большей выразительности. 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.

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

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 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 «кваизиопеделения» 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 уменьшенном 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.

С. И. Гуров

epAA3-00-1(Cont)

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*:

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

1) $(x \circ y) \circ z = x \circ (y \circ z)$ — *ассоциативность*;
2) $e \circ x = x \circ e = x$ — *свойство нейтрального элемента*;
3) $\forall\, x\, \exists!\, y : \; y \circ x = x \circ y = e$ — *существование обратных элементов* ко всем $x \in G$.

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

[1] как и все прочие алгебраические системы

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

Степень элемента при мультипликативной записи:

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

при которой справедливы обычные свойства степени:

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

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

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

Пример 1.2. Таблица умножения группы V_4.

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

— четверная группа Клейна

$$V_4 = \{e, a, b, c\}$$

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

Пример 1.3. 1. Четверная группа Клейна абелева.

2. *Числовые группы* — все они абелевы:

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

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

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

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

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

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

Ясно, что прямая сумма — абелева группа.

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

$$a^n = e.$$

[2)] Перестановки записываются в виде из разложения на циклы, сначала выполняется 2-я перестановка, потом — 1-я.

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

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

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

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

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

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

Теорема 1.4 (Лагранж). *Порядок подгруппы H конечной группы G делит порядок самой группы:*

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

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

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

Для коммутативных групп имеется усиление.

Теорема 1.5. *Пусть m — максимальный порядок элемента в конечной абелевой группе G. Тогда порядок любого элемента G делит m.*

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

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

Утверждение 1.6 (*о разложении группы на смежные классы*). *Левые смежные классы с разными представителями либо не пересекаются, либо совпадают и в совокупности составляют всю группу. То же справедливо и для правых смежных классов.*

Поскольку смежные классы группы по подгруппе либо не пересекаются, либо совпадают, то отображение $ah \leftrightarrow bh$, $h \in H \leqslant G \ni a, b$ является биекцией, откуда следует равномощность всех классов по данной подгруппе. Если $\forall\, x \in G$ всегда $xH = Hx$, то подгруппу H называют *нормальной*. Ясно, что, например, *в абелевой группе все подгруппы нормальны*.

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

Определение 1.7. 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*, 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 сохраняет групповую операцию: для любых $a, b \in G$ справедливо

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

Если существует изоморфизм между двумя группами, то они называются *изоморфными*, символически $G \cong G'$.

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

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

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

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

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

то такая группа называется *циклической*, а сам элемент a — *порождающим* (*образующим, генератором*).

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

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

Для циклических групп возможны два случая.

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

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

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

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

$$\operatorname{ord} a = |C| = n.$$

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, $\varphi(6) = \bigl|\{1, 5\}\bigr| = 2$.

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,

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

$\varphi(n)$	+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

1.2 Кольца и поля

Кольца: определение, основные свойства

<u>Определение</u> 1.11. Абелева группа $\langle\, R, +, 0 \,\rangle$ называется *кольцом*, символически $\langle\, R, +, \cdot, 0 \,\rangle$, если на ней определена бинарная операция *умножения* $\cdot$, связанная со сложением $+$ *дистрибутивными законами*

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

Дистрибутивные законы обеспечивают тот факт, что нейтральный элемент по сложению 0 будет являться одновременно нулём по умножению: для любого элемента x кольца справедливо $x \cdot 0 = 0$[3].

Отметим, что в кольце деление не постулируется.

Классическими примерами колец являются

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

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*, рассматривая его элементы как остатки от деления целых на n, и результаты обычных операций сложения и умножения берутся по $\mathrm{mod}\ n$[4].

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

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

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

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

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

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

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

Например, в кольце целых $\mathbb{Z}$ обратимы порождающие элементы $+1$ и -1.

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

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

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

Определение 1.14. 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 умножения на обратимые элементы представляется в виде произведения *неразложимых* элементов, называется *факториальным* или *кольцом с однозначным разложением на множители*.

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

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

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

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

Подкольцо *собственное*[5)], если оно не совпадает со всем кольцом.

Идеалы колец и факторкóльца. Важнейшими подкольцами являются так называемые идеалы.

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

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

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

[5)] 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.

Можно определить сумму и произведение идеалов и работать 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

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

Легко проверить, что вышеопределённое подмножество I кольца R действительно является его идеалом.

Во-первых, замкнутость I относительно операций сложения и умножения очевидна, а дистрибутивность умножения относительно сложения сохраняется. Таким образом, I — подкольцо R. Во-вторых, $x \in I \Leftrightarrow x = ua$, $\forall\, y \in R \;\Rightarrow\; x \cdot y = uya \in I$.

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

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

Примеры КГИ:

- Кольцо целых $\mathbb{Z}$ — все его идеалы имеют вид $(n) = n\mathbb{Z} = \{\, 0, \pm n, \pm 2n, \dots \,\}$.
- Кольцо $\mathbb{Z}_n$ — любой ненулевой идеал содержит НОД своих ненулевых элементов и им порождается.
  Например, для $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$: $\mathbb{Z}_6 = (1)$, $\{0, 2, 4\} = (2)$, $\{0, 3\} = (3)$ 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 матриц порядка n: совокупность матриц, у которых все столбцы, кроме первого — нулевые.

Определение 1.18. *Максимальным идеалом* коммутативного кольца называется всякий его собственный идеал, не содержащийся ни в каком другом собственном идеале.

В нетривиальном коммутативном кольце всегда существует максимальный идеал.

Пример 1.19. В кольце $\mathbb{Z}$

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

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

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

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

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

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

В качестве образующего класса вычетов $\overline{r}$ может быть выбран любой элемент из $\overline{r}$.

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 r — *представитель класса*, остаток от деления некоторого целого на n, $0 \leqslant r \leqslant n-1$.

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 $\mathbb{Z}_p$ при простом p есть поле.

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

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

Определение 1.21. Целостное кольцо $\langle R, +, \cdot, 0, 1 \rangle$ называется *евклидовым*, если для каждого его *ненулевого* элемента a определена *норма* $N(a) \in \mathbb{N}$ такая, что для любого элемента $b \neq 0$ существуют такие элементы q и r, что

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

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

Пример 1.22.

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

Все евклидовы кольца — КГИ.

Поля

Определение 1.23. Целостное кольцо, в котором все ненулевые элементы обратимы, называется *полем*[6].

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

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

Подмножество поля K, само являющееся полем и устойчивое относительно сужения на него операций из K, называется *подполем.* Примеры бесконечных полей и их подполей — числовые поля

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

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

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

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

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$;
2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

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

Иерархия колец:

$$\begin{array}{c}
\boxed{\text{ассоциативно-коммутативные}} \\
\downarrow \\
\boxed{\text{целостные}} \\
\downarrow \\
\boxed{\text{факториальные}} \\
\downarrow \\
\boxed{\text{КГИ}} \\
\downarrow \\
\boxed{\text{евклидовы}} \\
\downarrow \\
\boxed{\text{поля}}
\end{array}$$

1.3 Векторные пространства, гомоморфизмы, сравнения

Абстрактные векторные пространства

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

- $V = \{\,0, v, \ldots\,\}$ — множество *векторов*, являющееся коммутативной группой по сложению $(+)$ с нулевым элементом 0;

- $\cdot$ — бинарная операция *умножения элемента* («чисела́») *из* K *на вектор из* V: $K \times V \dot{\to} V$,

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

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

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

Например, булев куб $B^n = \{0, 1\}^n$ — n-мерное координатное пространство над полем $\mathbb{Z}_2 = \{0, 1\}$ с операциями сложения по $\mathrm{mod}\ 2$, умножения $\&$ и нулевым элементом $\widetilde{0}$.

n-мерное координатное пространство V над полем K имеет n-элементный базис, при этом обычно используют *естественный базис*:

$$\boldsymbol{e}_1 = [\ 1,\ 0,\ \ldots,\ 0\ ],\ \ldots,\ \boldsymbol{e}_n = [\ 0,\ 0,\ \ldots,\ 1\ ].$$

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 (АС) различных типов.

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

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

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

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

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

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

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

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

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

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) нелые числа относительно вычитания?
5) рациональные числа относительно умножения?
6) рациональные числа, отличные от нуля, относительно умножения?
7) положительные рациональные числа относительно умножения?
8) положительные рациональные числа относительно деления?
9) корни n-й степени из единицы (как действительные, так и комплексные) относительно умножения?
10) матрицы порядка n с действительными элементами относительно умножения?
11) невырожденные матрицы порядка n с действительными элементами относительно умножения?

12) перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок?

13) преобразования множества M, то есть взаимно-однозначные отображения этого множества на себя, относительно композиции отображений?

14) элементы n-мерного векторного пространства $\mathbb{R}^n$ относительно сложения?

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

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

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

1.3. Вычислите функцию Эйлера для:

$$\text{а) } 375; \quad \text{б) } 720; \quad \text{в) } 988.$$

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

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

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

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

1) квадратные матрицы данного порядка с *действительными* элементами относительно сложения и умножения матриц?
2) многочлены одного неизвестного с целыми коэффициентами относительно обычных операций сложения и умножения?
3) многочлены одного неизвестного с действительными коэффициентами относительно обычных операций?

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

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

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

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

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

Глава 2

Конечные кольца и поля

2.1 Поля Галуа

Простые поля Галуа — поля классов вычетов. Нам известно, что если p — простое число, то

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

— 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.

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

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

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

×	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

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

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

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

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

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

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

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

Если все суммы вида $1 + \ldots + 1$ различны, то полагают $\operatorname{char} K = 0$ (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” P/Q, где P и Q ($Q \neq 0$) — многочлены от формальной переменной x с коэффициентами из K. На множестве данных “дробей” вводятся отношение эквивалентности, операции сложения, умножения и деления, аналогично как это делается для рациональных чисел в форме простых дробей.

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

Будем рассматривать далее исключительно конечные поля.

В конечном поле возможно сильное упрощение вычисления степеней сумм.

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

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

Доказательство. В любом коммутативном кольце верна формула степени бинома

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

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

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. 15 обозначением, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ — мультипликативная группа q-элементного поля Галуа $\mathbb{F}_q$.

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

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

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

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

то все её элементы удовлетворяют уравнению

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

— *неизвестно*, то эффективных алгоритмов не найдено; используют заранее составленные таблицы, вероятностные алгоритмы...

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

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

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 с коэффициентами из некоторого поля K образует коммутативное евклидово кольцо, обозначаемое $K[x]$ и называемое *кольцом многочленов над* K.

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

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

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

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

Из разложения для многочленов

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

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

Неприводимые многочлены

Определение 2.3. Многочлен над 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

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

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

Вторая степень: $x^2 + ax + b$.

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

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

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

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

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

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

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

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

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$. Исключение делимости на $x+1$ приводит к условию

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

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

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

Пятая степень: $x^5 + ax^4 + bx^3 + cx^2 + dx + 1$. Исключение делимости на $x+1$ приводит к условию

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

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

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

Теорема 2.4 (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. 61).

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

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

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

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

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

Может возникнуть вопрос: *почему в обозначении*

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

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

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

Пример 2.5. Построим поле $\mathbb{F}_3^2$. Для этого выберем в $\mathbb{F}_3[x]$ неприводимый многочлен: пусть это будет x^2+1. Тогда искомое поле 9-элементное поле есть

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

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

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

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

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

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

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

2.2 Вычисления в конечных кольцах и полях

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

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

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

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

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

(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 $(252, 105) = 21$.

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

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

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

$$d = ax + by.$$

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

Замечание. Коэффициенты Безу могут быть выбраны неоднозначно, например

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

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

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

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

---

[5] Для взаимно простых чисел открыто Клодом Гаспаром Баше (Bachet de Mezeriac Gaspar Klod, 1581–1638) и опубликовано в 1624 г., за 106 лет до рождения Этьена Безу (Etienne Bezout, 1730–1783), который обобщил данное соотношение на кольцо многочленов (см. с. 45). Онлайн-калькулятор коэффициентов соотношения Безу доступен по адресу *http://wims.unice.fr/wims/wims.cgi.*

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

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

2. Иначе заменим матрицу E матрицей

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

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

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

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

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

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

2. Заменяем матрицу E матрицей

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

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

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

5. Заменяем матрицу E матрицей

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

6. Заменям пару чисел $(252, 105)$ парой $(42, 21)$ и перейдём к шагу 1.
7. Вычисляем $r = 42 - 21 \cdot 2 = 0$. Значения $x = -2$ и $y = 5$ найдены, как и $d = 21$.

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

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

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

1. Запишем исходные данные в виде двухстрочной таблицы

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

2. Вычислим частное q от деления друг на друга элементов первого столбца, то есть m на c: $m = q \cdot c + r$, $0 \leqslant r < c$.
3. Вычтем из 1-й строки 2-ю, домноженную на q и запишем результат в качестве 3-й строки таблицы.
4. Проводим аналогичные действия с двумя последними строками таблицы, пока в очередной строке не получим первый элемент 0. Тогда второй элемент *предпоследнй* строки есть c^{-1}.

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

$$4y = 1.$$

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

$$\begin{array}{c|cc|l}
1 & 101 & 0 & \\
2 & 4 & 1 & q = 25 \quad (\ 100\ 25\ ) \\
\hline
3 & 1 & \mathbf{-25} & q = 4 \\
4 & 0 & &
\end{array}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

вычисляем

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

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

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

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

вычисляем

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

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

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

Пример 2.11. Найдём $\left(x^2+x+3\right)^{-1}$ в поле

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

Для этого обобщённым алгоритмом Евклида решим соотношение Безу

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

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

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

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

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

2.3 Поля Галуа как векторные пространства

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

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

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

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

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

Базисом этого пространства являются векторы

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

или же, переходя к многочленам —

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

Легко установить, что для каждых простого p и натурального n существует ровно с точностью до изоморфизма поле Галуа. Действительно, свяжем нули двух полей из p^n отображением изоморфизма, тогда их мультипликативные группы также изоморфны как конечные циклические группы одинакового порядка.

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

степень α $\quad\alpha^4 = \alpha + 1$	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:

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

Теорема 2.12. *Поле $\mathbb{F}_p^m$ есть подполе $\mathbb{F}_p^n$, если и только если $m \mid n$.*

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

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

2.4 Корни многочленов над конечным полем

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

Определение 2.13. *Минимальным многочленом (м. м.)* элемента $\beta \in \mathbb{F}_p^n$ называется нормированный многочлен $m_\beta(x) \in \mathbb{F}_p[x]$ наименьшей степени, для которого β является корнем.

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

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

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

$$b(x) = b_0 + b_1x + \ldots + b_{n-1}x^m = 0,$$

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

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

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

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

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

Поэтому β — корень многочлена

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

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

Теорема 2.15. *Минимальные многочлены неразложимы.*

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

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

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

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

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

Теорема 2.16. *Пусть $m_\beta(x)$ — м. м. для элемента β в некоторого поля Галуа, а $f(x)$ — многочлен имеющий β своим корнем. Тогда $m_\beta(x) \mid f(x)$.*

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

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

Подставляя в это равенство β вместо x, получаем

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

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

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

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

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

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

Пример 2.18. 1. Многочлен

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

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

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

и $\operatorname{ord} x = 5$.

2. Для своего корня x многочлен

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

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

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

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

Теорема 2.19. *Любой элемент поля $GF(q)$ удовлетворяет равенству $x^q - x = 0$.*

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

Поскольку $q = p^n$, получим следующие

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Пример 2.23. Возвращаемся к разложению бинома $x^{15} + 1 \in \mathbb{F}_2[x]$.

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

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

Таким образом,

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

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

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

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

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

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

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

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

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

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

Возводим обе части этого равенства в степень p^n. Из тождества Фробениуса (см. теорему 2.1 на с. 31) и $\alpha^{p^n} = \alpha$ для любого $\alpha \in F$ получим

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

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

Корни неприводимого многочлена

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

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

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

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

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

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

Будем пользоваться далее свойствами сравнения (см. с. 25).

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

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

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

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

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

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

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

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 2.25.

Пример 2.26. 1. Найдём корни неприводимого над $\mathbb{F}_2$ многочлена

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

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

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

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

2. Найдём все корни многочлена

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

в минимальном расширении поля $\mathbb{F}_3$.

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

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

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

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

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

В этом поле $x^2 = -2x - 2 = x + 1$ и

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

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

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

1) $\beta^{p^d} = \beta$, тогда
$$m_\beta(x) = (x-\beta)\cdot(x-\beta^p)\cdot\ldots\cdot\bigl(x-\beta^{p^{d-1}}\bigr).$$

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

Пример 2.27. Найдём минимальные многочлены для элементов
$$\beta_1 = x^2 + x \quad \text{и} \quad \beta_1 = x + 1$$
поля $\mathbb{F}_2[x]/\bigl(x^4+x+1\bigr)$.

В этом поле $x^4 = x + 1$.

