**Конспект лекций по курсу**

# ПРИКЛАДНАЯ АЛГЕБРА

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

Лектор *С. И. Гуров*

ассистент *Д. А. Кропотов*

(кафедра *Математических методов прогнозирования*)

2018

*Вся моя работа должна была свестись к поискам благородной простоты, свободе от показного нагромождения 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.*

*К. В. Глюк.* Предисловие
к опере «Альцеста».

# Предисловие

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

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

конспекте некоторый материал, обычно неиспользуемый непосредственно на лекциях, но полезный при самостоятельной проработке материала.

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

Глава 3 написана совместно с Д. А. Кропотовым.

# Оглавление

# Глава 1

# Группы, кольца, поля (компендиум)

## 1.1 Группы

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

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

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

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

3) $\forall\, x\ \exists !\, y : \ y \circ x = x \circ y = e$ — *существование обратного элемента* к $x$.

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

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

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:

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

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

*Пример* 1.1. Таблица умножения группы $V_4$.

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

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

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

*Пример* 1.2. 1. Четверная группа Клейна абелева.

2. *Числовые группы* — все они абелевы:

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

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

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

Перестановки можно записывать в виде:

а) таблицы —

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

б) разложения на циклы —

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

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

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

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

Каноническое представление цикла $(t_1 t_2 \ldots t_k)$:
$t_1$ — наименьшее из чисел $\{t_1, t_2, \ldots, t_k\}$.
*Например*, для композиции перестановок:

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

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

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

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

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

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

$t$ — вращение на $120^\circ$ вокруг центра в выбранном направлении (по или против часовой стрелки),

$r$ — осевая симметрия относительно выбранной оси.

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

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

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

$t$ — вращение на $90^\circ$ вокруг центра в выбранном направлении,

$r$ — симметрия относительно некоторой оси, проходящей через центры противоположных сторон,

$f$ — симметрия относительно некоторой оси, проходящей противоположные вершины.

Легко видеть, что $|D_n| = 2n$.

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

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

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

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

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

$$H \leqslant G,\ x \in G \ \Rightarrow xH = \{\, xh \mid h \in H \,\},$$
$$Hx = \{\, hx \mid h \in H \,\}.$$

Утверждение 1.1 (*о смежных классах*). *Левые смежные классы с разными представителями либо не пересекаются, либо совпадают и вместе составляют всю группу.*

*То же справедливо и для правых смежных классов.*

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

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

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

называется *факторгруппой*, символически $G/H$.

Легко видеть, что результат $x \circ y$ находится в $abH$ независимо от выбора элементов $x \in aH$ и $y \in bH$.

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

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

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

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

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

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

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

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

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

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

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

Для циклических групп возможны два случая.

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

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

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

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

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

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

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

В рассматриваемом случае получаем конечную группу

$$\mathbb{Z}_n \;=\; \langle\, \{0, 1, \ldots, n-1\},\, +_{\bmod n},\, 0 \,\rangle\,,\; n = \operatorname{ord} a$$

(подробнее см. далее).

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

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

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

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

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

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

*Свойства функции Эйлера* ($p$ — простое):

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

*Иллюстрация свойств:*

$$\varphi(12) = \varphi(2^2 \cdot 3) = 2^1 \cdot 1 \cdot 2 = 4,$$
$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8,$$
$$\varphi(16) = \varphi(2^4) = 2^3 \cdot 1 = 8,$$
$$n = 12, D(12) = \{1, 2, 3, 4, 6, 12\},$$
$$\underbrace{\varphi(1)}_{=1} + \underbrace{\varphi(2)}_{=1} + \underbrace{\varphi(3)}_{=2} + \underbrace{\varphi(4)}_{=2} + \underbrace{\varphi(6)}_{=2} + \underbrace{\varphi(12)}_{=4} = 12.$$

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

Рис. 1.1. Первые 99 значений функции Эйлера

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

## Теорема Лагранжа и следствия из неё

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

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

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

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

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

## 1.2 Кольца и поля

### Кольца: определение, основные свойства

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

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

- Обычно рассматривают *ассоциативные кольца* с ассоциативной операцией умножения.
- Важный случай — *коммутативные кольца* с коммутативной операцией умножения.
- Если в кольце имеется единичный элемент 1 по умножению ($x \cdot 1 = 1 \cdot x = x$), то кольцо называется *кольцом с единицей* или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$.
- *Тривиальное кольцо* — $\{0\}$, в нём и только в нём $0 = 1$.

- Кольцо $R$ — *без делителей нуля*, если для любых $a, b \in R$ из $a \cdot b = 0$ следует $a = 0$ или $b = 0$.

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

*Пример* 1.3. 1. Классический пример кольца — кольцо целых чисел $\mathbb{Z}$ с обычными операциями сложения и умножения. Это кольцо целостно и имеет два обратимых элемента: $+1$ и $-1$.

2. Кольцо чётных $2\mathbb{Z}$ — кольцо без единицы.

3. $\mathbb{Z}_n$ — *кольцо классов вычетов*[1)] *по модулю* $n$, результаты операций $(+)$ и $(\cdot)$ по $\bmod\ n$.

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

   Класс вычетов числа $a$ по модулю $n$ — множество всех целых чисел, сравнимых с $a$ по модулю $n$, символически $[a]$ или $\overline{a}$ (число $n$ считается заданным):

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

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

[1)] вычет (лат. residum) — остаток

Сложение и умножение классов вычетов определяется формулами

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

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

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

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

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

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

(ясно, что тогда и элемент $b$ обратим).

Например, в кольце $Z_6$ обратимы элементы 1 и 5: $1 \cdot 1 = 5 \cdot 5 = 1$. Если $p$ — простое число, то все ненулевые элементы кольца $\mathbb{Z}_p$ обратимы: например, в $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$: $1 \cdot 1 = 1$, $2 \cdot 3 \equiv_5 1$, $4 \cdot 4 \equiv_5 1$.

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

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

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

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

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

## Идеалы колец и факторкóльца

*Определение* 1.10. Подкольцо $I$ коммутативного[3] кольца $\langle R, +, \cdot, 0 \rangle$ называется его *(двусторонним) идеалом*, символически $I \lhd R$, если оно устойчиво относительно относительно умножения на элементы $R$, т. е. для любых $i \in I$ и $r \in R$ справедливо $i \cdot r \in I$.

Пример идеала в кольце целых: все чётные числа.

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

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

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

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

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

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

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

Примеры КГИ:

- кольцо целых $\mathbb{Z}$ — все его идеалы имеют вид $(n) = n\mathbb{Z} = \{ 0, \pm n, \pm 2n, \dots \}$.
- кольцо $\mathbb{Z}_n$ — так как вместе с любыми элементами идеал всегда содержит их НОД.
  Например, для $\mathbb{Z}_6$: $(0) = 0$, $(1) = (5) = \mathbb{Z}_6$, $(2) = (4) = \{0, 2, 4\}$, $(3) = \{0, 3\}$.

Все КГИ факториальны.

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

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

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

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

$$a \in \overline{r} \;\Rightarrow\; \overline{a} = \overline{r}.$$

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

$$\overline{r} \;=\; \{\, r,\, r \pm n,\, r \pm 2n, \ldots\}$$

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

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

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

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

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

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

В нетривиальном коммутативном кольце всегда существует максимальный идеал.

*Пример* 1.5. В кольце $\mathbb{Z}$

- идеалы $(2)$ и $(3)$ максимальны;

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

### Евклидовы кольца

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

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

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

*Пример* 1.6.
- Классический пример евклидова кольца — *кольцо целых чисел* $\mathbb{Z}$; норма — абсолютная величина числа.
- Кольцо $\mathbb{R}[x]$ многочленов с действительными коэффициентами евклидово, норма — степень многочлена.

Все евклидовы кольца — КГИ.

### Поле

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

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

Для нас важны следующие свойства поля:

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

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

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

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

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

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

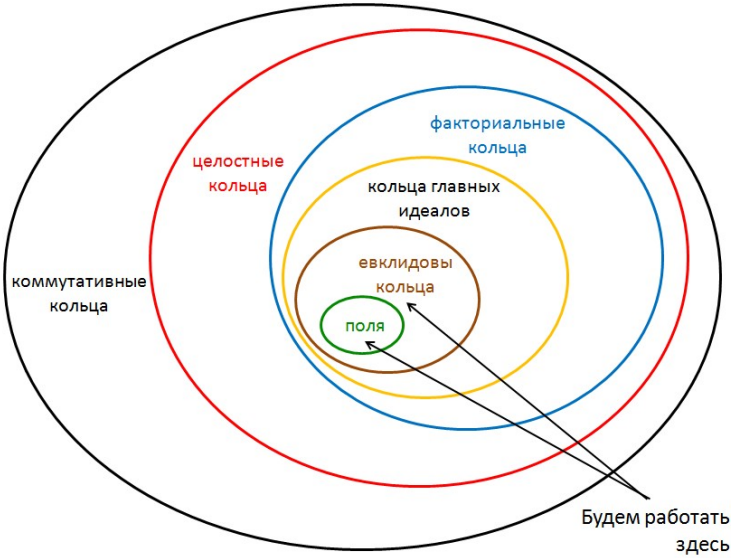


Рис. 1.2. От ассоциативных колец к полям

## 1.3 Задачи

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

1) целые числа, кратные данному натуральному числу $n$, относительно сложения?
2) неотрицательные целые числа относительно сложения?
3) нечетные целые числа относительно сложения?
4) нелые числа относительно вычитания?
5) рациональные числа относительно умножения?
6) рациональные числа, отличные от нуля, относительно умножения?
7) положительные рациональные числа относительно умножения?