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

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

Таким образом $m_\beta(x)$ — квадратный многочлен и
$$m_\beta(x) = (x-\beta)(x-\beta^2) = x^2 + (\beta^2+\beta)\,x + \beta^3.$$

Вычисляем коэффициенты многочлена:
$$\beta^2 + \beta = \bigl(x^2+x+1\bigr) + \bigl(x^2+x\bigr) = 1,$$
$$\beta^3 = \bigl(x^2+x+1\bigr)\bigl(x^2+x\bigr) = \ldots = (x+1) + x = 1,$$

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

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

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

поэтому $m_\beta(x) = x^4 + x + 1$.

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

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

Найдём, например, I_2^7. По формуле Гаусса

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

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

Из формулы Гаусса имеются важные

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

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

---

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

Приведём прямую формулу для определения I_p^n.

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

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

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

Теорема 2.29 (формула Гаусса).

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

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

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

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

2.5 Циклические подпространства колец вычетов

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

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

Теорема 2.30. *Пусть $f, \varphi \in \mathbb{F}_p[x]$, $\varphi \mid f$, а φ — неприводимый нормированный многочлен. Тогда*

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

Доказательство. Имеем

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

1. То, что (φ) есть идеал следует из определения главного идеала кольца (см. с.17).

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

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

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

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

В кольце $R = \mathbb{F}_2[x]/\big(x^4 - 1\big)$ 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	$x^3 + 1$

Циклическое пространство

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

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

Циклический сдвиг координат в этом базисе равносилен умножению на x:

$$\big(a_0 + a_1 x + \ldots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1}\big) \cdot x \;=$$

$$= a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{=1} =$$

$$= a_{n-1} + a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1}.$$

Теорема 2.33. *В кольце классов вычетов по модулю многочлена $x^n - 1$ подпространство является циклическим если и только если оно идеал.*

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

Обратно, пусть I — циклическое подпространство кольца $\mathbb{F}_p/(x^n - 1)$ и $g \in I$. Тогда циклические сдвиги

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

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

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

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

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

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

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

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

Пример 2.34. 1. Вернёмся к примеру с разложением бинома $x^{15}+1 \in \mathbb{F}_2[x]$. Относительно умножения на 2 вычеты по модулю $n = 15$ разбиваются на следующие орбиты:

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

Поэтому $x^{15} + 1$ разлагается в произведение одного неприводимого многочлена степени 1, одного неприводимого многочлена степени 2 и трех неприводимых многочленов степени 4. Конкретно разложение было найдено ранее (см. с. 56).

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

$$\{0\}, \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\},$$
$$\{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

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

Можно показать, что поле разложения бинома $x^n - 1 \in \mathbb{F}_p[x]$ при n некратном p есть $\mathbb{F}_p^m$, где m — максимальная степень неприводимого многочлена, его делящего: $m = \max\{d_1, \ldots, d_k\}$[7]. Это следует из того, что значение n как порядок группы корней из 1, должно делить порядок мультипликативной группы поля разложения.

2.6 Задачи

2.1. С помощью алгоритма Евклида вычислите НОД (a, b)

a) $a = 589$, $b = 43$; *b*) $a = 6188$, $b = 4709$;
c) $a = 12606$, $b = 6494$; *d*) $a = 20989$, $b = 2573$.

2.2. Найти

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

2.3. Решите сравнение

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

а) $7x = 11 \pmod{25}$;

б) $9x = 3 \pmod{10}$;

в) $6x + 2 = 3 \pmod{7}$;

г) $6x + 2 = 3 \pmod{9}$;

д) $6x + 2 = 4 \pmod{9}$;

е) $6x + 1 = 4 \pmod{9}$.

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

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

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

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

2.6 (Теорема Вильсона). Доказать, что

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

2.7. Построить поле из 4-х элементов.

2.8. В кольце $\mathbb{Z}_2[x]$ найти

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

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

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

1) построить таблицу соответствий между полиномиальным и степенным представлением его ненулевых элементов;
2) построить таблицу умножения элементов;

3) для каждого элемента поля указать обратные;
4) найти порождающие элементы поля;
5) найти минимальные многочлены всех элементов поля.

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

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

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

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

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

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

2.15. Многочлен

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

разложить на неприводимые множители.

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

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

2.18. Определить, является ли:

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

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

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

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

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

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

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

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

2.22. Найти количество нормированных неприводимых многочленов

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

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

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

С её помощью вычислить выражение

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

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

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

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

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

2.27. Разложить на неприводимые множители многочлен

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

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

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

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

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

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

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

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

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

Подход к решению (один из возможных!):

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

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

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

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

- $S = \{0, 1\}^k$ — пространство всех возможных *сообщений* длины k каждое.
- *Кодом* будем называть совокупность C всех кодовых слов, $|C| = Q = 2^k$ — *мощность кода*;
- Для обеспечения помехозащищённости вместо сообщений передают *кодовые слова* бо́льшей длины $n = k + m$, $m > 0$, и поэтому рассматриваемое кодирование называют *избыточным.*

  Если $m = 0$ или $k = 0$ говорят о *тривиальных кодах.*
- *Кодированием* будем называть взаимно-однозначное преобразование сообщения в кодовое слово[1)].

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

[1)] часто именно это отображение и называют кодом

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

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

Кодовое расстояние

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

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

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

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

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

[2)] часто — *минимальным кодовым расстоянием* что практически невозможно уже начиная с $k = 50$. Поэтому важной задачей является построение кодов с кодовым расстоянием не менее заданного.

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

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

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

- сообщение — вектор

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

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

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

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

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

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

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

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

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

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

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

<u>*1-й этап:*</u> 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).
Если произошло не более $r = \lfloor\, (d-1)/2 \,\rfloor$ ошибок, то $\widehat{\boldsymbol{v}} = \boldsymbol{v}$.

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

Ясно, что 1-й этап может быть выполнен перебором 2^n строк в $(2^n \times k)$-таблице кодовых слов. Это говорит о том, что декодирование блокового (n, k)-кода *общего вида* является крайне ресурсоёмким процессом, и использование таких кодов возможно лишь при небольших значениях n и k.

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

Плотная упаковка шаров в единичный куб

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

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

— граница Хэмминга (англ. volume bound).

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

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

— граница Гильберта.

Доказательство известно читателю из курса Дискретной математики. □

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

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

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

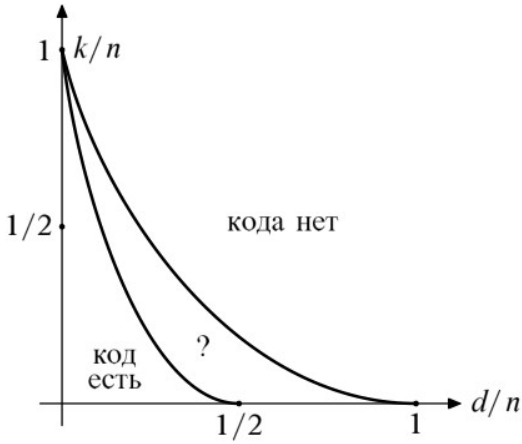

Рис. 3.1. Границы Гильберта (левая) и Хэмминга (правая) для $n \gg 1$.

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

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

Оказывается, такое удаётся только в двух нетривиальных случаях, когда получаются *совершенные* или *экстремальные коды*:

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

2) $n = 23$, $r = 3$ — *код Голея* (см. с. 91);
   у него $k = 12$ и $m = 11$.

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

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

Образуем сначала единичную матрицу порядка

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

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

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

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

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

Найдём кодовое расстояние построенного кода C. 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. Отсюда следует, что расстояние между кодовыми словами всегда не менее $3 = d(C)$.

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

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

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

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

3.2 Линейные коды

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

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

Линейный код обладает следующими свойствами.

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

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

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

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

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

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

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

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

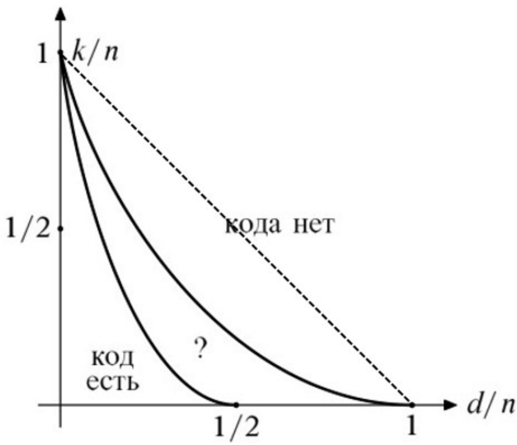

Рис. 3.2. Границы Гильберта, Хэмминга и Синглтона (пунктир) для $n \gg 1$.

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

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

Порождающая матрица. Составим из векторов некоторого базиса кода матрицу

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

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

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

Пример 3.9. Линейный код из примера 3.2 порождается матрицей

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

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

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

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

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

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

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

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

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

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

Подчеркнём ещё раз, что для того, чтобы узнать кодовое расстояние линейного кода, в обществе необходимо перебрать все его элементы. Для этого можно умножить порождающую матрицу на всевозможные ненулевые векторы сообщений

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

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

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

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

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

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

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

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

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

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

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

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

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

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

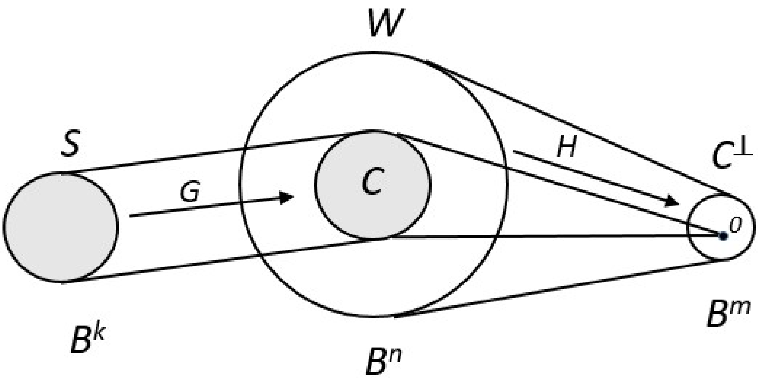

Рис. 3.3. Преобразования: G — сообщений в линейный код C и H — принятых слов в $C^{\perp}$.

ведливо

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

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

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

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

то матрица $H = \left[\ P_{m\times k}\ I_m\ \right]$ будет проверочной.

Действительно, в этом случае

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

— нулевая $m \times k$ матрица.

Пример 3.12. Для построенной в примере 3.11 порождающей матрицы $G_{7\times4}$ проверочной будет

$$H_{3\times7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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

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

$$G = \begin{bmatrix} P \\ I \end{bmatrix}, \quad H = \left[\ I\ P\ \right].$$

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

$H_{m\times n}$. Эти матрицы определены с точностью до элементарных преобразований столбцов и строк соответственно, что отвечает выбору различных базисов в пространствах C и $C^{\perp}$. Однако фиксирование позиций информационных бит задаёт G и H однозначно.

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

Пример 3.13. Пусть линейный $(6,3)$-код C задан порождающей матрицей

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

Требуется:

1. Кодом C осуществить несистематическое и систематическое кодирование векторов

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

2. Построить проверочную матрицу H' для систематического кодирования.

3. Определить кодовое расстояние d кода C.

Решение. 1. *Несистематическое кодирование* находим непосредственно:

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

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

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

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

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

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

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

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

Далее нужно

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

В итоге получим проверочную матрицу

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

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

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

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

Получаем $d = 3$.

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

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

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

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

---

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

3.3 Синдромное декодирование линейных кодов

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

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

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

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

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

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

Если же ошибки произошли, то

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

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

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

а кодовые слова являются решениями соответствующей однородной системы

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

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

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

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

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

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

Например, в *Примере* 3.11 получена матрица

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

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

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

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

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

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

Тогда порождающая матрица есть

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

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

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

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

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

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

Тогда синдром

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

указывает позицию ошибки.

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 NP-сложная задача.

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

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

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

3.4 Циклические коды

Определение и построение циклических кодов

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

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

Имеется биективное соответствие векторов и полиномов, введённое на с. 47:

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

Последнее соотношение описывает элементы образованного циклического пространства.

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

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

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

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

Порождающий многочлен полностью определяет циклический код.

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

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

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

При удачном выборе порождающего полинома получается код с приемлемым кодовым расстоянием d, однако определение d остаётся чрезвычайно трудоёмкой задачей.

Пример 3.17. Построим циклический код длины 23. В п. 2 примера 2.34 найдены число и степени неприводимых многочленов, факторизующих бином $x^{23} - 1$. Конкретно это разложение таково:

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

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

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

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

уже порождает циклический код.

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

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий:

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

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 разряды n-битного слова. Поделим теперь $x^m u(x)$ на $g(x)$ с остатком:

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

откуда

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

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

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени его неприводимых делителей, для чего применим способ разбиения $\mathbb{Z}_7$ на орбиты относительно умножения на 2 (см. с. 65):

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

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

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

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

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

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

Определяя конкретный код, выберем

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

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

2. Закодируем несистематическим и систематическим кодированием сообщение

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

Несистематическое кодирование.

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

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

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

то есть $r(x) = x$ и поэтому

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

Декодирование циклических кодов

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

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

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

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

3.5 Коды БЧХ. Кодирование

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

Циклотомические классы

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

Все сопряжённые элементы составляют *циклотомический класс*.

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

Ясно, что циклотомические классы

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

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

Поскольку в поле характеристики p значения любого полинома в точках α и α^p одинаковы, то циклотомические классы можно получать возведением в степень p какого-то одного его элемента. Это совпадает с построением орбиты отображения (см. с. 66)

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

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

Заметим, что если α — *примитивный элемент* поля $\mathbb{F}_2^t$, то его циклотомический класс *содержит ровно* t *элементов*: поскольку $\alpha^{2^t-1} = 1$, то $\alpha^{2^t} = \alpha$ и данный класс есть

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

Пример 3.21. Пусть $t = 4$ и α — примитивный элемент поля $F = \mathbb{F}_2^4$. Тогда мультипликативная группа

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

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

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

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

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

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

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

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

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

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

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

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

Алгоритм построения двоичного кода БЧХ, исправляющего не менее r ошибок

1. Выбрать величину t, определяющую длину кода $n = 2^t - 1 > 2r + 1$.
2. Выбрать неприводимый полином $a(x)$ степени t, определив 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 $2r$ нулей кода α, α^2, …, α^{2r}; 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 3.23. Выберем $t = 3$ и построим различные БЧХ-коды длины $n = 2^3 - 1 = 7$.

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

Поскольку многочлен $a(x)$ — примитивный, и, как показано в п. 1 примера 3.18 на с. 99, F^* разбивается на следующие циклотомические классы ($\alpha = x$):

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

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

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 $g(x) = a(x)$, $m = 3$ и в результате получаем уже известный $(7, 4, 3)$-код Хэмминга (см. пример 3.18).

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

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

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

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

Найдем м. м. для класса C_2:

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

Вычислим коэффициенты $g_2(x)$:

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

Таким образом $g_2(x) = x^3+x^2+1$[7] 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 тривиальный код с 7-кратным повторением, исправляющий 3 ошибки, и его скорость $R = 1/7$.

Пример 3.24. Попытаемся построить лучшие коды, взяв бóльшие их длины: выберем $t = 4$ и тогда длина кода $n = 2^4 - 1 = 15$.

Рассмотрим поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^4$, образованное некоторым неприводимым многочленом $a(x)$ степени $t = 4$. Тогда F^* относительно своего примитивного элемента α, как показано в п. 2 примера 3.21, разобьётся на 5 циклотомических классов над $\mathbb{F}_2$:

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

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

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

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

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

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

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

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

Тогда порождающий полином кода есть

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

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

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

Минимальные многочлены для C_1 и C_2 уже найдены. Далее, очевидно $g_3(x) = x^2 + x + 1$, поскольку это единственный неприводимый квадратный многочлен над $\mathbb{F}_2$. Тогда порождающий полином есть

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

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

3.6 Декодирование кодов БЧХ

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

В этом случае $d = 3$, и нулями кода являются α и α^2, где α — примитивный элемент поля $\mathbb{F}_2^n$ и $n = 2^t - 1$.

Для декодирования принятого слова $w(x)$ вычисляем синдром $s_1 = w(\alpha) = s$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется).

При $s = 0$ считаем, что ошибок не произошло. Если $s \neq 0$, то определяем значение j, для которого $\alpha^j = s$ и считаем, что произошла единичная ошибка в j-м разряде для $j = 0, 1, \ldots, n-1$.

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

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

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

$$[\,0\;1\;0\;0\;0\;\overset{\frown}{0}\;1\,]^T \leftrightarrow w(x) = x^6 + x.$$

Для декодирования $w(x)$ найдем синдром:

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

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

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

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, $j_1, \ldots, j_\nu$.

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

Перепишем полученную систему как зависимости с введёнными переменными:

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

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:

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

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

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

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

1. Найти все синдромы $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$; если все они равны 0, то считаем, что ошибок нет, $v(x) = w(x)$ и переходим к пункту 6.
2. Используя тот или иной декодер, найти полином локаторов ошибок $\sigma(x)$; число ν произошедших ошибок равно его степени.
3. Найти все корни $\sigma(x)$, например, перебором элементов F^*; пусть эти корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
4. Найти позиции ошибок $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
5. Найти полином ошибок $e(x) = x^{j_1} + \ldots + x^{j_\nu}$ и восстановить кодовое слово $v(x) = w(x) + e(x)$.
6. По $v(x)$ восстановить переданное сообщение $u(x)$.

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

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

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

Перемножив введённые полиномы, получим *полином значений ошибок*:

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

Его коэффициенты определяются соотношением для произведения многочленов —

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

Замечаем, что значения λ_i по данной формуле для $i = \nu + 1$, ..., $2r$ 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 по $\bmod\ x^{2r+1}$ (см. с. 45) с условием останова «*степень очередного остатка не более* r» и опусканием заключительного шага нормировки.

Пример 3.26. Рассматриваем БЧХ $(15, 5, 7)$-код с полем разложения $\mathbb{F}_2[x]/\big(x^4 + x + 1\big) = F$, построенный в п. 2 примера 3.24. При вычислениях будем пользоваться таблицей со с. 48.

Пусть передаётся сообщение

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

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

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

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

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

1. Найдём все $2r = 6$ синдромов:

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

Таким образом, синдромный полином есть

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

2. Применяя декодер на базе обобщённого алгоритма Евклида решаем относительно $\sigma(x)$ соотношение 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. $r_{-2}(x) = r_{-1}(x) q_0(x) + r_0(x),$
$q_0(x) = \alpha^{14} x + \alpha^{13},$
$r_0(x) = \alpha^8 x^5 + \alpha^{12} x^4 + \alpha^{11} x^3 + \alpha^{13},$
$\deg r_0(x) = 5 > 3 = r,$
$\sigma_0(x) = q_0(x).$

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

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

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

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

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

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

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

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

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

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

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

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

Замечания по практическому применению избыточного кодирования

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

3.7 Задачи

3.1. Построить порождающую G и проверочную H матрицы для

1) тривиального кода утраивания;
2) кода проверки на чётность.

3.2. Для кода Хемминга, заданного своей проверочной матрицей

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

требуется

1) построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;
2) найти такое кодирование для сообщений

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

3.3. Циклический $(9, 3)$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние d, а также осуществить систематическое кодирование полинома

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

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

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,
3) $w_3(x) = x^6 + x^3 + x^2 + x$.

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

3.6. Пусть α — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$. Для кода БЧХ с нулями α, α^2, α^3 и α^4 и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

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

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок есть

$$\sigma(x) \ = \ \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить *позиции ошибок* в $w(x)$.

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

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

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить позиции ошибок в данном слове.

Глава 4

Алгебраические основы криптографии

4.1 Основные понятия

Термины. *Криптография*[1] — 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.

Например, тексты на английском языке обычно представляют, используя *стандартную кодировку*

$$a = 01,\ b = 02,\ \ldots,\ z = 26,\ \text{пробел } = 00.$$

[1] от др.-греч. *тайнопись*

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. Алгоритм шифрования тщательно разрабатывается и меняется в редких случаях.

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 к данному тексту.

Расшифрование (decryption) — процесс, обратный к зашифрованию, реализуемый при известном значении ключа.

Дешифрование — процесс раскрытия криптограммы без знания секретного ключа.

Определения шифра и его ключа соответствуют принятому в современной криптографии правилу стойкости Керкгоффса[2)], согласно которому *в секрете*

[2)] 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.

держится только ключ, а сам алгоритм шифрования открыт.

Таким образом, *надёжность зашифрования определяется не секретностью шифра, а исключительно значением его секретного ключа*, известному только легальным пользователям. По необходимости ключ легко меняется: защищённость системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить.

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.

Типы шифрсистем. Сложность алгоритмов. Зашифрование открытого текста и его расшифровывание проводят с использованием, как правило, различных ключей, которые мы будем обозначать k_e и k_d соответственно. Множество возможных значений k_e и k_d 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 шифрсистема *гаммирования* (или *шифр Вернама*), когда криптограмму $\widetilde{\beta}$ получают из открытого текста $\widetilde{\alpha}$ путём сложения его по $\bmod 2$ с некоторым случайным двоичным 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*[3)], если ключ не содержит длинных повторяющихся битовых последовательностей и используется однократно.

Утверждённая в России с 1.06.2019 в качестве стандарта шифрсистема «Кузнечик» реализует симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит.

Объявленная в США с 26.05.2002 стандартом шифрсистема AES (Advanced Encryption Standard) реализует симметричный алгоритм блочного шифрования с размером блока 128 бит

[3)] Под «абсолютной» понимается стойкость к дешифрованию, обеспеченная фундаментальными законами природы, а не текущими 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 требуемого качества, решения проблем их хранения, передачи и уничтожения. На каждом из этих этапов жизненного цикла ключей имеется угроза их раскрытия. Все это делает данные системы непрактичными, дорогостоящими, и они применяется в исключительных случаях.

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. Шифрсистема 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 входного слова ℓ 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. *Экспоненциальным* называют алгоритм, имеющий оценку времени исполнения вида $exp(\ell)$.

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 — позволяет эффективно использовать в криптографии арифметику вычетов.

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

$$a^{53} = a^{2^5} \cdot a^{2^4} \cdot a^{2^2} \cdot a^{2^0}.$$

Вычисление первого сомножителя требует пяти умножений: $a^{2^5} = ((((a^2)^2)^2)^2)^2$. В процессе его вычисления запоминаются значения 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 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: $11 = 2^0 + 2^1 + 2^3 \leftrightarrow [\ 1\ 1\ 0\ 1\ ]$. Поэтому $3^{11} \equiv_5 a_0^1 \cdot a_1^1 \cdot a_2^0 \cdot a_3^1$.

2. Находим a_i, $i = 0, 1, 2, 3$:

$$a_0 = 3 \equiv_5 3, \qquad a_1 = 3^2 = 9 \equiv_5 4,$$
$$a_2 = 4^2 = 16 \equiv_5 1, \qquad a_3 = 1^2 \equiv_5 1.$$

3. Окончательно $3^{11} \equiv_5 3 \cdot 4 = 12 \equiv_5 2$.

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 2.19 (см. с. 54). 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

$$(a+1)^{p-1} = (a+1)^p(a+1)^{-1} \equiv_p (a^p+1)(a+1)^{-1} = \\ = (a+1)(a+1)^{-1} \equiv_p 1.$$

$\square$

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»)[4].

Например, в векторе

$$\boldsymbol{a} = [\ 43\ \underline{129}\ 215\ \underline{473}\ \underline{903}\ 302\ \underline{561}\ \underline{1165}\ 697\ 1523\ ],$$

подчёркнуты элементы, дающие в сумме $z = 3231$, то есть решением задачи для данного z будет вектор-столбец $\boldsymbol{x} = [\ 0\,1\,0\,1\,1\,0\,1\,1\,0\,0\ ]^T$ позиций выбранных чисел: $\boldsymbol{a} \times \boldsymbol{x} = z$. Неизвестны полиномиальные алгоритмы решения задачи о рюкзаке.

Односторонняя функция — центральное понятие криптографии.

Определение 4.4. *Односторонней* (или *однонаправленной*, one-way function) называется обратимая функция $f : X \to Y$, обладающая свойствами:

1) существует полиномиальный алгоритм вычисления значений $f(x)$;
2) не существует полиномиального алгоритма обращения функции f (то есть нахождения x по значению $y = f(x)$).

Неформально: имеющая обратную функция $f(x)$ называется однонаправленной, если для всех $x \in X$ достаточно легко вычислить $y = f(x)$, но почти для всех $y \in Y$, нахождение любого $x \in X$, для которого $y = f(x)$, *вычислительно не осуществимо.*

---

[4] Предполагается, что решение существует и единственно; другое название задачи — *проблема подмножества суммы*

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 FACT).
- Для известных a, b, n найти такое значение x, что $a^x = b \pmod{n}$ (задача DLOG нахождения *дискретного логарифма*).
- Решить задачу о рюкзаке для общего случая.
- Декодировать исправляющий ошибки линейный код общего вида.

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) почти для всех k и $y \in Y$, нахождение $f_k^{-1}(y)$ вычислительно неосуществимо без знания k.

Один из примеров, претендующих на то, чтобы являться односторонней функцией с лазейкой — функция $f(x) = x^m \pmod{n}$, m и n известны. Действительно, вычисление $f(x) = y$ производится методом быстрого возведения в степень, а эффективный алгоритм обратного преобразования $f^{-1}(y)$, то есть *вычисления корня m-й степени по* $\mathrm{mod}\ n$, требует знания примарного разложения n. Эта информация может считаться лазейкой.

Применение односторонних функций с секретом позволяет, например, организовать обмен шифрованными сообщениями по открытым каналов связи, снабдить документ электронной подписью и др.

4.2 Криптографические протоколы

Криптографический протокол (cryptographic protocol) — набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Электронная цифровая подпись (ЭЦП) — позволяет проверить авторство документа и отсутствие в нём искажений.

Для этого

1. Автор документа a вычисляет значение y его хэш-функции преобразования a в битовую строку установленной длины[5].

[5] Понятно, что хэш-функции осуществляют необратитмые преобразо-

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.

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 представляемых возможностях.

Выработка общего секретного ключа по открытому каналу связи — покажем, как это можно сделать на примере протокола DH Диффи–Хеллмана[6].

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.

вание информации. *Хэш* (или *дайджест*) y выступает как компактный представитель (паспорт) документа a. К хэш-функциям предъявляются специфические требования, которые мы не будем здесь обсуждать.

[6] Предложен в 1976 г. сотрудниками MTI У. Диффи (Bailey Whitfield 'Whit' Diffie, 1944) и М. Хеллманом (Martin Edward Hellman, 1945) и независимо от них Р. Мерклем (Ralph Charles Merkle, 1952).

Этот протокол положил начало криптографии открытого ключа.

Для этого они выбирают простое число p и в поле Галуа $GF(p)$ — некоторый примитивный элемент α; эти значения не являются секретом. Затем A и B независимо друг от друга выбирают по одному случайному натуральному числу x и y соответственно, которые держат в секрете. Далее каждый из них вычисляет новый элемент поля $GF(p)$:

$$X = \alpha^x, \quad Y = \alpha^y, \qquad (\mathrm{mod}\ p), \qquad (*)$$

которыми обмениваются по открытому каналу.

Абонент A, получив Y, вычисляет ключ:

$$K = Y^x \qquad (\mathrm{mod}\ p),$$

и аналогично поступает абонент B:

$$K = X^y \qquad (\mathrm{mod}\ p).$$

Тем самым у Алисы и Боба появился общий секретный ключ $K = \alpha^{xy} \in GF(p)$, 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 DLOG.

Заметим, что задача DLOG принадлежит классу NP, но её NP-полнота не доказана.

Протокол DH устойчив к пассивной атаке, но при 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[7].

Таким образом, протокол DH позволяет передавать секретный ключ по *частично защищенному каналу связи*, защищённому подмены и незащищеному от прослушивания.

Обмен шифртекстами по открытому каналу связи. Приведём пример использования односторонней функции с лазейкой при решении задачи о рюкзаке[8], 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,

---

[7] Вспоминаем *Сказку о царе Салтане А. С. Пушкина*: «... И в суму его пустую // Суют грамоту другую...»

[8] На ней основаны системы шифрования Меркля–Хеллмана и Шора–Ривеста.

$$\boldsymbol{a} = [\ \underline{25}\ 27\ \underline{56}\ 112\ 231\ \underline{452}\ \underline{916}\ 1803\ ] \ \text{ и } \ z = 1449.$$

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 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 4.5. 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 вектором будет

$$\boldsymbol{b} = [\ 3\ 6\ 12\ 24\ 11\ ].$$

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 $u = 25$;
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 — классическая асимметрическая криптосистема. В ней открытым ключом шифрования является пара (n, e) значений *модуля* n и *экспоненты* e. По данному шифртексту $y = x^e \pmod{n}$ требуется найти открытый тест x. Таким образом, функция шифрования f, использующаяся в RSA, есть

$$f_e : x \to x^e \pmod{n}. \tag{4.2}$$

Для расшифрования сообщения y нужно решить сравнение $x^e \equiv_n y$.

Искомое решение может быть представлено в виде

$$x = y^d \qquad (\text{mod } n), \tag{4.3}$$

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 $f_e(x)$ легко вычисляется с помощью алгоритма быстрого возведения в степень, также как и при известном d — обратная к ней функция $f_d(y)$.

Покажем, как можно было бы найти секретный ключ расшифрования d. Ясно, что он должен удовлетворять условию

$$x^{e \cdot d} \equiv_n x.$$

По теореме 4.3 Эйлера имеем

$$x^{\varphi(n)} \equiv_n 1, \text{ откуда } x^{k \cdot \varphi(n)} \equiv_n 1$$

для любого целого k. Отсюда

$$x^{1+k\cdot\varphi(n)} = x = x^{e \cdot d} \pmod{n},$$

и заключаем, что для ключа d должно выполняться условие

$$d \cdot e = 1 \pmod{\varphi(n)}. \tag{4.4}$$

Решить это сравнение можно было бы, например, с помощью алгоритма 2.2 со с. 43. 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 DLOG, 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 Р. Риве́ста, А. Шамира и Л. Адлемана (Ronald Linn Rivest, 1947; Adi Shamir, 1952; Leonard Adleman, 1945) из MTI[9)].

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

$$\varphi(n) = \varphi(pq) = (p-1)(q-1), \tag{4.5}$$

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 4.6. *Пусть $n = pq$, где p, q — простые числа. Тогда знание p, q равносильно знанию $\varphi(n)$.*

Доказательство. Зная p и q, легко находят
$\varphi(n) = (p-1)(q-1)$.

[9)] Однако согласно рассекреченным британским правительством в 1997 г. сведениям, идея основных принципов криптографии с открытым 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).

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, организация шифрованной переписки с помощью схемы RSA происходит следующим образом.

1. Организатор системы выбирает два достаточно больших простых числа p и q и находит произведение $pq = n$.
2. Затем он выбирает экспоненту $e < n$, достаточно большую, 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, а организатор легко сможет расшифровывать 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 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 $2^{2^k}+1$), представление которых содержит лишь две единицы: $3, 5, 17, 257, 65537$;
- нахождение ключа расшифрования d без знания $\varphi(n)$ (факторизация большого значения n) вычислительно неосуществимо;
- алгоритм (расшифрования) RSA намного медленнее симметрических криптоалгоритмов (например, AES — стандарт США).

Пример 4.7. Пусть $p = 11$, $q = 13$, тогда $n = pq = 143$.

Выберем значение $e = 13$, оно простое, и, очевидно, заведомо взаимно просто с

$$p - 1 = 10 \ \text{ и } \ q - 1 = 12.$$

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:

$$
\begin{array}{c|cc|ll}
1 & 120 & 0 & & \\
2 & 13 & 1 & q=9 & (\ 117\ 9\ ) \\
\hline
3 & 3 & -9 & q=4 & (\ 12\ \ -36\ ) \\
4 & 1 & \mathbf{37} & q=3 & \\
5 & 0 & & &
\end{array}
$$

и получим $d = 37$.

Получив криптограмму y, легальный получатель расшифровывает её:

$$3^{37} \;=\; 450\,283\,905\,890\,997\,363 \;\equiv_{143}\; 42 \;=\; x.$$

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 (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*»[10].

[10] «*Волшебные слова — привередливая скопа*» (скопа — крупная хищная птица) — 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.

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 простоты числа N.

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, т. е. они не будут выявлены данной проверкой. Эти числа называют *псевдопростыми* или *числами Кармайкла*[11)].

Отметим, что

- для составления *таблиц простых чисел* наилучшим является известный метод решета Эратосфена, несмотря на то, что он требует большого объёма памяти;
- на сегодняшний день разработаны быстрые и эффективные детерминированные алгоритмы определения простоты числа, основанные на эллиптических кривых.

Генерация ключей. Линейный конгруэнтный метод. Один из способов получения ключа шифрования — использовать генератор псевдослучайных чисел. Хорошие по статистическим свойствам последовательности псевдослучайных чисел получаются по формуле *линейного конгруэнтного метода*:

$$r_{i+1} \equiv_m a \cdot r_i + b, \quad i = 1, \ldots, N,$$

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 длина может

[11)] Роберт Дэниэл Кармайкл (R. D. Carmichael, 1879–1967) — американский математик, $561 = 3 \cdot 11 \cdot 17$ — пример числа Кармайкла.

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, что псевдослучайные последовательности в качестве ключей *использовать нельзя*.