8) положительные рациональные числа относительно деления?
9) корни $n$-й степени из единицы (как действительные, так и комплексные) относительно умножения?
10) матрицы порядка $n$ с действительными элементами относительно умножения?
11) невырожденные матрицы порядка $n$ с действительными элементами относительно умножения?
12) перестановки чисел $1, 2, \ldots, n$ относительно композиции перестановок?
13) преобразования множества $M$, то есть взаимнооднозначные отображения этого множества на себя, относительно композиции отображений?
14) элементы $n$-мерного векторного пространства $\mathbb{R}^n$ относительно сложения?
15) параллельные переносы трехмерного пространства $\mathbb{R}^3$ относительно композиции движений?
16) повороты трехмерного пространства $\mathbb{R}^n$ вокруг прямых, проходящих через данную точку $O$ относительно композиции движений?

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

1.3. Вычислите функцию Эйлера для:

а) 375; б) 720; в) 988.

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

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

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

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

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

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

$\varphi(r_1 + r_2) \;=\; \varphi(r_1) \oplus \varphi(r_2),\ \varphi(r_1 \cdot r_2) \;=\; \varphi(r_1) \otimes \varphi(r_2)$. Взаимно-однозначный гомоморфизм колец называется их *изоморфизмом*, символически $R \cong R'$.

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

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

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

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

# Глава 2

# Конечные кольца и поля

## 2.1 Поля Галуа

### Простые поля Галуа — поля вычетов

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

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

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

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

[1)] В честь Эвариста Галуа (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 |

| $\times$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

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

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\times$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

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

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

В конечном поле всегда найдётся первое $k$ такое, что

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

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

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

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

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

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

В конечном поле возможно сильное упрощение вычисления степеней сумм.

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

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

*Доказательство.* В любом коммутативном кольце верна формула для степени бинома

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

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

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

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

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

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

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

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

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

Попробуем их найти. Проверяем элемент 2:

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

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

| $k$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $3^k$ | 3 | 9 | 5 | 4 | 1 |

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

Как ускорить процесс?

Если примарное разложение числа $p-1$

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

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

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

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

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

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

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

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

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

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

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

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

Рис. 2.1. Деление многочленов «уголком»

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

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

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

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

В кольце многочленов над:

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

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

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

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

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

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

*Вторая степень:* $x^2 + ax + b$.

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

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

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

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

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

Проверкой устанавливаем, что оба эти варианта дают неприводимые многочлены

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

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

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

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

*Пятая степень:* $x^5+ax^4+bx^3+cx^2+dx+1$. Исключение делимости на $x+1$ приводит к условию $a+b+c+d=1$ — 8 вариантов. Далее исключая делимость на неприводимые многочлены 2 и 3-й степеней (их один и два соответственно, а их произведения дают два многочлена) находим 6 неприводимых многочленов 5-й степени:

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

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

— докажем позже.

Отметим, что для нахождения неприводимых многочленов в $\mathbb{F}_p[x]$ *нет эффективных алгоритмов.*

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

1) выбирая простое $p$, фиксируем поле $\mathbb{F}_p$ и рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над $\mathbb{F}_p$;
2) выбираем натуральное $n$ и *неприводимый многочлен* над $\mathbb{F}_p$ —
$$a(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x],\ a_n \neq 0;$$
3) идеал $(a(x))$ порождает факторкольцо $\mathbb{F}_p[x]/(a(x))$, элементы которого суть совокупности $\overline{r(x)}$ многочленов, дающих при делении на $a(x)$ остаток $r(x)$; множество всех таких остатков $\{r(x)\}$ есть совокупность всех многочленов из $\mathbb{F}_p[x]$ степеней от 0 до $n-1$.

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

Действительно, кольцо многочленов $\mathbb{F}_p[x]$ евклидово, многочлен $a(x)$ неприводим, следовательно идеал $(a(x))$ — максимальный и $\left\{\overline{r(x)}\right\}$ — поле. Данное поле обозначают $\mathbb{F}_p^n$ и называют *расширением n-й степени* простого поля $\mathbb{F}_p$.

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

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

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

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

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

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

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

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

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

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

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

и легко показать, что $\left(x^t+1\right) \not\vdots \left(x^3+x+1\right)$ ни при каком $4 \leqslant t < 7$.

Также и $\operatorname{ord} x = 7$:

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

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

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

## 2.2 Вычисления в конечных кольцах и полях

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

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

*Алгоритм Евклида EA-N*[2)]

*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;

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

3) иначе заменить пару чисел $(a, b)$ парой $(b, r)$ и перейти к шагу 1.

*Пример* 2.3. Найдём НОД $(252, 105)$ по алгоритму Евклида.

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

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

*Утверждение* 2.3 (соотношение Безу[3]). *Для любых натуральных $a$, $b$ и $d = НОД\,(a, b)$ найдутся целые коэффициенты Безу $x$, $y$ такие, что $d = ax + by$.*

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

*Замечание.* Коэффициенты Безу могут быть выбраны неоднозначно, например

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

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

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

*Обобщённый алгоритм Евклида EAA-Z*

решения соотношения $ax + by = d$, $a \geqslant b$ в кольце $\mathbb{Z}$

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

*Пример* 2.4. Обобщённым алгоритмом Евклида найдём натуральное $d$ и целые $x$ и $y$ такие, что
$$d = \text{НОД}\,(252, 105) = 252x + 105y.$$

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

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

(2) Заменяем матрицу $E$ матрицей

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

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

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

(5) Заменяем матрицу $E$ матрицей

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

(6) 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 $d = 21$.

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

*Обобщённый алгоритм Евклида Inv-Zm* нахождения в обратного к $c$ элемента в кольце $\mathbb{Z}_m$ при условии $\text{НОД}(c, m) = 1$

Шаг 0. Запишем исходные данные в виде двухстрочной таблицы

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

Шаг 1. Вычислим частное $q$ от деления друг на друга элементов первого столбца, т. е. $m$ на $c$: $m = q \cdot c + r$, $0 \leqslant r < c$.

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

Шаг 3. Проводим аналогичные действия с двумя последними строками таблицы, пока в очередной строке не получим первый элемент, равный 0. Тогда второй элемент *предпоследней* строки есть $c^{-1}$.

*Пример* 2.5. Решим в поле $\mathbb{Z}/(101)$ решить сравнение

$$4y = 1.$$

Применим алгоритм Inv-Zm, для удобства нумеруя строки и записывая значения частных и вычитаемые строки:

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

Таким образом, $y^{-1} = \text{-}25 \equiv_{101} 76$.

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

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

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

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

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

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

Для этого удобна следующая форма алгоритма.

*Обобщённый алгоритм Евклида EEA-P* нахождения в поле $\mathbb{F}_p[x]/(a(x))$ элемента $y(x)$, обратного к $b(x)$, $\deg a(x) \geqslant \deg b(x)$.

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

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

Для этого обобщённым алгоритмом Евклида решим соотношение Безу

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

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

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

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

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

## 2.3 Алгебра векторов над конечным полем

### Векторное пространство

Определение 2.1. *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* («числá») *из* $K$ *на вектор из* $V$: $K \times V \stackrel{\cdot}{\to} V$,

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

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

*Пример* 2.7. 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 векторное пространство, которое называют *$n$-мерным координатным пространством* над полем $K$. Ясно, что если $K$ — конечное поле, то $V$ содержит $|K|^n$ элементов.

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

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

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

*2. 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.

**Представление элементов конечных полей.** Поле $GF(p^n) = \mathbb{F}_p^n$, $n \in \mathbb{N}$ можно рассматривать

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

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

*Теорема* 2.3. *Базис* $\mathbb{F}_p^n$ *образуют* $n$ *элементов* $\overline{1}$, $\overline{x}$, $\ldots$, $\overline{x^{n-1}}$.

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

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

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

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

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

Приведём в качестве примера 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 $\alpha$ $\quad \alpha^4 = \alpha + 1$ | $1$ | $x$ | $x^2$ | $x^3$ |
|---|---|---|---|---|
| $\alpha$ | 0 | 1 | 0 | 0 |
| $\alpha^2$ | 0 | 0 | 1 | 0 |
| $\alpha^3$ | 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:

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

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

1) рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$ над ним;

2) в кольце $\mathbb{R}[x]$ возьмём неприводимый многочлен $x^2+1$;

3) построим поле $F$ как факторкольцо
$$F = \mathbb{R}[x]/\left(x^2+1\right);$$

4) базис $F$ как векторного пространства есть $\left\{\overline{1}, \overline{x}\right\}$ и каждый элемент $z \in F$ представим в виде $z = a\overline{1} + b\overline{x},\ a, b \in \mathbb{R}$.
Поле $F$ изоморфно полю *комплексных чисел* $\mathbb{C}$.