Сегодня специалисты сходятся во мнении, что источником истинно случайной последовательности может быть только какой-нибудь физический процесс: радиоактивный распад, тепловое движение атомов или молекул и т. п. 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 пользователя 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:

1) выберем *четное* число $R \xleftarrow{\$} [\ S, 4S + 2\ ]$ и положим $N = SR + 1$;

2) проверим число N на отсутствие малых простых делителей;
3) испытаем N на простоту каким-либо не слишком трудоёмким тестом достаточно много раз;
4) если выяснится, что N — составное, то выберем новое значение R и повторим вычисления.

Если N, выдерживает испытания данным алгоритмом, то возможно, что N — простое. Тогда следует попытаться доказать это с помощью более мощных и трудоёмких тестов[12)].

Факторизация и сплиттинг. *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 (RSA, некоторые схемы цифровой подписи и др.).

Отметим, что на существующих компьютерах распознавание простоты целого числа с 125 десятичными цифрами может быть выполнено за несколько минут, в то время как его факторизация потребует миллионы лет компьютерных вычислений, то есть практически неосуществима.

[12)] см. теорему 4 на с. 102 книги *Введение в криптографию / Под общ. ред. В. В. Ященко. — М.: МЦНМО, 2012.*

Сплиттингом натурального числа n называют представление его в виде

$$n = a \cdot b, \ \ a, b \in [\ 2,\ n-1\ ],$$

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
$$a := f(a),\ b := f(f(b)) \pmod{n}.$$
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 1.
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 4.8. 1. Разложим на нетривиальные сомножители число $n = 163\,829$.

1. $a = 5,\ b = 26$.

[13)] Предложен в 1975 г. британским математиком Джоном Поллардом (John M. Pollard, 1941). Название связано с тем, что алгоритм строит числовую последовательность, элементы которой, начиная с некоторого номера n образуют цикл, что иллюстрируется расположением чисел в виде греческой буквы ρ.

2. $a - b = 5 - 26 = -21 \equiv_{163\,829} = 163\,808$ и $d = \text{НОД}\,(163\,808, 163\,829) = 23.$
3. Поскольку $d \in [\,2,\ n-1\,]$, то $23 \mid 163\,829.$

Дальнейший анализ показывает, что $n/23 = 7\,123 = 17 \cdot 419.$

2. Пусть $n = 455\,459.$

Результаты вычислений по ρ-алгоритму Полларда приведены в таблице

	a	b	d
1	5	26	1
2	26	2871	1
3	677	179 685	1
4	2871	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

Задача DLOG. Криптосистема ЭльГамаля. Пусть G — мультипликативная абелева группа порядка n, $a, b \in G$. Задача нахождения решения уравнения

$$a^x \equiv_n b$$

называется *задачей (проблемой) дискретного логарифмирования* в группе G. Её решение x называется *дискретным логарифмом элемента* b *по основанию* a, символически $\log_a b$, если решение существует.

На сложности этой задачи DLOG базируется ряд асиметричных шифрсистем с отрытым ключом, в частности рассмотренная ранее система Диффи–Хелмана DH и система ElGamal, разработанная Эль-Гамалем[14].

Рассмотрим вариант последней, когда G есть мультипликативная группа простого поля $\mathbb{F}_p$, то есть

$$|G| = n = p - 1.$$

Пусть также α — 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

$$x_A, x_B \xleftarrow{\$} [\,2,\ p-2\,]$$

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).

[14] Taher ElGamal (1955) — американский криптограф египетского происхождения.

Пусть абонент A хочет передать абоненту B сообщение $m \in \mathbb{F}_p^*$. Для этого A выбирает ещё одно случайное число

$$s \xleftarrow{\$} [\,2,\ p-2\,],$$

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. Поэтому длина криптограммы в схеме ЭльГамаля вдвое длиннее исходного сообщения m.

Для расшифрования криптограммы, B вычисляет по $\bmod p$ значение m:

$$m = b(d_B)^{-s} = b(\alpha^{x_B})^{-s} = b(\alpha^s)^{-x_B} = ba^{p-1-x_B}.$$

Очевидно, шифрсистема фактически является ЭльГамаля одним из способов выработки открытых ключей Диффи-Хеллмана.

Пример 4.9. Алиса передаёт Бобу своё сообщение BUJ, используя шифрсистему ЭльГамаля.

Боб: вычисление ключей.

1) выбирает простое $p = 2357$ и находит генератор $\alpha = 2$ мультипликативной группы поля $\mathbb{F}_p$;
2) выбирает свой секретный улюч — 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

$$(\,p,\ \alpha,\ d_B\,) = (\ 2\,357,\ 2,\ 1\,185\ ).$$

Алиса: зашифрование.

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

$$s = 1520 \in [\,2,\, p-2\,];$$

4) вычисляет по mod 2 357 числа $a = \alpha^s = 1\,430$ и

$$b = m \cdot (d_B)^s = 2\,035 \cdot 1\,185^{1520} = 697;$$

5) посылает шифртекст $(\,1\,430,\, 697\,)$ Бобу.

Боб: расшифрование.

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 задачи DLOG 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 $\mathbb{Z}_p$, 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.

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 уравнение (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.

<u>*Алгоритм согласования*</u> решения уравнения (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

$$c^u \equiv_p b \cdot a^v \ \text{откуда} \ a^{Hu-v} \equiv_p b.$$

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 4.10. 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 4.11. Пусть требуется решить сравнение

$$2^x = 17 \pmod{25}.$$

Для этого рассмотрим группу $G = \mathbb{Z}_{25}^*$. Понятно, что $|G| = \varphi(25) = \varphi(5^2) = 5 \cdot \varphi(5) = 20 = n$, 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. $H = \lceil 20 \rceil = 5$.
2. $c = 2^5 \equiv_{25} 7$.
3. $u = 1, 2, 3, 5$

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 Нидеррайтера

Криптосистема МакЭлиса. Данная система зашифрования с открытым ключом основана на трудности решения задачи декодирования линейного кода, исправляющего ошибки[15)] (эта задача NP-трудна). Исторически первая система, использующая в процессе шифрования *рандомизацию* — преобразование

[15)] Разработана в 1978 г. американским математиком и инженером Р. Мак-Элисом (Robert J. McEliece, 1942).

данных во время зашифрования с помощью генератора псевдослучайных чисел. Кратко опишем простейший вариант данной криптосистемы.

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 $G_{n\times k}$.

Далее Алиса генерирует две квадратные матрицы:

P порядка n — перестановочную;

S порядка k — случайную невырожденную.

Вычисляя $n \times k$-матрицу

$$\widetilde{G} = P \times G \times S,$$

Алиса «маскирует» матрицу G.

Закрытым ключом является тройка матриц (S^{-1}, G, P^{-1}), а открытым — пара $(\widetilde{G}, r)$, который передаётся Бобу.

Боб, желая зашифровать своё сообщение $\boldsymbol{u}$ длины k, вычисляет вектор $\widetilde{G}\boldsymbol{u}$, добавляя к нему случайный n-вектор $\boldsymbol{e}$ с не более чем r единицами. В этом и состоит рандомизация информации.

Полученный шифртекст

$$\boldsymbol{w} = \widetilde{G}\boldsymbol{u} + \boldsymbol{e}.$$

Боб посылает Алисе.

Для расшифрования этой крипторгаммы Алиса вычисляет вектор

$$\widehat{\boldsymbol{w}} = P^{-1}\boldsymbol{w},$$

и, используя какой-либо алгоритм декодирования кода C, получает из $\widehat{\boldsymbol{w}}$ вектор $\widehat{\boldsymbol{u}}$. Исходно переданное сообщение Алиса получает, вычисляя

$$\boldsymbol{u} = S^{-1}\widehat{\boldsymbol{u}}. \tag{4.8}$$

Покажем, что описанная схемы расшифрования действительно восстанавливает исходное сообщение $\boldsymbol{u}$. Имеем:

$$\widehat{\boldsymbol{w}} = P^{-1}\boldsymbol{w} = P^{-1}\left[\widetilde{G}\boldsymbol{w} + \boldsymbol{e}\right] = \\ = P^{-1}\left[PGS\boldsymbol{w} + \boldsymbol{e}\right] = G\left[S\boldsymbol{w}\right] + P^{-1}\boldsymbol{e}.$$

Поскольку вектор $P^{-1}\boldsymbol{e}$ содержит не более r единиц, алгоритм декодирования кода C корректирует $\widehat{\boldsymbol{w}}$ до $S\boldsymbol{w} = \widehat{\boldsymbol{u}}$. Преобразование (4.8) завершает расшифрование.

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.

16) Харальд Нидеррайтер (Harald G. Niederreiter, 1944) — австрийский математик.

В отличие от неё, криптосистема Нидеррайтера использует проверочную H, а не порождающую матрица $(n, k, 2r+1)$-кода, и не использует рандоминзацию данных.

Открытым ключом является пара (H_{pub}, r), где $H_{pub} = S \times H \times P$, а S и P — выбранные квадратные матрицы: случайная невырожденная порядка $n-k$ и перестановок P 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 именно систему 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 Нидеррайтера взломаны российскими криптоаналитиками, однако они остаются стойкими при условии использовании *кодов Гоппы*[17].

[17] Криптосистема МакЭлиса на кодах Гоппы рассматривается Еврокомиссией как перспективная.

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

$$\text{а) } 6^x \equiv_{11} 2; \quad \text{б) } 8^x \equiv_{11} 3; \quad \text{в) } 2^x \equiv_{13} 3.$$

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

Эллиптическая криптография (ECC, Elliptic-curve cryptography) изучает асимметричные криптосистемы, основанные на эллиптических кривых (ЭК) над конечными полями.

Преимущество эллиптической криптографиии состоит в следующием:

1) существует бóльшая свобода в выборе ЭК, чем в выборе конечного поля, и поэтому они удобнее мультипликативных групп конечных полей;
2) наиболее быстрые методы, разработанные для конечных полей оказываются бесполезны в случае эллиптических кривых;
3) на сегодняшний день для них не известны даже субэкспоненциальные алгоритмы решения задачи DLOG на ЭК.

На эллиптических кривых 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.

5.1 Эллиптические кривые: введение

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* — 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.

Кривая E есть *неособенная* или *гладкая*, 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*

$$y^2 + a_1xy + a_3y \; = \; x^3 + a_2x^2 + a_4x + a_6, \tag{5.1}$$

называемому длинной формой Вейерштрасса.

<u>*Определение*</u> 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

$$-P \;=\; (x_0,\, -a_1x - a_3 - y_0) \tag{5.2}$$

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

$$y^2 \;=\; x^3 + ax + b. \tag{5.3}$$

В этом случае противоположная к $P = (x_0, y_0)$ точка эллиптической кривой E есть

$$-P \;=\; (x_0,\, -y_0). \tag{5.4}$$

Неожиданная нумерация индексов и название «эллиптическая кривая» объясняются следующими обстоятельствами. Формы Вейерштрасса при больших x ведут себя как полукубическая парабола $y^2 = x^3$ (см. рис. 5.1), допускающая одно-

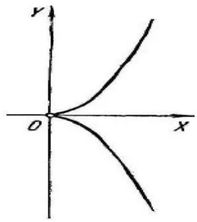

Рис. 5.1. Полукубическая парабола (парабола Нейла)

родную параметризацию $x = t^2$ и $y = t^3$. При данной параметризации индексы i коэффициентов a_i, $i = \overline{1,6}$ в (5.1) определяют степени, которые должны быть даны этим коэффициентам, чтобы уравнение стало однородным (то есть чтобы степень каждого слагаемого была равна 6). Кривым $y^2 = f(x)$ соответствуют *эллиптические интегралы* вида $\int \frac{dx}{\sqrt{f(x)}}$, не берущиеся в элементарных функциях, и, в свою очередь, 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 отличные от формы Вейерштрасса 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 $D > 0$ имеет три разных действительных корня, а при $D < 0$ — 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 абелеву группу.

Заметим, что на некоторых плоских кривых это можно осуществить, и простейшими примерами таких кривых являются прямая и окружность. Например, суммой двух точек $(r\cos\alpha, r\sin\alpha)$ и $(r\cos\beta, r\sin\beta)$, окружности $x^2 + y^2 = r$ будем считать точку $(r\cos(\alpha+\beta), r\sin(\alpha+\beta))$.

Замечательным свойством ЭК с $\Delta > 0$ является то, что прямая общего вида, проходящая через две

---

[1] Полукубическая парабола имеет точку возврата $(0, 0)$

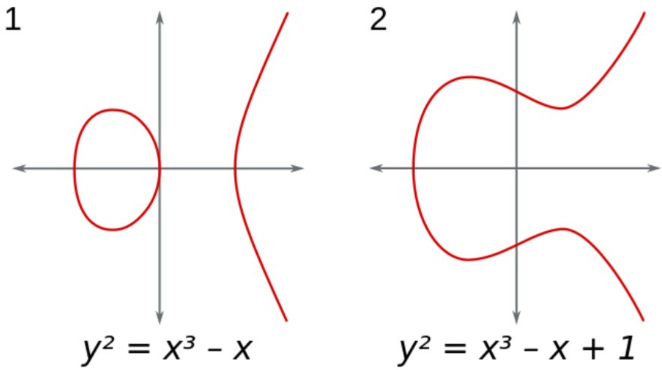

Рис. 5.2. Графики ЭК над $\mathbb{R}$ при (1) $\Delta = 64 > 0$ и (2) $\Delta = -368 < 0$

различные точки кривой, пересересечёт её ещё только в одной точке. Кроме того, касательная к ЭК в любой точке (кроме точек перегиба) также пересекает её 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 считаем, что ℓ пересекает E в бесконечной точке);

- если ℓ является касательной к E в некоторой точке, то такая точка считается дважды.

Такое определение сложения справедливо и для ЭК над любыми полями.

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 $y^2 = x^3 - x$.

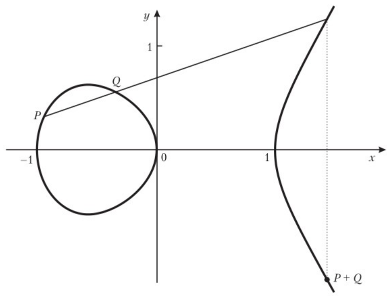

Рис. 5.3

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

$$Q = -P = -(x,y) = (x,-y). \qquad (5.7)$$

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

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{5.8}$$

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

$$\begin{cases} x_3 = \lambda^2 - 2x_1, \\ y_3 = -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{3x_1^2 + a}{2y_1}. \tag{5.9}$$

Геометрическую иллюстрацию формул суммирования и удвоения точек ЭК см. на рис. 5.4.

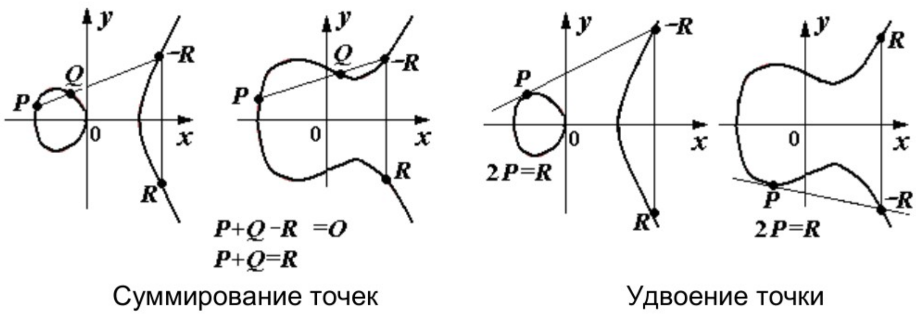

Рис. 5.4. Суммирование и удвоение точек на ЭК

Умножение точки P на целое положительное k определяется как сумма k точек P:

$$kP = P + P + \ldots + P.$$

Порядком точки ЭК называют наименьшее натуральное k такое, что $kP = \mathcal{O}$ (понятно, что такого k может и не существовать).

Арифметика эллиптических кривых не содержит прямых формул для вычисления кратного kP для заданной точки $P = (x, y)$, то эту операцию выполняют с использованием операций сложения, вычитания и удвоения точки.

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 (5.8) даёт $x_3 = 6$.
2. Тогда второе уравнение даёт $y_3 = 0$ и $P + Q = (6, 0)$ оказалась точкой перегиба.
3. Далее, подставляя $x_1 = -3$, $y_1 = 9$, $a = -36$ в первое из уравнение из (5.9) 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).

Ясно, что если точка P имеет порядок n, то множество

$$\{\, \mathcal{O},\ P,\ 2P,\ (n-1)P \,\}$$

образует циклическую подгруппу (по сложению) в группе точек ЭК и порядок точки n делит величину N — число точек ЭК.

5.2 Эллиптические кривые в конечных полях

Порядок эллиптической кривой. Множества точек эллиптической кривой над конечным полем, естественно, конечно. Порядок этой группы будем называть *порядком эллиптической кривой*.

Легко увидеть, что эллиптическая кривая над полем $K = GF(q)$, $q = p^n$, не может содержать более, чем $2q + 1$ точек: это бесконечная точка и не более, чем $2q$ пар $(x, y) \in K^2$, поскольку для каждого из q возможных значений $x \in K$ имеется не более 2-х значений y.

Но так как лишь у половины элементов K^* имеются квадратные корни, следует сразу ожидать, что порядок эллиптической кривой примерно вдвое меньше этого числа.

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
0	0	0
1	2	± 3
-1	5	—
2	3	—
-2	4	± 2
3	2	± 3
-3	5	—

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 $N = 5$.

4. Рассмотрим то же уравнение $y^2 = x^3 + x + 1$ над $K = \mathbb{Z}_5$ и найдём порядок $N = 9$ задаваемой им группы ЭК:

x	$x^3 + x + 1$	y
0	1	± 1
1	3	—
2	1	± 1
3	1	± 1
4	4	± 2

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 DLOG. 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 точки ЭК
над полем $GF(p)$

1. Определить $N_1 = p + 1 + 2\sqrt{p}$ (максимальная оценка порядка группы точек ЭК, полученная из теоремы Хассе) 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 1;
   - 5.2 если $\gamma = jP$, то считать $n = mi + j$; ОСТАНОВ.
   - 5.3 положить $\gamma = \gamma + \alpha$.

Пример 5.10. Найти порядок точки $P = (0, 1)$ эллиптической кривой

$$y^2 = x^3 + x + 1 \quad \text{над простым полем } GF(5).$$

Решение.

$$N_1 = p + 1 + 2\sqrt{p} = 5 + 1 + 2\sqrt{p} \approx 10 \Rightarrow$$
$$\Rightarrow m = \left\lceil \sqrt{N_1} \right\rceil = \left\lceil \sqrt{10} \right\rceil = 4.$$

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

$$n = mi + j = 4 \cdot 2 + 1 = 9.$$

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 $\mathrm{mod}\,(\mathrm{char}\,K)$.

Далее будем рассматривать точки ЭК

$$P = (x_1, y_1), \quad Q = (x_2, y_2)$$

и вычислять точек

$$-P, \quad P+Q \text{ и } 2P,$$

лежащих на рассматриваемой 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. 165 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 5.11. 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 5.12. *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 5.13. *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.*

Известны и следующие факты.

- При $q = p^n$, $p \geqslant 3$, $q = 3 \pmod 4$ порядок эллиптической кривой $y^2 = x^3 - n^2 x$ над полем $GF(q)$ равен $q + 1$.
- Порядок эллиптической кривой $y^2 = x^3 + b$ над простым полем $GF(p)$ при $p \equiv 2 \pmod 3$ равен $p + 1$.

  При этом для всякого y на кривой лежит ровно одна точка $\big((y^2 - b)^{1/3}, y\big)$.

$\underline{\operatorname{char} K = 3}$. В этом случае уравнение (5.1) при подходящей замене переменных принимает вид

$$y^2 \;=\; x^3 + ax^2 + bx + c, \quad a, b, c \in GF(3^n). \tag{5.10}$$

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 (5.8) для координат точки $P + Q = 2P$ остаются справедливыми.
4. При $x_1 = x_2$ точка $P + Q = 2P$ имеет координаты

$$\begin{cases} x_3 \;=\; \lambda^2 - a + x_1, \\ y_3 \;=\; -y_1 + \lambda \cdot (x_1 - x_3), \end{cases} \qquad \lambda = \frac{ax_1 - b}{y_1}. \tag{5.11}$$

Пример 5.14. 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
t	t
t^2	t^2
t^3	$t - 1$
t^4	$t^2 - t$
t^5	$-t^2 + t - 1$
t^6	$t^2 + t + 1$
t^7	$t^2 - t - 1$
t^8	$-t^2 - 1$
t^9	$t + 1$
t^{10}	$t^2 + t$
t^{11}	$t^2 + t - 1$
t^{12}	$t^2 - 1$
t^{13}	-1
t^{13+k}	$-t^k,\ k = \overline{1, 13}$

С её помощью составим таблицу значений многочлена $z(x) = x^3 + 2x + 1$ и $y = \pm\sqrt{z(x)}$.

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:

$$\Big\{ (0,\pm 1),\ (1,\pm 1),\ (-1,\pm 1),\ (t,0),\ (t^3,0),\ (t^9,0),\\ (-t^2,\pm t^7),\ (-t^4,\pm t^{11}),\ (t^5,\pm t^{11}),\ (-t^6,\pm t^8),\\ (-t^7,\pm t^{11}),\ (t^8,\pm t^7),\ (-t^{10},\pm t^8),\ (-t^{11},\pm t^8),\\ (-t^{12},\pm t^7),\ \mathcal{O} \Big\}.$$

<u>$\operatorname{char} K = 2$</u>. 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 — $\quad y^2 + a_3 y = x^3 + a_4 x + a_6,$

несуперсингулярная — $\quad y^2 + xy = x^3 + a_2 x^2 + a_6.$

Заметим, что в рассматриваемом случае не имеется ограничений на кратность корней полиномов в правых частях указанных уравнений.

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 5.15. 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 таких классов.

Главный недостаток суперсингулярных ЭК заключается в том, что для них известно сведение задачи DLOG 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 DLOG 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 эллиптические кривые задаются в короткой форме Вейерштрасса, а в качестве поля выбираются поля $GF(p)$ или $GF(2^n)$ где p, n достаточно велики. Но исследования ведутся и для произвольных конечных полей $GF(q)$, $q = p^n$.

Задача DLOG в группе точек ЭК. Вообще задача DLOG может быть поставлена для любой группы G, в том числе и для группы точек эллиптической кривой (ECDLP, Elliptic Curve Discrete Logarithm Problem).

Следует только действия над элементами мультипликативной группы заменить соответствующие действия над элементами ЭК — см. рис. 5.5.

Тогда задача DLOG принимает вид нахождения целого числа m из соотношения

$$m \cdot P = Q$$

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	$g \in Z_p{}^*$; $h \equiv g^a (\mathrm{mod}\, p)$; найти a	$P \in E(GF(p))$; $Q = mP$; найти m

Рис. 5.5. «Перевод» обычного криптоалгоритма в эллиптический

для точек P и Q ЭК.

Временна́я сложность наилучшего из всех известных алгоритмов решения этой задачи имеет порядок $O(p^{0,5})$. С такой сложностью решить задачу DLOG можно в любой группе, и до сих пор не удалось существенно использовать специфику самой группы точек ЭК. Поэтому использование группы точек ЭК при построении криптосистем позволило уменьшить параметры криптосистем при сохранении их стойкости.

Считается, что 256-битные операции ECC эквивалентны работе с модулем длиной 3072 бита в RSA.

Шифросистема Эль-Гамаля на эллиптических кривых над конечным полем $GF(q)$ основана на трудности решения задачи DLOG. Она аналогична шифрсистеме на циклической мультипликативной группе конечного поля.

Следует иметь в виду, что аддитивная группа точек ЭК циклической может не быть. Задача разработчика — найти подходящую ЭК и 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 q можно брать меньше, на практике его длина от 150 до 350 бит.

Рассмотрим алгоритм работы данной системы.

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 генератор 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 (или всем заинтересованным лицам) по незащищённому каналу.

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 и получить.
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 5.16. Пусть Алисе необходимо передать Бобу некоторое секретное сообщение. 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 набольшего порядка $N = 1486$ и определяется её генератор $P = (8, 2123)$.

Системные параметры суть набор (E, N, P).

Далее все вычисления проводятся по $\bmod N$ и формулам (5.7) и (5.8) 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

   $$\begin{aligned} d &= r \cdot Y = 1325 \cdot (589, 1045) = (2047, 1793), \\ g &= r \cdot P = 1325 \cdot (8, 2123) = (192, 742), \\ h &= M + d = (1634, 2494) + (2047, 1793) = \\ &\quad = (351, 33). \end{aligned}$$

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 $t = \mathrm{FA}$.

Решения задач

1. Группы, кольца, поля

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

1) целые числа, кратные данному натуральному числу n, относительно сложения?
2) неотрицательные целые числа относительно сложения?
3) нечетные целые числа относительно сложения?
4) нелые числа относительно вычитания?
5) рациональные числа относительно умножения?
6) рациональные числа, отличные от нуля, относительно умножения?
7) положительные рациональные числа относительно умножения?
8) положительные рациональные числа относительно деления?
9) корни n-й степени из единицы (как действительные, так и комплексные) относительно умножения?
10) матрицы порядка n с действительными элементами относительно умножения?
11) невырожденные матрицы порядка n с действительными элементами относительно умножения?
12) перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок?
13) преобразования множества M, то есть взаимнооднозначные отображения этого множества на себя, относительно композиции отображений?
14) элементы n-мерного векторного пространства $\mathbb{R}^n$ относительно сложения?
15) параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений?

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

(1) Да, (2) нет (противоположного элемента), (3) нет (устойчивости), (4) нет (ассоциативности), (5) нет (обратного у 0), (6) да, (7) да, (8) нет (ассоциативности), (9) да, (10) нет (обратных у всех), (11)–(16) да.

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

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

1. Все подгруппы циклической группы — циклические. Порождающими элементами *подгрупп* $\mathbb{Z}_{24}$ будут делители m порядка группы 24: то есть $m = 1, 2, 3, 4, 6, 8, 12, 24 \equiv 0$.
Порядок соответствующей подгруппы — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle = C \cong \mathbb{Z}_{24}$;
$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12}$;
$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_8$;
$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_6$;
$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_4$;
$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_3$;
$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_2$;
$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — единичная.

2. Циклическая группа $\mathbb{Z}_{24}$ имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \cdot \varphi(2) \cdot \varphi(3) = 4 \cdot 1 \cdot 2 = 8$ генераторов. Они взаимно просты с 24 и суть 1, 5, 7, 11, 13, 17, 19, 23.

1.3. Вычислите функцию Эйлера для:

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

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

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

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

1. Все подгруппы циклической группы — циклические. Порождающими элементами подгрупп $\mathbb{Z}_{24}$ будут делители m порядка группы 24: то есть $m = 1$, 2, 3, 4, 6, 8, 12, $24 \equiv 0$.
Порядок соответствующей подгруппы — $24/m$.

$m = 1 : \{ 1, 2, \ldots, 23, 0 \} = \langle 1 \rangle = C \cong \mathbb{Z}_{24};$

$m = 2 : \{ 2, 4, 6, \ldots, 22, 0 \} = \langle 2 \rangle \cong \mathbb{Z}_{12};$

$m = 3 : \{ 3, 6, 9, \ldots, 21, 0 \} = \langle 3 \rangle \cong \mathbb{Z}_{8};$

$m = 4 : \{ 4, 8, 12, \ldots, 20, 0 \} = \langle 4 \rangle \cong \mathbb{Z}_{6};$

$m = 6 : \{ 6, 12, 18, 0 \} = \langle 6 \rangle \cong \mathbb{Z}_{4};$

$m = 8 : \{ 8, 16, 0 \} = \langle 8 \rangle \cong \mathbb{Z}_{3};$

$m = 12 : \{ 12, 0 \} = \langle 12 \rangle \cong \mathbb{Z}_{2};$

$m = 24 : \{ 0 \} = \langle 0 \rangle \cong E$ — единичная.

2. Циклическая группа $\mathbb{Z}_{24}$ имеет $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2 \cdot \varphi(2) \cdot \varphi(3) = 4 \cdot 1 \cdot 2 = 8$ генераторов m, взаимно простых с 24, то есть $m = 1$, 5, 7, 11, 13, 17, 19, 23.

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

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

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) =$$
$$= p_1^{\alpha_1 - 1}\varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_k) =$$
$$= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_1) \cdot \ldots \cdot \varphi(p_k) =$$
$$= \frac{n}{p_1 \cdot \ldots \cdot p_k} \cdot (p_1 - 1) \cdot \ldots \cdot (p_k - 1) =$$
$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

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

1. квадратные матрицы данного порядка с *действительными* элементами относительно сложения и умножения матриц?
2. многочлены одного неизвестного с целыми коэффициентами относительно обычных операций сложения и умножения?
3. многочлены одного неизвестного с действительными коэффициентами относительно обычных операций?

(1) Кольцо (обратной матрицы может не быть), (2) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы), (3) кольцо (многочлены $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ в случае $a_0 = 0$ необратимы.

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

По дистрибутивности

$$x\cdot(y+z) = x\cdot y + x\cdot z \Rightarrow x\cdot(0+0) = x\cdot 0 = x\cdot 0 + x\cdot 0 \Rightarrow \\ \Rightarrow x\cdot 0 = 0.$$

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

Нет! Хотя $f(x+y) = 2(x+y) = 2x+2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x)\cdot(2y) = f(x)\cdot f(y)$.

1.9. Показать, что множество векторов пространства с операциями сложения и векторного умножения является кольцом.

Является ли оно ассоциативным? коммутативным?

Множество векторов V содержит нулевой вектор $\mathbf{0}$ и является, очевидно, абелевой группой по сложению, а операция $\times$ векторного умножения связана со сложением дистрибутивными законами

$$\boldsymbol{x} \times (\boldsymbol{y} + \boldsymbol{z}) = \boldsymbol{x} \times \boldsymbol{y} + \boldsymbol{x} \times \boldsymbol{z}, \\ (\boldsymbol{y} + \boldsymbol{z}) \times \boldsymbol{x} = \boldsymbol{y} \times \boldsymbol{x} + \boldsymbol{z} \times \boldsymbol{x}.$$

Кольцо $\langle V, +, \times, \mathbf{0} \rangle$ некоммутативно: $\boldsymbol{x} \times \boldsymbol{y} \neq \boldsymbol{y} \times \boldsymbol{x}$ и неассоциативно: $\boldsymbol{x} \times (\boldsymbol{y} \times \boldsymbol{z}) \neq (\boldsymbol{x} \times \boldsymbol{y}) \times \boldsymbol{z}$.

Однако в рассматриваемом кольце выполняются тождества, заменяющие, в некотором смысле коммутативность и ассоциативность:

$$\boldsymbol{x} \times \boldsymbol{y} = -\boldsymbol{y} \times \boldsymbol{x} \quad \text{(антикоммутативность)}, \\ (\boldsymbol{x} \times \boldsymbol{y}) \times \boldsymbol{z} + (\boldsymbol{y} \times \boldsymbol{z}) \times \boldsymbol{x} + \\ + (\boldsymbol{z} \times \boldsymbol{x}) \times \boldsymbol{y} = \mathbf{0} \quad \text{(тождество Якоби)}.$$

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

В кольце $\mathbb{Z}_6$ классы вычетов по идеалу $(3) = \{0, 3\}$ суть

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

1.11. Является ли поле $\mathbb{Z}_2$ подполем поля $\mathbb{Z}_5$?

Нет! В $\mathbb{Z}_2 : 1 + 1 = 0$, а в $\mathbb{Z}_5$: $1 + 1 = 2$, то есть операция сложения в $\mathbb{Z}_5$ неустойчива при переходе к своему подмножеству $\{0, 1\}$.

2. Конечные кольца и поля

2.1. С помощью алгоритма Евклида вычислите НОД (a, b)

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.

2.2. Найти

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

Вычислять x^{-1} в кольцах $\mathbb{Z}_n$ можно используя соотношение Безу (подбором коэффициентов или обобщённым алгоритмом Евклида). В некоторых очевидных случаях (напр. в пункте в)) можно обойтись без вычислений.

а) $1 = 2 \cdot 3 - 1 \cdot 5,\ 2 \cdot 3 = 1 + 1 \cdot 5,\ 2 \cdot 3 \equiv_5 1,\ 3^{-1} \equiv_5 2;$

Или

$$\begin{array}{c|cc|l}
1 & 5 & 0 & \\
2 & 3 & 1 & q = 1 \\
\hline
3 & 2 & \text{-1} & q = 1 \\
4 & 1 & \mathbf{2} & q = 2 \quad (\ 2 \ldots) \\
5 & 0 & &
\end{array}$$

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

$$\begin{array}{c|cc|l}
1 & 14 & 0 & \\
2 & 9 & 1 & q = 1 \\
\hline
3 & 5 & \text{-1} & q = 1 \\
4 & 4 & 2 & q = 1 \\
5 & 1 & \text{-}\mathbf{3} & q = 4 \quad (\ 4 \ldots) \\
6 & 0 & &
\end{array}$$

Таким образом, $9^{-1} = \text{-}3 \equiv_{14} 11$.