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

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

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

## 2.4 Корни многочленов над конечным полем

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

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

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

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

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

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

$$a_0 + a_1\overline{x} + \ldots + a_n(\overline{x})^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} = \overline{0},$$

а значит и корень $a_n^{-1}a(x)$.

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

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

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

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

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

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

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

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

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

*Утверждение* 2.5. *Минимальные многочлены неразложимы.*

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

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

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

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

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

Подставляя в это равенство $\beta$ вместо $x$, получаем

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

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

*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, т. е. эти многочлены совпадают.

**Свойства многочленов над конечным полем.**

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

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

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

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

Для $q = p^n$ имеем 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 бинома $x^{p^n-1}-1=0$, 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)* Для случая $n=1$ доказана *малая теорема Ферма: любой элемент $a \in \mathbb{F}_p$, взаимно простой с $p$, удовлетворяет сравнению*

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

*Теорема* 2.5 (о делимости биномов). *В кольце многочленов*

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

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

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

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

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

*Доказательство.*

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

$n>1$. Выбираем неприводимый нормированный многочлен $f(x)$ степени $n$ из $\mathbb{F}_p[n]$ и строим поле $\mathbb{F}_p[x]/\big(f(x)\big)$.
В нём $x$ — корень и своего м. м. $f(x)$, и, по теореме 2.4, бинома $x^{p^n-1}-1$. По свойствам м. м. (утверждение 2.6) $x^{p^n-1}-1$ делится на $f(x)$. □

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

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

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

Таким образом,

$$x^{15}+1 = \left(x^4+x+1\right)\left(x^4+x^3+1\right)\left(x^4+x^3+x^2+x+1\right)\left($$

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

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

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

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

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

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:

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

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

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

то есть $\beta$ — корень $(*)$.

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

## Корни неприводимого многочлена

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

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

Из тождества Фробениуса следует, что

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

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

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

Предположим, что $\beta^{p^l} = \beta^{p^k}$, $0 \leqslant l < k \leqslant n-1$, но тогда $\beta^{p^{k-l}} = 1$, а это значит, что при $n > 1$ среди корней $\beta$, $\beta^p$, $\beta^{p^2}$, …, $\beta^{p^{n-1}}$ находится $1 \in \mathbb{F}_p$. В свою очередь, это означает, что $f(x)$ делится на $x - 1$ (см. с. 32), т. е. многочлен $f(x)$ разложим. □

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

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

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

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

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

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

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

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

2. *Задача*: найти все корни многочлена

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

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

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

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

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

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

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 $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right) = \mathbb{F}_3^2$ 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 $\beta^p$, $\beta^{p^2}$, ..., пока на некотором шаге $d$ окажется, что

1) $\beta^{p^d} = \beta$, тогда

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

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

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

В этом поле $x^4 = x + 1$.

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

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

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

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

Вычисляем коэффициенты многочлена:

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

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

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

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

поэтому $m_\beta(x) = x^4+x+1$.

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

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

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

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

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

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

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

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

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

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

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

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

*Теорема* 2.9 (формула Гаусса).

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

*Например*:

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

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

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

## 2.5 Циклические подпространства колец вычетов

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

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

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

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

*Доказательство.* $u,v,\varphi\in\mathbb{F}_p[x]$, $k=\deg\varphi\leqslant\deg f$,

$$\varphi=a_0+a_1x+\ldots+a_{k-1}x^{k-1}+x^k,\quad f=\psi\varphi.$$

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

Во-первых,

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

И, во-вторых,

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

2. Покажем, что в $(\varphi)$ нет других, кроме

$$\varphi = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k$$

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

Пусть $g = b_0 + b_1 x + \ldots + x^m$. Тогда

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

3. Без доказательства. □

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

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

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

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

Приведём элементы этого идеала:

| $a\ b\ c$ | элементы $(\varphi)$ |
|---|---|
| 0 0 0 | $0$ |
| 0 0 1 | $x+1$ |
| 0 1 0 | $x^2+x$ |
| 0 1 1 | $x^2+1$ |
| 1 0 0 | $x^3+x^2$ |
| 1 0 1 | $x^3+x^2+x+1$ |
| 1 1 0 | $x^3+x$ |
| 1 1 1 | $x^3+1$ |

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

**Циклическое пространство.**

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

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

Циклический сдвиг координат в этом базисе равносилен умножению на $\overline{x}$:

$$\overline{a_0 + a_1 x + \ldots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}} \cdot \overline{x} = \\ = \overline{a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{=1}} = \\ = \overline{a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1}}.$$

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

*Доказательство.* Если подпространство $I$ — идеал, то оно замкнуто относительно умножения на $\overline{x}$, 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 $g \cdot \overline{x}$, $g \cdot \overline{x^2}$, ... также принадлежат $I$. Значит, $g \cdot \overline{f} \in I$ для любого многочлена $f$, поэтому $I$ — идеал. □

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

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

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

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

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

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

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

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

Поэтому $x^{15} + 1$ разлагается в произведение одного неприводимого многочлена степени 1, одного неприводимого многочлена степени 2 и трех неприводимых многочленов степени 4. Конкретно разложение было найдено ранее (см. с. 54).

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

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

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

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

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

## 2.6 Задачи

2.1. 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) $3^{-3} \pmod 8$.

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

2.3. Решите сравнение

а) $7x = 11 \pmod{25}$;

б) $9x = 3 \pmod{10}$;

в) $6x + 2 = 3 \pmod{7}$;

г) $6x + 2 = 3 \pmod{9}$;

д) $6x + 2 = 4 \pmod{9}$;

е) $6x + 1 = 4 \pmod{9}$.

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

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

где $\beta_1$, $\beta_2$, $\beta_3$ — 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

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

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

2.30. Найти минимальный многочлен элемента $\alpha^3$, где $\alpha$ — примитивный элемент поля

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

2.31. Примитивен ли элемент $x$ в полях

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

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

2.32. Найти корни многочлена

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

2.33. Является ли многочлен

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

примитивным?

2.34. 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?

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

2.36. Решить уравнение

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

2.37. Решить уравнение

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

2.38. Найти корень многочлена

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

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

# Глава 3

# Коды, исправляющие ошибки

## 3.1 Блоковое кодирование: основные понятия

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

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

*Подход к решению* (один из возможных!):

1) входной поток информации разбить на *сообщения* — последовательные непересекающиеся блоки фиксированной длины $k$;

2) каждый блок *кодировать* (модифицировать) —
   а) независимо от других — *блоковое кодирование*;
   б) в зависимости от предыдущих — *свёрточное* или *потоковое кодирование* (турбо-коды).

Далее рассматриваем только *блоковое кодирование*:

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

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

## Кодовое расстояние.

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

Ясно, что код $C$ может исправить не менее $r$ ошибок, если шары радиусов $r$ с центрами в кодовых словах непересекаются. Действительно, если в векторе $\widetilde{\alpha}$ искажено не более $r$ бит, то набор останется в шаре $S_r(\widetilde{\alpha})$ и искомое кодовое слово — центр шара, ближайший к полученному набору.

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

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

**Блоковое кодирование и декодирование**

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

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

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

*Код-повторение* $a \mapsto \underbrace{a\ldots a}_{2r+1 \text{ раз}}$, очевидно, исправит $r$ ошибок. Простейший вариант — утраивание: $0 \mapsto 000$, $1 \mapsto 111$.

Ясно, однако, что такое кодирование крайне неэффективно.

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

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

Обозначения:

- сообщение — вектор

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

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

Блоковое кодирование всегда можно осуществить с использованием таблицы размера $2^k \times n$. Однако такое «табличное» кодирование требует большой памяти: 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 тех и только тех битах, в которых произошли ошибки.

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

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

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

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

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

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

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

**Плотная упаковка шаров в единичный куб.** Чтобы построить код минимальной избыточности, исправляющий данное количество $r$ ошибок, нужно вложить в единичный куб $B^n$ максимально возможное число непересекающихся шаров радиуса $r$ — это *задача плотной упаковки*.

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

*Ответ:* Такое удаётся только в двух нетривиальных[2)] случаях, когда получаются *совершенные* или *экстремальные коды*:

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

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

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

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

Для *оценки снизу* построим негрупповой код:

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

[2)] для групповых кодов, см. ниже

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

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

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

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

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

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

Найдём кодовое расстояние построенного кода:

- в каждой строке таблицы — не менее трёх единиц;

- если сложить

  *две строки* — в левой части будет две единицы, а в правой — хотя бы одна,

  *не менее трёх строк* — в левой части будет не менее трёх единиц.

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

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 |

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

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

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

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

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

## 3.2 Линейные коды

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

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

Легко видеть, что кодовое расстояние $d$ группового кода равно

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

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

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

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

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

Отсюда получаем оценку $\min\limits_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho(\widetilde{\alpha}, \widetilde{\beta}) \geqslant \min\limits_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|$, которая достигается, например, при $\widetilde{\beta} = \widetilde{0}$.