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) $1 = 3 \cdot 3 - 8,\ 3 \cdot 3 = 1 + 8,\ 3 \cdot 3 \equiv_8 1,$
$3^{-1} \equiv_8 3,\ 3^{-3} = (3^{-1})^3 = 3^3 = 27 = 3 \pmod 8.$

2.3. Решите сравнение

а) $x = 7^{-1} \cdot 11 = 18 \cdot 11 = 198 = 23 \pmod{25};$

б) $x = 9^{-1} \cdot 3 = (-1)^{-1} = 3 = -3 = 7 \pmod{10};$

в) $6x \equiv_7 1,\ x = 6^{-1} = -1 = 6 \pmod 7;$

г) $6x \equiv_9 1$ решений нет: элемент 6 не обратим в $\mathbb{Z}_9$;

д) $6x \equiv_9 2$; решений нет: сравнение можно сократить — $3x \equiv_9$, но элемент 3 не обратим в $\mathbb{Z}_9$;

е) $6x \equiv_9 3$. Такое равенство можно сократить на 3 вместе с модулем: $2x \equiv_3 1$, откуда $x = 2^{-1} = 2 \pmod 3$. Множество решений — $\{2, 5, 8\} \pmod 9$.

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

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

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

Имеем

$$F = \mathbb{F}_2[x]/\bigl(x^2 + x + 1\bigr) = \{\,0, 1 = \alpha^3, \alpha, \alpha + 1 = \alpha^2\,\},$$

где α — порождающий элемент мультипликативной группы F^*. Поэтому

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

$$
\begin{aligned}
&= (x+1)\left(x^2+\alpha x+x+\alpha x+\alpha^2+\alpha\right) = \\
&= (x+1)\left(x^2+x+\alpha^2+\alpha\right) = \\
&= \big(x^3+(\alpha+1)x^2+(\alpha+1)x^2+(\alpha^2+\alpha+1)x+ \\
&\qquad +\alpha^2+\alpha\big) = x^3+1,
\end{aligned}
$$

и по теореме 2.19:

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

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

Все элементы $\mathbb{F}_p^*$ суть корни уравнения

$$x^{p-1}-1 = 0,$$

их *сумма* по теореме Виета есть коэффициент при x^{p-2} в этом уравнении, то есть 0.

2.6. Доказать, что

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

При $p=2$ утверждение тривиально.

При $p > 2$ порядки всех элементов мультипликативной циклической группы $\mathbb{F}_p^* = \{1, \ldots, p-1\}$ делят её порядок то есть все они являются корнями уравнения

$$x^{p-1}-1 = 0. \qquad (*)$$

Других корней у этого уравнения нет (многочлен степени $p-1$ имеет не больше $p-1$ корней). По теореме Виета их произведение равно свободному члену многочлена $(*)$, то есть -1.

Ещё одно Решение. Для $p = 2, 3$ утверждение тривиально. При $p \geqslant 5$ обозначим

$$1\cdot\underbrace{2\cdot\ldots\cdot(p-2)}_{=\pi}\cdot(p-1) = (p-1)!,$$

и заметим, что $(p-1)^2 = p^2 - 2p + 1 \equiv_p 1$.

Легко видеть, что произведение $\pi = 1$: каждый из элементов $2, \ldots, p-2$ поля $\mathbb{F}_p$ имеет единственный обратный, и он входит в $\pi = 1$, т. к. элемент $p-1$ обратен сам себе.

Отсюда $(p-1)! = p-1$, или $(p-1)! \equiv_p -1$.

2.7. Построить поле из 4-х элементов.

Это поле $\mathbb{F}_2^2$, оно может быть построено как факторкольцо $\mathbb{F}_2[x]/\left(a(x)\right)$, где $a(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$ степени 2. Но такой многочлен только один: $x^2 + x + 1$.

Следовательно, $\mathbb{F}_2^2 = \{\, 0,\, 1,\, x,\, x+1 \,\}$ и $x^2 = x+1$ (черту над элементами не пишем).

Таблицы сложения и умножения в построенном поле (операции с 0 опускаем):

$+$	1	x	$x+1$
1	0	$x+1$	x
x	$x+1$	0	1
$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

2.8. В кольце $\mathbb{Z}_2[x]$ найти

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

Воспользуемся алгоритмом Евклида:

$$x^5 + x^2 + x + 1 = \left(x^2 + x\right)\left(x^3 + x^2 + x + 1\right) + \\ + \underline{\left(x^2 + 1\right)},$$

$$x^3 + x^2 + x + 1 = (x+1)\underline{\left(x^2+1\right)}.$$

Ответ: $x^2 + 1$.

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

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

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

Поле $F = \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$ содержит 8 элементов: 0 и степени 1, …, 7 порождающего элемента α. Можно полагать $x = \alpha$, т. к. $a(x)$ — примитивный многочлен.

1. Таблица соответствий между полиномиальным и степенным представлением его ненулевых элементов:

$x^3 = x + 1$ степень x	1	x	x^2
x	0	1	0
x^2	0	0	1
$x^3 = x + 1$	1	1	0
$x^4 = x^2 + x$	0	1	1
$x^5 = x^2 + x + 1$	1	1	1
$x^6 = x^2 + 1$	1	0	1
$x^7 = 1$	1	0	0

2. Таблица умножения:

$\times$	x	x^2	x^3	x^4	x^5	x^6
x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1
x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1	x
x^3	x^2+x	x^2+x+1	x^2+1	1	x	x^2
x^4	x^2+x+1	x^2+1	1	x	x^2	$x+1$
x^5	x^2+1	1	x	x^2	$x+1$	x^2+x
x^6	1	x	x^2	$x+1$	x^2+x	x^2+x+1

3. Обратные элементы:

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

4. Поле F имеет $\varphi(7)=6$ порождающих элементов: все кроме 0 и 1.

5. Находим м. м. элементов поля. Ясно, что
   - $m_0(x)=x$;
   - $m_1(x)=x+1$;
   - остальные элементы F суть порождающие его мультипликативной группы, и их м. м. будут совпадать с $a(x)$.

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

Поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$ если и только если $k \mid n$, поэтому подполями $GF\left(2^{30}\right)$ будут поля $GF\left(2^k\right)$, $k \in D(30) = \{1,2,3,5,6,10,15,30\}$, $GF\,(2)$ — *простейшее* и $GF\left(2^{30}\right)$ — *несобственное* подполя.

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

Выведете из полученной формулы малую теорему Ферма: *если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.* Если не отождествлять раскраски указанного типа, то всех раскрасок r^p.

Исключим одноцветные раскраски, остальных — $r^p - r$. Вращение раскрашенного более, чем в один цвет p-угольника вокруг своего центра на p углов $\frac{2\pi}{p}$, $2\frac{2\pi}{p}$, …, 2π даст одинаковые раскраски.

Итого, число различных раскрасок в более, чем один цвет равно $\frac{a^p - a}{p}$, и тогда всех раскрасок — $C = \frac{a^p-a}{p} + a$.

$C = \frac{a\left(a^{p-1}-1\right)}{p} + a$ — целое число. Отсюда, если $a \not\vdots\, p$, то $(a^{p-1}-1) \vdots\, p$, т. е. $(a^{p-1}-1) \equiv_p 0$ или $\frac{a^{p-1}-1}{p}$.

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

В поле $\mathbb{F}_2$ имеем $x - 1 = x + 1$.

1. $f(1) = 0 \Rightarrow 1$ — корень f.
2. Делим $f(x)$ на $x + 1$, получаем
$$x^4 + x^3 + x + 1 = f_1(x).$$
3. $f_1(1) = 0 \Rightarrow 1$ — корень f_1; $\frac{f_1}{x+1} = x^3 + 1 = f_2(x)$.
4. $f_2(1) = 0 \Rightarrow 1$ — корень f_2; $\frac{f_2}{x+1} = x^2 + x + 1$.
5. Многочлен $x^2 + x + 1$ неприводим.

Ответ: $x^5 + x^3 + x^2 + 1 = (x+1)^3\left(x^2 + x + 1\right)$.

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

1. $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$,
   $(x - 2) \equiv_5 (x + 3)$
2.
$$
\begin{array}{r|r}
x^3 + 2x^2 + 4x + 1 & x + 3 \\
\cline{2-2}
\underline{x^3 + 3x^2 } & x^2 + 4x + 2 \\
4x^2 + 4x & \\
\underline{4x^2 + 2x } & \\
2x + 1 & \\
\underline{2x + 1} & \\
0 &
\end{array}
$$
3. Перебором убеждаемся, что многочлен $x^2 + 4x + 2$ неприводим в $\mathbb{F}_5$.

Ответ: $x^3 + 2x^2 + 4x + 1 = (x + 3)\big(x^2 + 4x + 2\big)$.

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: $f(x) = x^4 + x^3 + x + 2 = \big(x^2 + 1\big)\big(x^2 + x + 2\big)$.

2.15. Многочлен

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

разложить на неприводимые множители.

1. $f(x) \neq 0$ ни при каком $x = 0, 1, 2, 3, 4$, то есть $f(x)$ не имеет линейных делителей.

2. Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем

Ответ: $f(x) = \left(x^2 + x + 1\right)\left(x^2 + 2x + 4\right)$.

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

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

Перебором коэффициентов $b, c \in \{0, 1, 2\}$ в выражении x^2+bx+c, находим подходящие многочлены:

$$\begin{aligned} f_1(x) &= x^2 + 1, \\ f_2(x) &= x^2 + x + 2, \\ f_3(x) &= x^2 + 2x + 2. \end{aligned}$$

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

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

$$\begin{aligned} f_1(x) &= x^3 + 2x + 1, \\ f_2(x) &= x^3 + 2x + 2, \\ f_3(x) &= x^3 + x^2 + 2, \\ f_4(x) &= x^3 + 2x^2 + 1, \\ f_5(x) &= x^3 + x^2 + x + 2, \\ f_6(x) &= x^3 + x^2 + 2x + 1, \end{aligned}$$

$$f_7(x) = x^3 + 2x^2 + x + 1,$$
$$f_8(x) = x^3 + 2x^2 + 2x + 2.$$

2.18. Определить, является ли:

1. многочлен $a(x) = x^2 + 2x + 4 \in \mathbb{F}_5[x]$ — неприводимым?
2. элемент $4x^2 + 2$ — корнем $a(x)$ в факторкольце/поле $\mathbb{F}_5[x]/(x^3 + 2x + 4)$?

1. Перебором элементов из $\mathbb{F}_5$ —

$$a(0) = 4,\ a(1) = 2,\ a(2) = 1,\ a(3) = 2,\ a(4) = 1,$$

убеждаемся, что квадратный многочлен $a(x)$ неприводим.

Следовательно, факторкольцо $\mathbb{F}_5[x]/\big(x^2 + 2x + 4\big)$ *является полем*; в нём $x^2 = -2x - 4 = 3x + 1$.

2. $a(4x^2 + 1) = \big(2(2x^2 + 1)\big)^3 + 2 \cdot 2(2x^2 + 1) + 4 =$
$= 3(3x^6 + 2x^4 + x^2 + 1) + 3x^2 + 3 = 4x^6 + x^4 + x^2 + 1 =$
$= 4(3x + 1)^2 + 3x^2 + x + x^2 + 1 = x^2 + 4x + 4 + 3x^2 + x + x^2 + 1 = 0$ — да, является.

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

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

1. $a(x) = x^2 + x - 1$, $a(0) = 6$, $a(1) = 1$, $a(2) = 5$, $a(3) = 4$, $a(4) = 6$, $a(5) = 1$, $a(6) = 6$, то есть многочлен $a(x)$ — *неприводим* в $\mathbb{F}_7$ и F — поле ($\cong \mathbb{F}_7^2$).

2. $\mathbb{F}_7^2 = \left\{\, ax + b \mid a, b \in \mathbb{F}_7,\ x^2 = 1 - x = 6x + 1 \,\right\}$

$$(ax+b)\cdot(6x+1) \;=\; \ldots \;=\; (2a+6b)x+(6a+b) \;=\; 1$$

$$\begin{cases} 6a+b &= 1 \\ a+3b &= 0 \end{cases} \Rightarrow \begin{cases} a=1 \\ b=2 \end{cases}$$

Ответ: $(1-x)^{-1} = x+2$ в F.

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

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

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

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

Мультипликативная группа указанных полей состоит из $2^4-1=15$ элементов.

Примарное разложение 15: $15 = 3\cdot 5$, поэтому равенство $\beta^d = 1$ нужно проверить для $d = 15/5 = 3$ и $d = 15/3 = 5$.

1. $\underline{x^4 = x+1}$

$$\begin{aligned} \beta^2 \;&=\; x^2(x+1)^2 \;=\; x^4+x^2 = x^2+x+1, \\ \beta^3 \;&=\; x(x+1)\left(x^2+x+1\right) \;=\; x\left(x^3+1\right) \;= \\ &=\; x^4+x = x+1+x \;=\; 1. \end{aligned}$$

Ответ: В поле F_1 $\operatorname{ord}\beta = 3$.

2. $\underline{x^4 \;=\; x^3+1}$

$$\begin{aligned} \beta^2 \;&=\; x^4+x^2 \;=\; x^3+x^2+1, \\ \beta^3 \;&=\; x(x+1)\left(x^3+x^2+1\right) \;= \\ &=\; x\left(x^4+x^2+x+1\right) \;=\; x\left(x^3+x^2+x\right) \;= \\ &=\; x^4+x^3+x^2 \;=\; x^2+1 \;\neq\; 1, \end{aligned}$$

$$\beta^5 = x^2x^3 = \left(x^3+x^2+1\right)\left(x^2+1\right) =$$
$$= \left(x^5+x^4+x^2+x^3+x^2+1\right) = \ldots$$
$$\ldots = \left(x^3+1\right)x = x^4+x = x^3+x+1 \neq 1.$$

Ответ: В поле F_2 $\operatorname{ord}\beta = 15$.

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

Мультипликативная группа поля

$$\mathbb{F}_2[x]/\left(x^6+x^3+1\right)$$

состоит из $2^6-1 = 63$ элементов.

Простые делители $63 = 3^2 \cdot 7$ суть 3 и 7, поэтому равенство $x^d = 1$ нужно проверить только для $d = 21 = \frac{63}{3}$ и $d = 9 = \frac{63}{7}$.

В рассматриваемом поле $x^6 = x^3+1$ и

$$x^9 = x^6x^3 = \left(x^3+1\right)x^3 = x^6+x^3 = \cancel{x}^3+1+\cancel{x}^3 = 1.$$

Т.о. $\operatorname{ord} x = 9 \neq 63$ и многочлен $f(x)$ *не примитивен*.

2.22. Найти количество нормированных неприводимых многочленов

1) степени 7 над полем $\mathbb{F}_2$;
2) степени 6 над полем $\mathbb{F}_5$.

$$\sum_{d|n} d \cdot I_p^d = p^n.$$

1. $\underline{((7))\text{ над }\mathbb{F}_2}$

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

$((1)) = 2$: это x и $x+1$, отсюда $((7)) = \frac{128-2}{7} = 18$.

2. $\underline{((6))\ \text{над}\ \mathbb{F}_5}$

$$((6)) = \frac{1}{6}\sum_{d|6}\mu(d)\,5^{\frac{6}{d}} = \frac{1}{6}\left[\,\mu(1)5^6+\mu(2)5^3+\right.$$

$$\left.+\mu(3)5^2+\mu(6)5\,\right] = \frac{15625-125-25+5}{6} = 2\,580.$$

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

С её помощью вычислить выражение

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

Поскольку $\operatorname{char} F = 3$, то $-2x^2+x+2 \equiv_3 x^2+x+2 = a(x)$.

$F = \mathbb{F}_3^2$, F^* содержит $3^2-1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1,8}$ примитивного элемента α.

Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в $\mathbb{F}_3^2$ проводятся по $\mod a(x)$, будем иметь

$$x^2+x+2 = 0 \Rightarrow x^2 = -x-2 = 2x+1.$$

Найдём порядок элемента x: т. к. $8 = 2^3$, $\frac{8}{2} = 4$, проверим равенство $x^4 = 1$:

$$x^4 = \left(x^2\right)^2 = (2x+1)^2 = x^2+x+1 =$$
$$= \cancel{2}x+1+\cancel{x}+1 = 2 \neq 1,$$

то есть x — примитивный элемент F: $\operatorname{ord} x = 8$ и $x^8 = 1$.

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над $\mathbb{F}_3$, иначе примитивный элемент поля F пришлось бы искать.

Теперь вычислим значение заданного выражения. Имеем $2^8 = 256 \equiv_3 1$, $x + 2 = -x^2$, $x^4 = 2$ и далее:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} =$$
$$= x^6 + x^4 = \left(x^2\right)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \cancel{1} + \cancel{2} =$$
$$= 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

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

В данном 9-элементном поле

$$x^2 + 1 = 0 \;\Rightarrow\; x^2 = -1 \equiv_3 2.$$

1. Найдём порядок элемента x, для чего проверим равенство $x^4 = 1$ (т. к. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = \left(x^2\right)^2 = 4 \equiv_3 1.$$

Следовательно $\operatorname{ord} x = 4$ и элемент x не является генератором группы F^* (и $x^2 + 1$ — не есть примитивный многочлен над $\mathbb{F}_3$:
$x^4 - 1 = x^4 + 2 = \left(x^2+1\right)\left(x^2+2\right)$).