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

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

Это означает, что в *линейном* коде $C$:

1) сумма любых кодовых слов — кодовое слово, то есть это *групповой* код;
2) кодовое расстояние $d(C) = \min\limits_{\widetilde{\gamma} \in C \setminus \{\widetilde{0}\}} \|\widetilde{\gamma}\|$;
3) существует базис $\{ \boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1} \}$ из $k$ векторов $\boldsymbol{g}_i \in B^n$, $i = 0, \ldots, k-1$, поэтому любой вектор $\boldsymbol{v} \in C$ может быть представлен как
$$\boldsymbol{v} = \sum_{i=0}^{k-1} u_i \, \boldsymbol{g}_i, \quad u_i \in \{0, 1\}.$$
4) значение $k < n$, вообще говоря, произвольно.

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

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

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

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

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

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

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

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

$$G_{7\times4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

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

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

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

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

*Замечания*:

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

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

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

Ясно, что

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

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

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

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

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

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

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

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

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

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

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

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

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

матрицей

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

Требуется:

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

1. *Несистематическое кодирование* находим непосредственно:

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

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

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

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

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

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

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

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

Далее нужно

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

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

В итоге получим проверочную матрицу

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

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

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

$$C = [\, \boldsymbol{v}_1 \ldots \boldsymbol{v}_8 \,] = \widetilde{G} \times [\, \boldsymbol{u}_1 \ldots \boldsymbol{u}_8 \,] =$$

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

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

$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_8$ — все 8 возможных сообщений, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_8$ — все 8 возможных кодовых слов. Оказалось $d = 3$.

## 3.3 Синдромное декодирование линейных кодов

### Синдром

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

Свойства синдрома:

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

Отсюда следует, что вектор ошибок $\boldsymbol{e}$ удовлетворяет неоднородной недоопределенной СЛАУ

$$H\boldsymbol{e} = \boldsymbol{s}, \qquad (*)$$

а кодовые слова являются решениями соответствующей однородной системы

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

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

$$\boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u}.$$

**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 $(*)$.

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 минимального веса несколько, то в качестве лидера может быть выбран любой из них.

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

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

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

Например, в *Примере* 3.2 получена матрица

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

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

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

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

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

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

Тогда порождающая матрица есть

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

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

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

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

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 $\boldsymbol{s} = \widetilde{H}\boldsymbol{w} = [\,1\,0\,1\,]^T$ указывает позицию ошибки.

## 3.4 Циклические коды

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

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

## Определение и построение циклических кодов

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

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

Поэтому построить циклический $(n, k)$-код длины можно следующим образом[3)].

1. Задаёмся нечётным (чтобы обеспечить взаимную простоту с $p = 2$) значением $n$ и выбираем любой делитель $g(x)$ бинома $x^n - 1$.
   Многочлен $g(x)$ называют *порождающим* или *образующим*; $\deg g(x) = m$, $k = n - m$.
2. Идеал $(g(x))$ кольца $R = \mathbb{F}_p[x]/(x^n - 1)$, образующий циклическое векторное подпространство в $R$, состоит из всех многочленов вида $f(x) \cdot g(x)$, $\deg f(x) \leqslant k$.
   Коэффициенты многочленов из этого идеала будут кодовыми словами. При удачном выборе порождающего полинома получается код с приемлемым значением $d$.

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

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

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

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

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

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

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

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 |

уже порождает циклический код.

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

*Несистематическое кодирование* осуществляется путём умножения кодируемого полинома на порождающий:

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

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

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

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

откуда

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

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

Для этого нужно выбрать какой-либо делитель бинома $x^7 - 1$. Определим сначала число и степени неприводимых делителей данного бинома, для чего применим способ разбиения вычетов по модулю 7 на орбиты относительно умножения на 2 (см. с. 63):

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

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

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

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

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

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*[4)].

Определяя код, выберем конкретно

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

2. Закодируем несистематическим и систематическим кодированием сообщение

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

*Несистематическое кодирование.*

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

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

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

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

поэтому

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

## Декодирование циклических кодов

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

Свойства синдрома $s(x)$:

- $0 \leqslant \deg s(x) < m$;
- $s(x) = 0 \Leftrightarrow w(x)$ — кодовое слово;
- $s(x) \equiv_{g(x)} w(x) \equiv_{g(x)} v(x)+e(x) \equiv_{g(x)} e(x)$.

*Схема синдромного декодирования слова $w(x)$:*

1) *вычисляется синдром $s(x)$;*
2) для всех $2^k$ возможных сообщений $u(x)$ 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 декодирования циклических кодов будут даны при рассмотрении БЧХ-кодов[5)].

## 3.5 Коды БЧХ

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

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

Для бинарных кодов $k = 1$, и это понятие тесно связано с понятием орбиты отображения $t \mapsto 2t \mod (2^l - 1)$ элементов мультипликативной группы (см. с. 64) поля $\mathbb{F}_2^l$, когда оно является полем разложения неприводимых над $\mathbb{F}_2$ полиномов.

*Определение* 3.6 (для поля $\mathbb{F}_2$). *Циклотомическим классом* элемента $\alpha \neq 0$ поля $\mathbb{F}_2^l$ над своим простым

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

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

подполем $\mathbb{F}_2$ называется множество всех *различных* элементов $\alpha$, $\alpha^2$, $\alpha^4$, ... из $\mathbb{F}_2^l$.

*Свойства циклотомических классов.*

1. Циклотомические классы $C_0$, $C_1$, ... различных элементов либо совпадают, либо не пересекаются, и в совокупности образуют *разбиение* мультипликативной группы поля $\mathbb{F}_2^l$, или, как говорят, её *разложение на классы*.
2. Если $\alpha$ — *примитивный элемент* поля $\mathbb{F}_2^l$, то его циклотомический класс *содержит ровно $l$ элементов*: поскольку $\alpha^{2^l} = 1$, данный класс есть
$$C_1 = \left\{ \alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{l-1}} \right\}.$$
3. Минимальный многочлен некоторого элемента циклотомического класса является общим *для всех элементов этого класса*.

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

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

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

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

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

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

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

Далее, поскольку

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

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

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

*Для построения кода БЧХ нужно*:

1) выбрать величину $l$, определяющую длину кода $n = 2^l - 1$ и степень расширения простого поля $\mathbb{F}_2$;

2) задать величину конструктивного расстояния $d_c = 2r + 1 < n$, если необходимо исправлять до $r$ ошибок;

3) выбрав неприводимый полином $a(x) \in \mathbb{F}_2[x]$ степени $l$, определить поле $\mathbb{F}_2^l = \mathbb{F}_2[x]/(a(x))$ с примитивным элементом $\alpha$;

4) найти циклотомические классы поля $\mathbb{F}_2^l$ над $\mathbb{F}_2$, в которые попадают $d_c - 1$ нулей кода $\alpha$, $\alpha^2$, ..., $\alpha^{2r}$; пусть таких классов $h$;

5) найти минимальные многочлены $g_1(x)$, ..., $g_h(x)$ каждого циклотомического класса;

6) вычислить порождающий полином кода

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

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

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

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

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

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

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

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

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

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

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

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

Найдем м. м. для $C_2$:

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

Вычислим коэффициенты $g_2(x)$:

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

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

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

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

$$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

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

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

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

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

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

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

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

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

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

$$g_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = \ldots$$

$$\ldots = x^4 + x^3 + x^2 + x + 1.$$

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

2. *Код БЧХ длины $n = 15$, исправляющий $r = 3$ ошибки.* Теперь $2r = 6$ и нужно найти полином, являющийся м. м. для нулей $\alpha$, $\alpha^2$, $\ldots$, $\alpha^6$, которые попадают в циклотомические классы $C_1$, $C_2$ и $C_3$.

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

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

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

## 3.6 Декодирование кодов БЧХ

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

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

Для декодирования принятого слова $w(x)$ вычисляем синдром $s_1 = w(\alpha) = s$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется). При $s = 0$ считаем, что ошибок не произошло. Если $s \neq 0$, то определяем значение $j$, для которого $\alpha^j = s$ и считаем, что произошла единичная ошибка в $j$-м разряде для $j = 0, 1, \ldots, n-1$.

*Пример* 3.10. Рассматриваем $(7, 4)$-код Хэмминга, построенный в примере 3.6 для циклических кодов, где был выбран порождающий полином $g(x) = x^3 + x + 1$ и найдено систематическое кодирование $v(x)$ сообщения $u(x) = x^3 + x^2 \leftrightarrow [\,0\,0\,1\,1\,]^T$:

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

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

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

Для декодирования $w(x)$ найдем синдром:

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

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

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

и 5-я позиция ошибки определена верно.

**Декодирование кодов БЧХ: общий случай.** Рассмотрим $(n, k, d)$-код БЧХ длины $n = 2^l - 1$ при построении которого для определения порождающего полинома использовалось поле $F = \mathbb{F}_2^l = \mathbb{F}_2[x]/(a(x))$, $\deg a(x) = l$ и пусть $\alpha$ — нуль кода.

Пусть при передаче кодового слова произошло $\nu \leqslant r = \lfloor (d-1)/2 \rfloor$ ошибок в позициях $j_1, \ldots, j_\nu$. 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 ошибок не произошло. Иначе для $1 \leqslant \nu$ запишем с учётом $(\alpha^i)^j = (\alpha^j)^i$ значения синдромов через степени $\alpha$:

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

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

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

Перепишем полученную систему:

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

Определим *полином локаторов ошибок*

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

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

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

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

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

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

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

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

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

После нахождения $\sigma(x)$ можно отыскать все $\nu$ его корней $\alpha^{-j_i}$, а по ним — позиции ошибок $j_i$, $i = \overline{1, \nu}$.

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

Пусть $n = 2^l - 1$, $\alpha$ — нуль кода, примитивный элемент поля $F = \mathbb{F}_2[x]/(a(x)) = \mathbb{F}_2^l$, $\deg a(x) = l$ и принято слово $w(x)$.

1. Найти все синдромы $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$; если все они равны 0, то считаем, что ошибок нет, $v(x) = w(x)$ и переход к пункту 6.
2. Используя тот или иной декодер, найти полином локаторов ошибок $\sigma(x)$; число произошедших ошибок $\nu = \deg \sigma(x)$.
3. Найти все корни $\sigma(x)$, например, перебором элементов $F^*$; пусть эти корни суть $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
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 $v(x) = w(x) + e(x)$.

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

6. По $v(x)$ восстановить 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 —

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

Замечаем, что значения $\lambda_i$ по данной формуле для $i = \nu{+}1, \ldots, 2r$ суть левые части соотношений $(*)$, то есть все они равны 0. Значит, полином значений ошибок имеет нулевую «среднюю часть». Обозначим его начальную часть $\lambda(x)$, а из заключительной вынесем за скобку $x^{2r+1}$:

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

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 поле $F$ (см. с. 42) с условием останова $\deg\lambda(x) \leqslant r$, конкретно — «*степень полученного остатка не более* $r$», и опусканием заключительного шага нормировки.

*Пример* 3.11. Будем использовать БЧХ $(15, 5, 7)$-код с полем разложения $\mathbb{F}_2[x]/\big(x^4 + x + 1\big) = F$, построенный в п. 2 примера 3.9. При вычислениях будем пользоваться таблицей со с. 47.

Пусть передаётся сообщение

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

При систематическом кодировании порождающим полиномом (3.1) кодовым словом, как можно показать, будет

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

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

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

1. Найдём все $2r = 6$ синдромов:

$$s_1 = w(\alpha) = (\underbrace{\alpha^3+1}_{\alpha^{14}}) + (\underbrace{\alpha^3+\alpha^2+\alpha}_{\alpha^{11}}) + (\underbrace{\alpha^2+1}_{\alpha^8}) +$$
$$+ (\underbrace{\alpha^3+\alpha^2}_{\alpha^6}) + (\underbrace{\alpha+1}_{\alpha^4}) + \alpha^3+\alpha^2+\alpha+1 = \alpha,$$
$$s_2 = w(\alpha^2) = (w(\alpha))^2 = s_1^2 = \alpha^2,$$
$$s_3 = w(\alpha^3) = \alpha^{42}+\alpha^{33}+\alpha^{24}+\alpha^{18}+\alpha^{12}+\alpha^9+$$
$$+\alpha^6+\alpha^3+1 = \ldots = \alpha^8,$$
$$s_4 = w(\alpha^4) = s_1^4 = \alpha^4,$$
$$s_5 = w(\alpha^5) = \alpha^{70}+\alpha^{55}+\alpha^{40}+\alpha^{30}+\alpha^{20}+\alpha^{15}+$$
$$+\alpha^{10}+\alpha^5+1 = \ldots = 1,$$
$$s_6 = w(\alpha^6) = s_3^2 = \alpha^{16} = \alpha.$$

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

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

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

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

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

и установлено число ошибок $\nu = \deg \sigma(x) = 3$.

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

$\sigma(\alpha) = \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2$,
$\sigma(\alpha^2) = \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha$,
$\sigma(\alpha^3) = \alpha^{10} + \alpha^{11} + \alpha^2 + \alpha^{13} = \mathbf{0}$,
$\sigma(\alpha^4) = \alpha^{13} + \alpha^{13} + \alpha^3 + \alpha^{13} = \alpha^2 + 1$,
$\sigma(\alpha^5) = \alpha + 1 + \alpha^4 + \alpha^{13} = \alpha^{13}$,
$\sigma(\alpha^6) = \alpha^4 + \alpha^2 + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^2$,
$\sigma(\alpha^7) = \alpha^7 + \alpha^4 + \alpha^6 + \alpha^{13} = \alpha^3 + 1$,
$\sigma(\alpha^8) = \alpha^{10} + \alpha^6 + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + 1$,

$$\begin{aligned}
\sigma(\alpha^9) &= \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = \mathbf{0},\\
\sigma(\alpha^{10}) &= \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha,\\
\sigma(\alpha^{11}) &= \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha,\\
\sigma(\alpha^{12}) &= \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1,\\
\sigma(\alpha^{13}) &= \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{14}) &= \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1,\\
\sigma(\alpha^{15}) &= \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = \mathbf{0}.
\end{aligned}$$

4. По найденным корням $\alpha^3$, $\alpha^9$, $\alpha^{15}$ вычисляем позиции ошибок:

$$j_1 = \text{-}3 \equiv_{15} 12, \quad j_2 = \text{-}9 \equiv_{15} 6, \quad j_3 = \text{-}15 \equiv_{15} 0.$$

5. Таким образом полином ошибок

$$e(x) = x^{12} + x^6 + 1$$

определён и переданное кодовое слово есть

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

Проверка $v(\alpha) = v(\alpha^2) = \ldots = v(\alpha^6) = 0$ говорит от том, что восстановление верное (или же произошло $r \gg 3$ ошибок, что маловероятно).

6. Поскольку применялось систематическое кодирование, исходное сообщение $u(x)$ восстанавливается элементарно.

*Помехоустойчивое кодирование применяется:*

- Для получения надежной связи либо при малом отношении сигнал/шум канала, либо в системах, критичных к ошибкам (ВТ).

- Для защиты данных во внутренних и внешних ЗУ: ленты, SSD диски, flash-память.
- При синтезе отказоустойчивых дискретных управляющих устройств (например, БИС).

*Справка.* В системах передачи данных широко используется двоичный $(255, 231, 7)$-код БЧХ, для которого $l = 8$ и степень порождающего код многочлена $g(x)$ есть $m = 24$. При этом в общем количестве слов длины 255 доля кодовых есть $2^{-24} \approx 17 \cdot 10^{-6}$, а все шары радиуса 3 с центрами в кодовых словах занимают $\approx 16{,}5\%$ объёма куба $B^{255}$.

В течении многих лет не было случая, чтобы ошибка передачи прошла незамеченной.

*Замечание.* Исправление ошибок может требоваться не всегда: часто достаточно лишь проверить наличие ошибок и при необходимости повторить передачу нужное число раз. В этих случаях применяются коды, предназначенные только для обнаружения ошибок.

## 3.7 Задачи

3.1. Для линейного кода, заданного своей проверочной матрицей

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

требуется

1) построить порождающую матрицу $G$ кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;
2) найти такое кодирование для сообщений

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

3.2. Циклический $(9,3)$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить его кодовое расстояние $d$, а также осуществить систематическое кодирование полинома

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

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

Требуется декодировать полиномы

1) $w_1(x) = x^6 + x^2 + x$,
2) $w_2(x) = x^6 + x^5 + x^3 + x^2 + x$,
3) $w_3(x) = x^6 + x^3 + x^2 + x$.

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

3.5. Пусть $\alpha$ — примитивный элемент поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/\big(x^4 + x + 1\big)$. Для кода БЧХ с нулями $\alpha$, $\alpha^2$, $\alpha^3$ и $\alpha^4$ и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

3.6. Рассмотрим код БЧХ, нули которого определяются степенями $\alpha$, где $\alpha$ — 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 $w(x)$.

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

3.8. Рассмотрим БЧХ-код, нули которого есть степени примитивного элемента $\alpha$ 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.

*Основные криптографические термины*

*Открытый текст* (plaintext) — текст, подлежащий зашифрованию; как правило, это последовательность двоичных битов и мы будем так считать в дальнейшем.

*Шифртекст, криптограмма* (ciphertext — результат зашифрования открытого текста; также будем считать, что шифртекст есть битовая последовательность.

[1)] дословно — тайнопись

*Шифр* (cipher) — семейство обратимых отображений множества последовательностей открытых текстов в множество последовательностей шифртекстов.

Алгоритм шифрования тщательно разрабатывается и меняется в редких случаях.

*Ключ* (key) или *криптопеременная* (cryptovariable) — параметр(ы), определяющий(ие) выбор конкретного отображения из входящих в шифр, его сменная часть.

*Зашифрование* (encryption) — процесс преобразования открытого текста в шифрованный с помощью шифра.