2. Проверим на примитивность элемент $x + 1$:

$$(x+1)^4 = (x+1)(x+1)^3 = (x+1)\left(x^3+1\right) =$$

$$= (x+1)(2x+1) = 2x^2 + \cancel{x} + \cancel{2}x + 1 = 4+1 = 2 \neq 1$$

то есть $\alpha = x+1$ оказался примитивным элементом. Его степени:

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

Замечание: вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

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

Сначала убедимся, что многочлен $f(x) = x^2+x+2$ неприводим: ни одно из значений $f(x)$, $x \in \mathbb{F}_3$ не равно 0.

Далее проверим, является ли $f(x)$ делителем x^4+1?

$$x^4+1 = \left(x^2+x+2\right) t \left(x^2+2x+2\right) \text{ — да, является}$$

Поэтому искомый идеал составят многочлены из R, кратные $f(x)$:

$$\left(x^2+x+2\right) = \left\{ \left(x^2+x+2\right)(ax+b) \mid a, b \in \mathbb{F}_3, x^4 = 1 \right\}.$$

Теперь проведём умножение:

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

Перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $\left(x^2+x+2\right)$:

a	b	$ax^3 + (a+b)x^2 + (2a+b)x + 2b$
0	0	0
0	1	$x^2 + x + 2$
0	2	$2x^2 + 2x + 1$
1	0	$x^3 + x^2 + 2x$
1	1	$x^3 + 2x^2 + 2$
1	2	$x^3 + x + 1$
2	0	$2x^3 + 2x^2 + x$
2	1	$2x^3 + 2x + 2$
2	2	$2x^3 + x^2 + 1$

А если бы $f(x) \nmid a(x)$? Тогда в R существует идеал, порождённый элементом НОД $(f(x), a(x))$.

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

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

Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \cdot \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ с учётом $x^2 = 2x + 2$:

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

2. Найдём обратный к $4x + 3$ элемент, решая соотношение Безу

$$\bigl(x^2+3x+3\bigr)\,a(x)+(4x+3)b(x) \;=\; 1$$

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*

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x)+r_0(x),\\ q_0(x) &= 4x+4,\\ r_0(x) &= 1, \;\; // \;\; \deg r_0 = 0 \;\Rightarrow\; \textit{ОСТАНОВ}\\ y_0(x) &= y_{-2}(x)-y_{-1}(x)q_0(x) \;=\\ &\quad = -q_0(x) \;=\; -4x-4 \;=\; x+1. \end{aligned}$$

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 множителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.

Таковых над $\mathbb{F}_2$ только один — x^2+x+1.

При делении $f(x)$ на x^2+x+1, получаем

$$f(x) \;=\; \bigl(x^2+x+1\bigr)\cdot$$

$$\cdot\,(\underbrace{x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1}_{g(x)}).$$

Делим частное $g(x)$ на x^2+x+1:

$$g(x) = x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = \left(x^2+x+1\right)\cdot\left(x^7+x^4+x^3+x^2+x+1\right)+x$$

— не делится нацело, то есть x^2+x+1 — делитель $f(x)$ кратности 1.

3. Неприводимых многочленов 3-й степени над $\mathbb{F}_2$ только два: x^3+x+1 и x^3+x^2+1.
Пробуем поделить $g(x)$ на x^3+x+1:

$$x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = \left(x^3+x+1\right)(\underbrace{x^6+x^5+x^3+x^2+1}_{h(x)}) \quad \text{— делится!}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

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

Поскольку многочлен $h(x)$ 6-й степени не имеет делителей 3-й и меньших степеней, то он является неприводимым.

Ответ: В $\mathbb{F}_2[x]$ справедливо разложение

$$f(x) = x^{11}+x^9+x^8+x^4+x^3+x^2+1 = \\ \left(x^2+x+1\right)\left(x^3+x+1\right)\left(x^6+x^5+x^3+x^2+1\right).$$

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

1. Найдём разложение многочлена $f(x)$ на *неприводимые* множители над $\mathbb{F}_3$.

- Ищем корни: $f(0) = 2,\ f(1) = 1,\ f(2) = 0$. Поскольку $x - 2 \equiv_3 x + 1$, то $f(x) = (x+1)\big(x^2 + 2x + 2\big)$.
- Многочлен $g(x) = x^2 + 2x + 2$ не имеет корней в $\mathbb{F}_3$, его степень 2, т. е. он неприводим.
- Окончательно: $f(x) = (x+1)\big(x^2 + 2x + 2\big)$.

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 $\mathbb{F}_3[x]/\big(x^2+2x+2\big)$ 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 $\mathbb{F}_3[x]/\big(x^2+2x+2\big)$ 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 $\mathbb{F}_3[x]/\big(x^2+2x+2\big) = GF(3^2)$.

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

$$\beta \in \{\,0,\, 1,\, \alpha,\, \ldots,\, \alpha^{14}\,\} = F, \quad x^4 = x+1.$$

$\beta = 0$: $m_0(x) = x$.

$\beta = 1$: $m_1(x) = x+1$.

$\beta = \alpha$: сопряжённые с α элементы — α^2, α^4, α^8 и

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = \ldots$$
$$\ldots = x^4+x+1 = 0.$$

Это означает, что x^4+x+1 — примитивный многочлен и $m_\alpha(x) = x^4+x+1$.

$\beta = \alpha^3$: сопряжённые с α^3 элементы суть α^6, α^{12}, $\alpha^{24} = \alpha^9$, их м. м. —

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) =$$
$$= x^4 + \big(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\big)\,x^3 +$$

$$+\left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2+$$
$$+\left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x+$$
$$+\left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right) = x^4+\big(\alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha)+$$
$$+(\alpha^3+\alpha^2+\alpha+1)\big)x^3+(\ldots)x^2+(\ldots)x+\alpha^{30} =$$
$$= x^4+x^3+x^2+x+1.$$

$\beta = \alpha^5$: единственный сопряжённый с α^5 элемент — α^{10} (т. к. $\alpha^{20}=\alpha^5$), их м. м. —

$$m_{\alpha^5}(x) = (x-\alpha^5)(x-\alpha^{10}) = x^2+x+1.$$

$\beta=\alpha^7$: сопряжённые с α^7 элементы — α^{14}, $\alpha^{28}=\alpha^{13}$, $\alpha^{56}=\alpha^{11}$, их м. м. —

$$m_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) =$$
$$= x^4+x^3+1.$$

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

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

1. Любой многочлен в поле характеристики 5 вместе с корнем α^3 имеет корнями и все сопряжённые с ним элементы $(\alpha^3)^5=\alpha^{15}$, $(\alpha^3)^{5^2}=\alpha^{75}$, $(\alpha^3)^{5^3}=\alpha^{375}$ и т. д.

2. В поле F имеем $\alpha^{5^2-1}=\alpha^{24}=1$, и сопряжённым с α^3 будет только элемент α^{15}, т. к. $\alpha^{75}=\alpha^3$. Поэтому минимальный многочлен элемента α^3 — квадратный:

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2-(\alpha^3+\alpha^{15})x+\alpha^{18}.$$

3. Найдём коэффициенты данного многочлена, учитывая $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = \\ &= 4(4\alpha+3) + 3\alpha = 4\alpha + 2, \\ \alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = \\ &= 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\ &= 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3, \\ \alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\ \alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\ &= 4(4\alpha+3) + 4\alpha + 1 = 3.\end{aligned}$$

Ответ: $m(x) = x^2 + 3$.

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

1. По одной формуле

$$\sum_{d|6} d \cdot I_2^d = 1 \cdot I_2^1 + 2 \cdot I_2^2 + 3 \cdot I_2^3 + 3 \cdot I_2^6 = 2^6 = 64.$$

Поскольку $I_2^1 = I_2^3 = 2$ и $I_2^2 = 1$, то

$$(64 - (2+2+6)/6) = 54/6 = 9.$$

2. По другой формуле

$$I_2^6 = \frac{1}{6}\sum_{d|6} \mu(d) \cdot 2^{\frac{6}{d}} =$$

$$= \frac{1}{6}\left[\,\mu(1)\cdot 2^6 + \mu(2)\cdot 2^3 + \mu(3)\cdot 2^2 + \mu(6)\cdot 2^1\,\right] =$$

$$= \frac{1}{6}\left[\,64 - 8 - 4 + 2\,\right] = 54/6 = 9.$$

2.32. Примитивен ли элемент x в полях

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

1) Поскольку $|F_1^*| = 2^3-1 = 7$ — простое число, то каждый неединичный элемент мультипликативной группы F^* — её генератор, в т. ч. и x. Это означает, что x — *примитивный элемент* поля F и м.м. многочлен $a(x)$ примитивен.
2) Поскольку $|F_2^*| = 2^4-1 = 15 = 3\cdot 5$, то для определения значения $\operatorname{ord} x$ нужно проверить на равенства $x^3 = 1$ и $x^5 = 1$.

   Первое равенство явно не имеет места, поэтому вычисляем с учётом $x^4 = x^3+x^2+x+1$:

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

   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 $x^3+3x^2+4x+4 = (x-3)\cdot\bigl(x^2+x+2\bigr)$.

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:

$$x^5 \;=\; \left(x^2\right)^2 x \;=\; x(4x+3)^2 \;=\; x\left(x^2+4x+4\right) \;=\\ =\; x(4x+3+4x+4) \;=\; x(3x+2) \;=\; 3x^2+2x \;=\\ =\; 2x+4+2x \;=\; 4x+4.$$

Ответ: $\{\, 3,\, x,\, 4x+4 \,\}$.

2.34. Является ли многочлен

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

примитивным?

Подстановкой в $f(x)$ всех элементов $0,\,\ldots,\,4$ поля $\mathbb{F}_5$ убеждаемся, что данный многочлен 2-й степени не имеет линейных делителей и, следовательно, *неприводим*.

Порядок мультипликативной группы $GF(5^2)$ есть $24 = 2^3 \cdot 3$. Определим порядок элемента её x, для которого $x^2 = -x-2 = 4x+3$.

Поскольку простые делители 24 суть 2 и 3, проверим равенство $x^d = 1$ для $d = 24/2 = 12$, $24/3 = 8$. Вычисляем:

$$x^4 = \left(x^2\right)^2 \;=\; (4x+3)^2 \;=\; x^2+4x+4 \;=\; \ldots\\ \ldots \;=\; 3x+2 \;\neq\; 1,$$

$$x^8 = \left(x^4\right)^2 \;=\; (3x+2)^2 \;=\; -x^2+2x+4 \;=\; \ldots\\ \ldots \;=\; 3x+1 \neq\; 1.$$

$$x^{12} = x^8x^4 \;=\; (3x+1)(3x+2) \;=\; -x^2+4x+2 \;=\; \ldots\\ \ldots \;=\; 4 \neq\; 1.$$

Следовательно $\operatorname{ord} x = 24$ и рассматриваемый многочлен *примитивен* в поле $\mathbb{F}_5[x]/\big(x^2+x+2\big)$.

2.35. Для бинома $x^{40}-1 \in \mathbb{F}_5[x]$ определить количество и степени неприводимых сомножителей.

В каком минимальном поле расширения $\mathbb{F}_5[x]$ данный бином раскладывается на линейные множители?

Поскольку $n = 40 = 5 \cdot 8$, то корни бинома $x^{40} - 1$ суть все корни $x^8 - 1$ (они все различны), но 5-й кратности.

Рассмотрим разложение многочлена x^8-1 над $\mathbb{F}_5$. Относительно умножения на 5 вычеты по модулю 8 $\{\,\overline{0},\,\overline{1},\,\ldots,\,\overline{7}\,\}$ разбиваются на орбиты:

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

Пояснение: $5 \cdot 5 = 25 \equiv_8 1$, $2 \cdot 5 = 10 \equiv_8 2$ и т. д.

Поэтому:

- бином $x^8-1 \in \mathbb{F}_5[x]$ разлагается в произведение четырёх линейных и двух неприводимых квадратных многочленов;
- бином $x^{40} - 1 = \bigl(x^8 - 1\bigr)^5$ 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):

$$\begin{aligned}
x^8-1 &= \left(x^4-1\right)\left(x^4+1\right),\\
x^4-1 &= \left(x^2-1\right)\left(x^2+1\right),\\
x^2-1 &= (x-1)(x+1),\\
x^2+1 &\equiv_5 x^2-4 = (x-2)(x+2),\\
x^4+1 &\equiv_5 x^4-4 = \left(x^2-2\right)\left(x^2+2\right).
\end{aligned}$$

$$\text{Итого в } \mathbb{F}_5[x]:$$

$$x^8-1 = (x+1)(x-1)(x+2)(x-2)\cdot$$
$$\cdot\left(x^2+2\right)\left(x^2-2\right).$$

И далее

$$x^{40}-1 = (x+1)^5(x-1)^5(x+2)^5(x-2)^5\cdot \\ \cdot\left(x^2+2\right)^5\left(x^2-2\right)^5.$$

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

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

$\deg f(x)=2$ и поэтому $f(x)$ имеет 2 корня.

(1) Полином $f(x)$ неприводим над $\mathbb{F}_2$ $\Rightarrow$ его корни суть x и x^2.

(2) Полином $f(x)$ приводим над $\mathbb{F}_3$:

$$x^2+x+1 = x^2-2x+1 = (x-1)^2,$$

поэтому $f(x)$ над $\mathbb{F}_3$ имеет корень 1 степени 2.

(3) Полином $f(x)$ неприводим над $\mathbb{F}_5$ $\Rightarrow$ его корни x и x^5.

2.37. Найти корни многочлена

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

Вычисляем значения $f(x)$ для всех x из $\mathbb{F}_5 = \{\,0,\,1,\,2,\,3,\,4\,\}$: $f(0) = 4$, $f(1) = 1$, $f(2) = 0$ и, таким образом, $x = 2$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x - 2 = x + 3$, получим $2x^4 + x^3 + 4x^2 + 4 = (x+3)\cdot(2x^3+4x+3)$.

Для удобства нормируем частное $2x^3+4x+3$: т. к. $2^{-1} = 3$, то вместо корней многочлена $2x^3 + 4x + 3$ будем искать корни

$$f_2(x) \,=\, 3\cdot(2x^3+4x+3) \,=\, x^3+2x+4.$$

Перебором элементов $x \in \mathbb{F}_5$ —

$$f(0) \,=\, 4,\ f(1) \,=\, 2,\ f(2) \,=\, 1,\ f(3) \,=\, 2,\ f(4) \,=\, 1,$$

убеждаемся, что $f_2(x) = x^3 + 2x + 4$ — неприводимый многочлен[2)].

В поле $\mathbb{F}_5[x]/\bigl(x^3+2x+4\bigr)$ корнями многочлена $f_2(x) = 0$ будут $x,\ x^5,\ x^{25}$.

Вычисляем — с учётом $x^3 = -2x - 4 = 3x + 1$:

$$\begin{aligned} x^5 \,&=\, x^2(3x+1) \,=\, 3x^3+x^2 \,=\, 4x+3+x^2 \,= \\ &=\, x^2+4x+3; \\ x^{25} \,&=\, \bigl(x^5\bigr)^5 \,=\, \bigl(x^2+4x+3\bigr)^5 \,=\, x^{10}+4^5x^5+3^5 \,= \\ &=\, x^{10}+4\left(x^2+4x+3\right)+3 \,=\, x^{10}+4x^2+x. \end{aligned}$$

(поскольку $4^5 = 2^{10} = 102\underline{4}$ и $3^5 = 81\cdot 3 = 24\underline{3}$).

Найдём отдельно x^{10}:

$$x^{10} \,=\, \bigl(x^5\bigr)^2 \,=\, \bigl(x^2+4x+3\bigr)^2 \,=$$

---

2) а если бы это был многочлен 4-й степени?

$$= x^4 + x^2 + 3^2 + 3x^3 + 4x + x^2 =$$
$$= x^4 + 3x^3 + 2x^2 + 4x + 4 =$$
$$= \cancel{3}x^2 + \cancel{x} + \cancel{4}x + 3 + \cancel{2}x^2 + 4x + 4 = 4x + 2.$$

Продолжаем:

$$x^{25} = x^{10} + 4x^2 + x = \cancel{4}x + 2 + 4x^2 + \cancel{x} = 4x^2 + 2.$$

Ответ: уравнение $f(x) = 2x^4 + x^3 + 4x^2 + 4 = 0$, где $f(x) \in \mathbb{F}_5[x]$ имеет корни 2, x, $x^2 + 4x + 3$, $4x^2 + 2$ в поле $F = \mathbb{F}_5[x]/\big(x^3 + 2x + 4\big)$ (поскольку корень $2 \in F$).

2.38. Найти корни многочлена

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

В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{\big(x^4 + x^3 + 1\big)}_{f_1(x)}\underbrace{\big(x^4 + x^3 + x^2 + x + 1\big)}_{f_2(x)}.$$

Уравнения $f_1(x) = 0$ и $f_2(x) = 0$ ранее были решены: их корни соответственно суть

x, x^2, $x^3 + 1$, $x^3 + x^2 + x$

в поле $F_1 = \mathbb{F}_2[x]/\big(x^4 + x^3 + 1\big)$

и x, x^2, x^3, $x^3 + x^2 + x + 1$

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

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:

$$\begin{aligned} x &\mapsto x + 1, \\ x^2 &\mapsto (x + 1)^2 = x^2 + 1, \\ x^3 &\mapsto (x + 1)^3 = x^3 + x^2 + x + 1, \\ x^3 + x^2 + x + 1 &\mapsto \big(x^3 + x^2 + x + 1\big) + \big(x^2 + 1\big) + \\ &\quad + (x + 1) + 1 = x^3. \end{aligned}$$

Проверим, что, например, $x^2 + 1$ — корень $f(x)$:

$$\begin{aligned} f\left(x^2 + 1\right) \;&=\; \left(x^2 + 1\right)^8 + \left(x^2 + 1\right)^4 + \left(x^2 + 1\right)^2 + \\ &\quad + \left(x^2 + 1\right) + 1 \;= \\ &=\; \left(x^{16} + 1\right) + \left(x^8 + 1\right) + \left(x^4 + 1\right) + x^2. \end{aligned}$$

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 $\mathbb{F}_3[x]/\big(x^4+2x+2\big)$.

В нём $f(x)=x^4+2x+2=0$, то есть $x^4=x+1=0$, и корни $f(x)$ суть x, x^3, x^{3^2}, x^{3^3}.

Вычислим x^9 и x^{27}:

$$\begin{aligned} x^9 &= \big(x^4\big)^2 x = (x+1)^2 x = x^3+2x^2+x; \\ x^{27} &= \big(x^9\big)^3 = \big(x^3+2x^2+x\big)^3 = x^9+2x^6+x^3 = \\ &= \ldots = x^3+x^2+x. \end{aligned}$$

Ответ: полином $f(x)=x^4+2x+2$ имеет корни x, x^3, x^3+2x^2+x, x^3+x^2+x в поле $\mathbb{F}_3[x]/(f)$.

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

Поскольку $f(0)=f(1)=1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

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

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\big(x^5+x^2+1\big)$. В нём $f(x)=x^5+x^2+1=0$, 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}:

$$\begin{aligned} x^8 &= x^5x^3 = \big(x^2+1\big)x^3 = x^5+x^3 = x^3+x^2+1; \\ x^{16} &= \big(x^8\big)^2 = \big(x^3+x^2+1\big)^2 = x^6+x^4+1 = \\ &= x^5x+x^4+1 = (x^3+x)+x^4+1 = \\ &= x^4+x^3+x+1. \end{aligned}$$

Ответ: в поле $\mathbb{F}_2[x]/\big(x^5+x^2+1\big)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

имеет корни x, x^2, x^4, $x^3 + x^2 + 1$, $x^4 + x^3 + x + 1$.

3. Коды, исправляющие ошибки

3.1. Построить порождающую G и проверочную H матрицы для

1. тривиального кода утраивания;
2. кода проверки на чётность.

1. Код утраивания является линейным $(3, 1)$-кодом, у которого

$$G_{3,1} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \; I_1 = \begin{bmatrix} 1 \end{bmatrix}, \; P_{2,1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; H_{2,3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

2. Код проверки задаётся порождающей матрицей

$$G = \begin{bmatrix} I \\ 1 \dots 1 \end{bmatrix} = \begin{bmatrix} 10 \dots 0 \\ 01 \dots 0 \\ 00 \dots 1 \\ 11 \dots 1 \end{bmatrix}$$

или проверочной матрицей

$$H = \begin{bmatrix} 1 \dots 1 \; I \end{bmatrix} = \begin{bmatrix} 11 \dots 1 \end{bmatrix}.$$

3.2. Для кода Хемминга, заданного своей проверочной матрицей

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

требуется

1) построить порождающую матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;
2) найти такое кодирование для сообщений
$$\boldsymbol{u}_1 = [\,1\;1\;0\;1\,]^T,\ \boldsymbol{u}_2 = [\,1\;0\;0\;1\,]^T.$$

Проверочная матрица H имеет размерность 3×7, и код при длине $n = 7$ содержит $m = 3$ проверочных и $k = 7 - 3 = 4$ информационных бит.

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_4 \end{bmatrix}$.

Матрицу P можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, преобразуя *строки*:

$$\begin{bmatrix} 0&0&1&0&1&1&1\\ 0&1&0&1&1&1&0\\ 1&0&1&1&1&0&0 \end{bmatrix} \xrightarrow{(1)\leftrightarrow(3)} \begin{bmatrix} 1&0&1&1&1&0&0\\ 0&1&0&1&1&1&0\\ 0&0&1&0&1&1&1 \end{bmatrix} \to$$
$$\xrightarrow{(1)+(3)\mapsto(1)} \begin{bmatrix} 1&0&0&1&0&1&1\\ 0&1&0&1&1&1&0\\ 0&0&1&0&1&1&1 \end{bmatrix}$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование.

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

3.3. Циклический $(9,3)$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние d, а также осуществить систематическое кодирование полинома

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

Для определения кодового расстояния найдём все кодовые слова:

$$\begin{aligned} v(x) &= g(x)(ax^2+bx+c) = \\ &= \left(x^6+x^3+1\right)\left(ax^2+bx+c\right) = \\ &= ax^8+bx^7+cx^6+ax^5+bx^4+cx^3+ax^2+bx+c. \end{aligned}$$

В векторном виде все кодовые слова представляются как

$$[\,a,\,b,\,c,\,a,\,b,\,c,\,a,\,b,\,c\,].$$

Очевидно, это тривиальный код трёхкратного повторения и $d=3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$u(x) \mapsto v(x) = x^6u(x) + r(x).$$

1) Вычисляем $x^6u(x) = x^6\left(x^2+x\right) = x^8+x^7$.

2) Находим остаток $r(x)$ от деления $x^6u(x)$ на $g(x)$:

$$\begin{array}{r|l} x^8 + x^7 \qquad\qquad\qquad\qquad & x^6+x^3+1 \\ \cline{2-2} x^8 \qquad + x^5 \qquad\quad + x^2 \quad & x^2+x \\ \cline{1-1} x^7 + x^5 \qquad + x^2 \quad & \\ x^7 \qquad + x^4 \qquad + x & \\ \cline{1-1} x^5 + x^4 + x^2 + x & \end{array}$$

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. 198):

Находим позицию j ошибки.

1. $x^6 + x^2 + x = \left(x^3 + x + 1\right)^2 + \underbrace{x + 1}, \; j = 3.$

Действительно,

$$w(\alpha) = \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1.$$

2. $x^6 + x^5 + x^3 + x^2 + x =$
$= \left(x^3 + x^2 + x + 1\right)\left(x^3 + x + 1\right) +$
$+ \underbrace{x^2 + x + 1}, \; j = 5;$

Действительно,

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

3. $x^6 + x^3 + x^2 + x = \left(x^3 + x\right)\left(x^3 + x + 1\right) + \underbrace{0},$
т. е. ошибки не произошло.

3.5. Имеем $\alpha^{31} = 1$ и разложение F^* над $\mathbb{F}_2$ есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8\, \alpha^{16}\},$$
$$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}, \{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\},$$
$$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}, \{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\},$$
$$\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}.$$

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

Будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов данного поля со с. 48.

С её помощью вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\
&\quad = (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\
&\quad = \alpha^3 + \alpha + 1 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \big(w(\alpha^2)\big)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1.$$

Решим соотношение Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \quad \deg \lambda(x) \leqslant 2.$$

с помощью обобщённого алгоритма Евклида:

$$\begin{aligned}\text{Шаг 0.}\quad & r_{-2}(x) \,=\, x^5,\\ & r_{-1}(x) \,=\, s(x),\\ & \sigma_{-2}(x) \,=\, 0,\\ & \sigma_{-1}(x) \,=\, 1.\end{aligned}$$

$$\begin{aligned}\text{Шаг 1.}\quad & r_{-2}(x) \,=\, r_{-1}(x)q_0(x) + r_0(x),\\ & q_0(x) \,=\, \alpha^2 x,\\ & r_0(x) \,=\, s(x),\\ & \sigma_0(x) \,=\, -q_0(x) \,=\, \alpha^2 x.\end{aligned}$$

$$\begin{aligned}\text{Шаг 2.}\quad & r_{-1}(x) \,=\, r_0(x)q_1(x) + r_1(x),\\ & q_1(x) \,=\, \alpha^{12}x + \alpha^5,\\ & r_1(x) \,=\, \alpha^{14}x^2 + 1,\\ & \quad \deg r_1(x) = 2 \leqslant r,\\ & \sigma_1(x) \,=\, \sigma_{-1}(x) - \sigma_0(x)q_1(x) \,=\\ & \qquad\quad = 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) \,=\\ & \qquad\quad = \underbrace{\alpha^{14}x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} \,=\, \sigma(x).\end{aligned}$$

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

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок есть

$$\sigma(x) \,=\, \alpha^2 x^2 + \alpha^6 x + 1.$$

Требуется определить *позиции ошибок* в $w(x)$.

Найдём корни (их 2, полином квадратный) полинома локаторов ошибок полным перебором.

Для вычислений удобно пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной в предыдущей задаче.

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3,\\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = \mathbf{0},\\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^7) &= \alpha^{16} + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\
\sigma(\alpha^8) &= \alpha^{18} + \alpha^{14} + 1 = \mathbf{0}.
\end{aligned}$$

Дальше можно не вычислять: оба корня $\sigma(x)$ найдены. Итак, данный полином локаторов ошибок имеет корни α^5 и α^8. Определяем позиции ошибок:

$$\text{-}5 \equiv_{15} 10, \qquad \text{-}8 \equiv_{15} 7.$$

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

Имеем $n = 31 = 2^5 - 1$, $t = 5$, $\delta - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни α, α^2, α^3, α^4, α^5, α^6, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $C_1 = \{\, \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16} \,\}$.

При решении задачи 3.5 на с. 229 о разложение F^* на классы было установлено, что эти классы также будут пятиэлементными:

$$C_2 = \{\, \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17} \,\};$$
$$C_3 = \{\, \alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18} \,\}.$$

На с. 37 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 —

$$\left(x^5+x^4+x^3+x+1\right)\Big|_{x=\alpha^5} = \alpha^{25}+\alpha^{20}+\alpha^{15}+\alpha^5+1 = \\ = (\alpha^3+1)^5+(\alpha^3+1)^4+(\alpha^3+1)^3+\alpha^5+1 = \ldots = 0.$$

Таким образом,

$g_2(x) = x^5+x^3+x^2+x+1$, $g_{\alpha^5}(x) = x^5+x^4+x^3+x+1$

[3)] например, [8], Том 1, Таблица C.

и порождающий многочлен для $(31, 16, 7)$-кода БЧХ есть

$$\begin{gathered} g(x) \;=\; g_1(x)\cdot g_2(x)\cdot g_3(x) \;= \\ =\; x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1, \\ \deg g(x) = m = 15,\; k = n-m = 16. \end{gathered}$$

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

Пусть для некоторого принятого слова найден полином локаторов ошибок: $\sigma(x) = \alpha^6 x + \alpha^{15}$. Определить позиции ошибок в данном слове.

Для вычислений в поле F нам понадобится таблица, уже построенная на с. 48.

Перебором найдём корни полинома ошибок

$$\sigma(x) \;=\; \alpha^6 x + \alpha^{15} \;=\; (\alpha^3+\alpha^2)\, x + 1 :$$

$$\begin{aligned} \sigma(\alpha) \;&=\; \alpha^4+\alpha^3+1 \;=\; \alpha+1+\alpha^3 \;\neq\; 0; \\ \sigma(\alpha^2) \;&=\; \alpha^5+\alpha^4+1 \;=\; \alpha^2+\alpha+\alpha+1+1 \;=\; \alpha^2 \;\neq\; 0; \\ &\ldots\ldots \\ \sigma(\alpha^9) \;&=\; \alpha^{12}+\alpha^{11}+1 \;= \\ &=\; (\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+1 \;=\; \mathbf{0}. \end{aligned}$$

Линейный полином $\sigma(x)$ имеет один корень α^9, и поэтому позиция единственной ошибки есть -9 $\equiv_{15}$ 6.

4. Алгебраические основы криптографии

4.1. 1. Решить комбинаторную задачу.

Пусть p — простое число, большее 2. Сколько существует способов C раскрасить вершины правильного p-угольника в a цветов, если раскраски, получающиеся совмещением при вращении многоугольника вокруг своего центра, считать одинаковыми?

2. На основе полученного решения доказать малую теорему Ферма.

Теорема 4.17 (Ферма, малая). *Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.*

1. Если не отождествлять раскраски указанного типа, то всех раскрасок a^p.

Исключим одноцветные раскраски, остальных — $a^p - a$. Вращение раскрашенного более, чем в один цвет p-угольника вокруг своего центра на p углов $\frac{2\pi}{p}$, $2\frac{2\pi}{p}$, …, 2π даст неразличимые раскраски.

Итого, число различных раскрасок в более, чем один цвет равно $\frac{a^p-a}{p}$, и тогда всех раскрасок —

$$C = \frac{a^p - a}{p} + a = \frac{a\left(a^{p-1} - 1\right)}{p} + a.$$

2. Если $p = 2$, то a нечётно и утверждение теоремы тривиально.

Иначе показано, что C — целое число, откуда при $a \not\vdots\, p$ должно выполняться $(a^{p-1} - 1) \vdots\, p$, т. е. $a^{p-1} \equiv_p 1$.

4.2. 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:

$$\begin{array}{r|rr|ll}
1 & 72 & 0 & & \\
2 & 29 & 1 & q = 2 & (\ 58\ 2\ ) \\
\hline
3 & 14 & -2 & q = 2 & (\ 28\ \ -4\ ) \\
4 & 1 & \mathbf{5} & q = 14 & \\
5 & 0 & & &
\end{array}$$

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

$$d \cdot 11 = 1 \pmod{12}.$$

$$\begin{array}{c|cc|l} 1 & 12 & 0 & \\ 2 & 11 & 1 & q=1 \\ \hline 3 & 1 & \mathbf{-1} & q=11 \\ 4 & 0 & & \end{array}$$

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. 150).

(а) $\underline{6^x \equiv_{11} 2}$. Имеем $p = 11$, $a = 6$, $b = 2$.

1. $H = \lceil \sqrt{11} \rceil = 4$.
2. $6^4 = 1\,296 \equiv_{11} 9 = c$ $(1296 = 117 \cdot 11 + 9)$.

3. $u = 1, 2, 3, 4$

u	1	2	3	4
9^u	9	$9 \cdot 9 = 81$	$4 \cdot 9 = 36$	$3 \cdot 9 = 27$
$9^u \pmod{11}$	9	4	3	5

4. $v = 0, \ldots, 4$

v	0	1	2	3	4
6^v	1	6	36	216	1296
$2 \cdot 6^v$	2	12	72	432	2592
$2 \cdot 6^v \pmod{11}$	9	1	6	3	7

5. Совпал элемент 3 таблиц при $u = 3$ и $v = 3$. Отсюда $Hu - v = 4 \cdot 3 - 3 \equiv_{10} 9$.

Ответ: $x = 9$.

(б) $\underline{8^x \equiv_{11} 3}$. Имеем $p = 11$, $a = 8$, $b = 3$.

1. $H = 4$.

2. $8^4 = 4\,096 \equiv_{11} 4 = c$.

u	1	2	3	4
3. 4^u	4	$4 \cdot 4 = 16$	$5 \cdot 4 = 20$	$9 \cdot 4 = 36$
$4^u \pmod{11}$	4	5	9	3

4.

v	0	1	2	3	4
8^v	1	8	64	512	4096
$3 \cdot 8^v$	3				
$3 \cdot 8^v \pmod{11}$	3				

5. Совпал элемент 4 таблиц при $u = 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 4 = 16 \equiv_{10} 6$.

Ответ: $x = 6$.

(в) $\underline{2^x \equiv_{13} 3}$. Имеем $p = 13$, $a = 2$, $b = 3$.

1. $H = 4$.
2. $2^4 = 16 \equiv_{13} 3 = c$.
3. Таблица:

u	1	2	3	4
c^u	3	9	27	3
$c^u \pmod{13}$	**3**	9	1	3

4. Таблица:

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. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. — М.: КомКнига, 2006.
4. *Введение* в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.
5. *Вернер М.* Основы кодирования. Учебник для ВУЗов. — М: Техносфера, 2004.
6. *Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н.* Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.
7. *Касами Т., Токура Н., Ивадари Ё., Инагаки Я.* Теория кодирования. — М.: Мир, 1978.
8. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. — М.: Мир, 1988.

9. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.

10. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

11. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.

12. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.