*Расшифрование* (decryption) — процесс, обратный к зашифрованию, реализуемый при известном значении ключа.

*Дешифрование* — процесс раскрытия сообщения злоумышленником без знания секретного ключа, т. е. взлом криптосистемы.

Определения шифра и его ключа соответствуют принятому в современной криптографии правилу стойкости О. Керкгоффса[2)], согласно которому в секрете держится только ключ, а сам алгоритм шифрования открыт[3)]. Поэтому надёжность шифрования

[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.

[3)] Как сформулировал К. Шеннон, «враг знает систему».

определяется исключительно значением секретного ключа, известному только легальным пользователям. По необходимости ключ легко меняется. В современных шифрсистемах ключ задается двоичным числом длиной 128...4096 бит.

Шифры подразделяются на:

*блочные* — сообщение разбивается на блоки фиксированной длины, которые при данном значении ключа шифруются одним преобразованием;

*поточные* — сообщение шифруется последовательно посимвольно (символ может быть длины 32, 64, ... битов), причем при данном ключе преобразование шифрования изменяется во времени за счёт создаваемого т. н. «ключевого потока».

**Симметрические и асимметрические шифрсистемы. Сложность алгоритмов.** Зашифрование открытого текста и его расшифрование проводят с использованием, как правило, различных ключей[4)]; будем обозначать их $k_e$ и $k_d$ соответственно. Множество возможных значений $k_e$ и $k_d$ называют *пространством ключей*.

Если ключ $k_d$ может быть легко получен из $k_e$, то соответствующая система называется *симметрической*, а в противном случае — *ассиметрической*. Понятно, что при использовании симметрической криптосистемы оба ключа должны быть известны только

[4)] Примером системы с совпадающими ключами является шифрсистема *гаммирования*, когда криптограмму получают из открытого текста путём сложения его по mod 2 с некоторой случайным двоичным словом $\gamma$, а вторичное такое сложение её расшифровывает.

легальным абонентам, а для всех остальных — оставаться секретными.

При ассиметрическом шифровании ключ расшифрования $k_d$ остаётся секретным, а ключ зашифрования $k_e$ делается общедоступным. Расшифровать криптограмму может только абонент, которому известен секретный ключ, который нельзя 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 простом переборе элементов пространства секретных ключей. *Экспоненциальным* называют алгоритм, имеющий оценку вида $exp(l)$.

Часто существует и субэкспоненциальный алгоритм подбора ключа $k_d$. Время работы *субэкспоненциального* алгоритма асимптотически меньше любой экспоненты, но больше любого полинома.

**Алгоритм быстрого возведения в степень** — позволяет эффективно использовать в криптографии арифметику вычетов.

Если $x$ — произвольное число, то при возведении его степень можно использовать его двоичную запись

$$x = a_0 2^0 + a_1 2^1 + \ldots + a_k 2^k,\ a_i \in \{0,1\},\ i = \overline{0,k}.$$

Пусть, например, требуется вычислить $y = a^{53}$. Показатель степени представляется в виде $53 = 2^5 + 2^4 + 2^2 + 1$, поэтому

$$a^{53} = \left(\left(\left(\left(a^2\right)^2\right)^2\right)^2\right)^2 \cdot \left(\left(\left(a^2\right)^2\right)^2\right)^2 \cdot \left(a^2\right)^2 \cdot a.$$

Вычисление первой скобки требует 5 умножений. В процессе получения её значения вычисляются также вторая и третья скобки, значения которых запоминаются. Перемножение четырёх сомножителей требует ещё трёх умножений. Таким образом, для вычисления $y$ требуется только $5 + 3 = 8$, а не 52 умножения.

Заметим, что возведение числа в степень двойки реализуется на компьютере чрезвычайно просто — сдвигом слова.

При получении степени элемента по некоторому модулю $n$, заметим, что остаток от на $n$ проще возводить в квадрат, чем само число. Поэтому

$$a^x \equiv_n \left\{\frac{a^{a_0 2^0}}{n}\right\} \cdot \left\{\frac{a^{a_1 2^1}}{n}\right\} \cdot \ldots \cdot \left\{\frac{a^{a_k 2^k}}{n}\right\}, \qquad (4.1)$$

где $\left\{\frac{a^2}{n}\right\}$ — остаток от деления $a^2$ на $n$. Но $a^{2\cdot 2} = \left(a^2\right)^2 = \left\{\frac{a^2}{n}\right\}^2 \pmod n$ и окончательно получим

$$a^{2^k} \equiv_n \left\{\left\{\frac{a^2}{n}\right\}^2 \ldots\right\}^2.$$

Способ (4.1) вычисления $a^x$ по mod $n$ называют методом *повторного возведения в квадрат.*

*Пример* 4.1. Вычислим $b = 3^{14} \pmod 5$.
1. Находим вектор $[\, a_0, \dots \,]$ двоичного представления числа 14: $14 = 8+4+2 = 0+2^1+2^2+2^3 = [\, 0\ 1\ 1\ 1 \,]$.
2. Вычисляем степени 3 по mod 5:

$$a_0 \equiv_5 3, \qquad a_1 = 3^2 = 9 \equiv_5 4$$
$$a_2 = 4^2 = 16 \equiv_5 1, \qquad a_3 = 1^1 \equiv_5 1.$$

3. Окончательно вычисляем $b = 3^0 \cdot 4^1 \cdot 1^1 \cdot 1^1 = 4 \equiv_5 4$.

**Китайская теорема об остатках.**

*Теорема* 4.1. *Пусть* $n_1, \dots, n_k$ — *попарно взаимно простые числа и* $M = n_1 \cdot \ldots \cdot n_k$. *Тогда для любых целых* $r_1, \dots, r_k$ *система сравнений*

$$\begin{cases} x \ \equiv_{n_1} r_1, \\ \quad \dots \\ x \ \equiv_{n_k} r_k, \end{cases}$$

*имеет в интервале* $0 \leqslant x \leqslant M-1$ *единственное решение*

$$x = \sum_{j=1}^{k} r_j \cdot M_j \cdot N_j \pmod M,$$

*где* $M_j = M/n_j$ *и* $N_j = M_j^{-1} \pmod{n_j}$.

**Задача о рюкзаке** — выбрать такие элементы вектора-строки $\boldsymbol{a} = [\ a_1\ \dots\ a_n\ ]$ *различных* целых, чтобы их сумма в точности равнялась данному $z$ («размер рюкзака»)[5].

[5] предполагается, что решение существует и единственно; другое название задачи — *проблема подмножества суммы*

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 будет вектор-столбец $\boldsymbol{x} = [\ 0\,1\,0\,1\,1\,0\,1\,1\,0\,0\ ]^T$ позиций выбранных чисел: $\boldsymbol{a} \times \boldsymbol{x} = 3231 = z$.

Неизвестны полиномиальные алгоритмы решения задачи о рюкзаке.

**Односторонняя функция** — центральное понятие криптографии.

*Определение* 4.1. *Односторонней* (или *однонаправленной*, англ. 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 инвертирования функции $f$ (т. е. решения уравнения $f(x) = y$ относительно $x$).

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* (невозможно за полиномиальное время).

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. Бóльшая их часть 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 $a^x \equiv_n b$ (задача DLOG).
- Решить задачу о рюкзаке.
- Декодировать исправляющий ошибки линейный код общего вида.

Данное понятие послужило толчком к определению однонаправленной функции с секретом.

**Односторонняя функция с секретом** (или лазейкой; англ. trap-door one-way function) — зависящая от параметра $k$, называемым *секретным ключом* или *лазейкой*, обратимая функция $f_k(x) : X \to Y$ такая, что

1) для вычисления значения $f_k(x)$ за полиномиальное время не требуется знания параметра $k$;
2) имеется полиномиальный алгоритм, вычисляющий при известном $k$ значение $f_k^{-1}(y)$ для всех $y \in Y$;
3) почти для всех $k$ и $y \in Y$, нахождение $f_k^{-1}(y)$ вычислительно неосуществимо без знания $k$.

Один из примеров односторонней функции с лазейкой — функция $f(x) = x^m \pmod n$, $m$ и $n$ известны: вычисление $f(x) = y$ производится одним из методов быстрого возведения в степень, а эффективный

алгоритм обратного преобразования $f^{-1}(y)$ (*вычисления корня $m$-й степени по* $\bmod n$) требует знания примарного разложения $n$. Эта информация может считаться секретным ключом.

Применение односторонних функций с секретом позволяет, например, организовать обмен шифрованными сообщениями по открытым каналов связи, снабдить документ электронной подписью.

**Электронная цифровая подпись (ЭЦП)** — позволяет проверить авторство документа и отсутствие в нём искажений.

Идея организации электронной подписи на основе односторонних функций с секретом проста:

1. Автор для своего сообщения $a$ вычисляет значение $y$ его хэш-функции, преобразующей $a$ в битовую строку установленной длины[6)].
2. Используя свой секретный ключ $k$ к односторонней функции с секретом $f_k$, автор вычисляет значение $x = f_k^{-1}(y)$ и посылает сообщение $a$, его хэш $y$ и вычисленное значение $x$ адресатам.
3. Проверку авторства документа $a$ легко проводит любой адресат, вычисляя $f_k(x)$ и сравнивая полученное значение с $y$.

[6)] Понятно, что хэш-функции осуществляют необратитмые преобразование информации, поскольку у них множество значений аргумента значительно превосходит множество значений функции. Хэш $y$ выступает как компактный представитель (паспорт) сообщения $a$. К хэш-функциям предъявляются специфические требования, которые мы не будем здесь обсуждать.

4. Снабдить ЭЦП данного автора какой-либо документ без знания секрета — вычислительно неосуществимая задача.

**Обмен шифртекстами по открытому каналу связи.** Приведём пример использования односторонней функции с лазейкой при решении задачи о рюкзаке[7)]. Рассмотрим простейшую рюкзачную систему, задаваемую вектор-строкой $\boldsymbol{a}$.

Пусть открытый текст состоит из двоичных векторов-сообщений $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^n$. 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 решение задачи элементарно.

Действительно, пусть, например,

$$\boldsymbol{a} = [\, 25\ 27\ 56\ 112\ 231\ 452\ 916\ 1803 \,] \ \text{ и } \ z = 1449.$$

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.

[7)] На ней основаны системы шифрования Меркля–Хеллмана и Шора–Ривеста.

Рассуждая аналогично, получаем код позиций выбираемых элементов: [ 1 0 1 0 0 1 1 0 ].

Преобразуем сверхрастущий вектор $\boldsymbol{a}$ в вектор $\boldsymbol{b}$, для чего выберем модуль $m$, больший суммы всех элементов $\boldsymbol{a}$, возьмем некоторое $t$, взаимно простое с $m$, и каждый элемент $\boldsymbol{b}$ будем вычислять по правилу $b_i \equiv_m a_i \cdot t$. Вектор $\boldsymbol{b}$ уже не является сверхрастущим и может быть опубликован в качестве открытого ключа, а лазейкой будут значения $m$ и $t$.

*Пример* 4.2. 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 $t = 40$. 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, зная секретный ключ $(m, t) = (37, 40)$, находит такое $u$, что $t \cdot u \equiv_m 1$. В нашем случае $u = 25$: $40 \cdot 25 = 1000 \equiv_{37} 1$.

Затем, получив шифртекст $\boldsymbol{y}$ и отрытый ключ $\boldsymbol{b}$ легальный получатель —

1) восстанавливает вектор $\boldsymbol{a} \equiv_m u\boldsymbol{b}$:

$$\boldsymbol{a} = 25 \cdot [\ 3\ 6\ 12\ 24\ 11\ ] \equiv_{37} [\ 1\ 2\ 4\ 8\ 16\ ];$$

2) находит вектор $\boldsymbol{z} \equiv_m u\boldsymbol{y} = [\ z_1\ z_2\ z_3\ ]$:

$$\boldsymbol{z} = 25 \cdot [\ 39\ 29\ 14\ ] \equiv_{37} [\ 13\ 22\ 17\ ];$$

3) легко решает 3 задачи о рюкзаке со сверхрастущим $\boldsymbol{a}$ и $z_1 = 13$, $z_2 = 22$, $z_3 = 17$, определяя передаваемые сообщения $\boldsymbol{x}^1$, $\boldsymbol{x}^2$, $\boldsymbol{x}^3$.

**Протокол выработки общего секретного ключа по открытому каналу связи** — покажем, как это можно сделать на примере протокола DH Диффи–Хеллмана[8)].

Два лица — традиционно $A$ (Алиса) и $B$ (Боб) — обмениваются сообщениями по открытому каналу, то есть читать их может кто угодно. Чтобы обеспечить секретность переписки, $A$ и $B$ должны выработать общий секретный ключ. Для этого они выбирают простое число $p$[9)] и в поле Галуа $GF(p)$ — некоторый примитивный элемент $\alpha$. Значения $p$ и $\alpha$ открыты.

Для выработки секретного ключа $A$ и $B$ независимо друг от друга выбирают по одному случайному натуральному числу $x$ и $y$ соответственно, которые

[8)] Предложен сотрудниками MTI У. Диффи, М. Хеллманом и независимо от них Р. Мерклем в 1976 г.

[9)] в современных криптосистемах $p$ имеет длину порядка 2000 бит

держат в секрете. Далее каждый из них вычисляет новый элемент поля $GF(p)$:

$$X \equiv_p \alpha^x, \qquad Y \equiv_p \alpha^y, \qquad (*)$$

которыми обмениваются по открытому каналу.

Абонент $A$, получив $Y$, вычисляет ключ — элемент $GF(p)$:

$$K \equiv_p Y^x$$

и аналогично поступает абонент $B$:

$$K \equiv_p X^y.$$

Тем самым у Алисы и Боба появился общий секретный ключ $K = \alpha^{xy} \in GF(p)$.

Злоумышленник — традиционно $E$ (Ева[10], от англ. eavesdropper, подслушивающий) — не может узнать ключ $K$: его определение связано с решением одного из уравнений $(*)$, а это вычислительно трудная задача DLOG.

Заметим, что задача DLOG принадлежит классу $NP$, но $NP$-полнота её не доказана, также, как и для задачи факторизации.

Мы видим, что протокол DH устойчив к пассивной атаке, но при беззащитен от активного вмешательства типа «человек посередине». Действительно, при обмене сообщениями Алиса, ни Боб не могут достоверно определить, кем является их собеседник. Предположим, к каналу связи имеет доступ злоумышленник — традиционно $M$ (Меллори[11]), который перехватывает сообщения и Алисе выдает себя за Боба, а Бобу представляется Алисой.

[10] пассивный злоумышленник, перехватывающий, но не изменяющий сообщений

[11] от malicious — активный злоумышленник; в отличие от пассивного, Мэллори может изменять сообщения, полностью подменять их и т .д.

Тогда Алиса и Боб в действительности общаются не между собой, а с Мелори. Он получает ключ $k_{AM}$, общий с Алисой, и один ключ $k_{BM}$ с Бобом. Поэтому Мелори может, получив сообщение от Алисы, расшифровать его ключом $k_{AM}$, произвольно изменить, и зашифровав ключом $k_{BM}$, передать Бобу. При этом подлог может оставаться незамеченным очень долгое время.

В качестве защиты от такого вмешательства $A$ и $B$ могут воспользоваться ЭЦП.

## 4.2 Система шифрования RSA

RSA[12)] — классическая ассиметрическая криптосистема с открытым ключом.

В системе RSA 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

$$f : x \to x^e \pmod n. \tag{4.2}$$

Для расшифрования сообщения $y = f_d(x)$ нужно решить сравнение

$$x^e \equiv_n y.$$

Основной вопрос системы RSA — выбор параметра открытого ключа $(n, e)$, при котором нахождение этого решения является сложной задачей.

[12)] аббревиатура от фамилий авторов Рональда Ривеста, Ади Шамира и Леонарда Адлемана (R. Rivest, A. Shamir, L. Adleman) из MTI; предложена в 1978 г.

Искомое решение может быть представлено в виде

$$x \equiv_n y^d, \tag{4.3}$$

которое будет единственным при предположениях, что число $n$ свободно от квадратов, а значения $e$ и $\varphi(n)$ взаимно просты. Пара $(d, \varphi(n))$ является секретным ключом криптосистемы RSA.

Функция $f(x)$ легко вычисляется с помощью алгоритма быстрого возведения в степень, также как и при известном $d$ — обратная к ней функция $f_d : y \to y^d \pmod n$.

Получить секретный ключа $d$ можно, решив, например с помощью алгоритма 2.2 со с. 40, сравнение

$$d \cdot e \equiv 1 \pmod{\varphi(n)}. \tag{4.4}$$

Для этого, в свою очередь, надо определить $\varphi(n)$, что просто реализуется при известной факторизации числа $n$. А вот последняя задача чрезвычайно трудоёмка: *схема RSA основана на сложности задачи FACT.*

Конкретно, авторы этой схемы предложили выбирать число $n$ в виде произведения двух больших простых множителей $p$ и $q$, примерно одинаковых по величине. Тогда $\varphi(n) = \varphi(pq) = (p-1)(q-1)$, и единственное условие на выбор экспоненты $e$ есть взаимная её простота с $p-1$ и $q-1$.

*Утверждение* 4.1. *Пусть $n = pq$, где $p, q$ — простые числа; тогда знание $p, q$ равносильно знанию $\varphi(n)$.*

*Доказательство.* Зная $p, q$ легко находят $\varphi(n) = (p-1)(q-1)$.

Обратно, зная $\varphi(n) = pq - (p+q) + 1$, имеем (значение $n$ открыто)

$$\begin{cases} p + q = n + 1 - \varphi(n), \\ pq = n. \end{cases}$$

Теперь $p, q$ 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 их произведение $n = pq$.
2. Затем он выбирает экспоненту $e$, достаточно большую и взаимно простую с числами $p - 1$ и $q - 1$, а перемножая последние — получает $\varphi(n)$; наконец по (4.4) определяет $d$.
3. Числа $n$ и $e$ публикуются, число $d$ остается секретным.
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), что без знания секретного ключа $d$ вычислительно невозможно.

*Пример* 4.3. Пусть $p = 11$, $q = 13$, тогда $n = 143$.

Выберем значение $e = 13$, оно, очевидно, взаимно просто с $p - 1 = 10$ и $q - 1 = 12$. Вычисляем $\varphi(143) = 10 \cdot 12 = 120$.

Решим относительно $d$ сравнение

$$d \cdot 13 \equiv_{120} 1$$

Применияя алгоритм Inv-Zm

| | | | |
|---|---|---|---|
| 1 | 120 | 0 | |
| 2 | 13 | 1 | $q = 9$ ( 117 9 ) |
| 3 | 3 | -9 | $q = 4$ ( 12 -36 ) |
| 4 | 1 | **37** | $q = 3$ ( 3 . . . ) |
| 5 | 0 | | |

получаем $d = 37$.

Возьмём фрагмент текста, соответствующий, например, числу $x = 42$, и зашифруем его:

$$y = 42^{13} = 1\,265\,437\,718\,438\,866\,624\,512 \equiv_{143} 3.$$

Получив криптограмму $y$, легальный получатель расшифровывает её:

$$3^{37} = 450\,283\,905\,890\,997\,363 \equiv_{143} 42.$$

Перескажем близко к оригиналу тест из [5].

Для иллюстрации своего метода Ривест, Шамир и Адлеман зашифровали предложенным ими способом некоторую английскую фразу. Сначала она стандартным образом ($a = 01$, $b = 02$, …, $z = 26$, пробел $= 00$) была записана в виде целого числа $x$, а затем зашифрована с помощью отображения (4.2) при

$$n = 11438162575788886766932577997614661201021829672124$$
$$236256256184293570693524573389783059712356395870$$
$$5058989075147599290026879543541 \quad (129 \text{ знаков}),$$

и $e = 9007$. 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 соответствующее сообщение

$$y = 9686961375462206147714092225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4 \quad (123 \text{ знака}),$$

была обещана награда в \$100.

Видный американский криптограф Р. Риверст предполагал, что для расшифровки понадобится 40 квадрильонов лет. Однако в 1994 г., т. е. всего через 17 лет, D. Atkins, M. Graff, A. K. Lenstra и P. C. Leyland сообщили о решении задачи: в результате дешифровки получилась фраза «*The magic words are squeamish ossifrage*»[13]. Соответствующие числа $p$ и $q$ оказались равными

$$p = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$q = 2769132993266709549961988190834461413177642967992942539798288533.$$

Выполнение вычислений потребовало колоссальных по тем временам ресурсов: в работе, возглавлявшейся четырьмя авторами проекта 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 в области поиска эффективных алгоритмов факторизации был достигнут большой прогресс, и в 2015 г. для дешифрирования этого сообщения при использовании облачных вычислений потребовалось около одного дня.

[13] *Волшебные слова — привередливая скопа* (скопа — крупная хищная птица отряда ястребообразных), по-видимому, нарочито бессмысленная фраза.

Заметим, что созданы и используются специальные языки программирования для вычислений с большими числами (например, свободно распространяемые PARI и UBASIC).

## 4.3 Простота и факторизация натуральных чисел

**Тесты на простоту числа.** Элементарный способ убедится в простоте числа $N$ называется *методом пробных делений*, и состоит в проверке делимости $N$ на все простые числа из диапазона $\left[2, \sqrt{N}\right]$. Однако для проверки простоты чисел порядка $10^{30}$–$10^{40}$ этот метод уже неприменим[14)].

В общем случае для определения простоты числа (без разложения его на множители!) является использование

*Теорема* 4.2 (Ферма, малая). *Если $a$ — целое, а $p$ — простое то*

$$a \not\vdots p \;\Rightarrow\; a^{p-1} \equiv_p 1.$$

Поэтому, если каком-то $a$, не делящимся на $N$ окажется, что сравнение

$$a^{N-1} \equiv_N 1, \tag{4.5}$$

[14)] Количество простых в указанном промежутке, асимптотически равно $2\sqrt{N}/\ln n$, то есть находим, что при $N$, записываемом 100 десятичными цифрами, найдется не менее $4 \cdot 10^{42}$ простых чисел и компьютеру, выполняющему миллион делений в секунду, для разложения таких $N$ методом перебора потребуется не менее, чем $10^{35}$ лет.

нарушается, то $N$ — *составное*. Иначе вопрос остаётся открытым и можно попробовать испытать $N$ при другом значении $a$.

Имеется, однако, бесконечно много составных чисел, для которых сравнение (4.5) выполняется при всех $a$, взаимно простых с $N$, т. е. они не будут выявлены данной проверкой. Эти числа называют *псевдопростыми* или *числами Кармайкла*[15)].

Можно несколько улучшить приведённый тест. Если $N$ — простое число и

$$N-1 \;=\; 2^s \cdot t, \quad \text{где } t \text{ нечетно},$$

то согласно малой теореме Ферма для каждого $a$ с условием взаимной простоты с $N$, хотя бы одна из скобок в произведении

$$(a^t-1)(a^t+1)(a^{2t}+1)\ldots(a^{2^{s-1}t}+1) \;=\; a^{N-1}-1$$

делится на $N$. Обратим это свойство.

Пусть $N$ — нечетное составное число и $N-1=2^s\cdot t$, где $t$ нечетно. Назовем целое число $a\in[\,2,\,N-1\,]$, «хорошим» для $N$, если нарушается хотя бы одно из двух *условий*:

(А) $N \not\vdots a$;

(Б) $a^t \equiv_N 1$ или существует целое $k\in[\,0,\,s-1\,]$ такое, что

$$a^{2^k t} \;\equiv_N\; -1.$$

Построим вероятностный

*Алгоритм проверки непростоты числа $N$*

[15)] $561 = 3\cdot 11\cdot 17$ — пример такого числа. По мере возрастания числа Кармайкла становятся более редкими.

1. Выбирается случайное натуральное $a < N$ и для него проверяются свойства (А) и (Б).
2. Если хотя бы одно из них нарушается, то $N$ — составное.
   Иначе возвращаемся к шагу 1.

Показано, что для *простого* числа $N$ не существует «хороших» чисел $a$, если же $N$ *составное*, то их существует не менее $\frac{3}{4}(N-1)$. Поэтому вероятность того, что после однократного выполнения шагов данного алгоритма составное число не будет опознано как таковое не превосходит $4^{-1}$, а после $k$ повторений — $4^{-k}$, то есть убывает очень быстро.

Для составления таблиц простых чисел наилучшим является известный метод решета Эратосфена, несмотря на то, что он требует большого объёма памяти. Метод состоит в вычёркивании из списка чисел 2, 3, ..., $N$ все числа, делящиеся на 2, кроме 2, затем все числа, делящиеся на 3, кроме 3 и т. д; в итоге останутся лишь простые числа. Имеются эффективные алгоритмы, реализующие данный метод.

На сегодняшний день разработаны быстрые и эффективные детерминированные алгоритмы определения простоты числа, основанные на эллиптических кривых[16)].

[16)] Алгоритм Адлемана-Померанса-Румели-Ленстры имеет сложность $O\left((\log n)^{c \log\log\log n}\right)$ арифметических операций и его реализация позволила проверять на простоту числа $n$ порядка $10^{100}$ за несколько минут.

Алгортим Аткина–Морейна проверки простоты числа порядка $10^{800}...10^{1000}$ требует нескольких недель вычислений.

**Генерация ключей. Линейный конгруэнтный метод.** Ключ шифрования должен быть случайным. Один из способов его получения — с помощью генератора псевдослучайных чисел.

Хорошие по статистическим свойствам последовательности получаются по формуле *линейного конгруэнтного метода*:

$$r_{i+1} \equiv_m a \cdot r_i + b, \quad i = 1, 2, \ldots,$$

где $r_i$ — $i$-й член псевдослучайной последовательности, $a$, $b$, $m$ — некоторые целые числа. Качество псевдослучайной последовательности зависит от выбора этих взаимно простых чисел.

Очевидно, рассматриваемая последовательность будет периодической. Однако показано, что её длина может достигать значения $m$. Часто данный генератор используют с параметрами

$$a = 214\,013,\ b = 2\,531\,011,\ m = 2^{32},$$

а в качестве $r_1$ берут текущее время с точностью до тика таймера.

Ясно, что значение $r_1$ однозначно определяет значения всех следующих членов последовательности. Поэтому при выборе в качестве ключа вектора $(r_1, \ldots, r_N)$ различных двоичных последовательностей будет $2^{\text{размер}\, r_1}$. 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 случайного 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.** Для этой задачи наиболее эффективное средство — использование малой теоремы Ферма.

Пусть имеется большое простое число $S$. Для построения существенно большего простого $N$

1) выберем случайным образом четное число $R$ на промежутке $S \leqslant R \leqslant 4S + 2$ и положим $N = SR + 1$;
2) проверим число $N$ на отсутствие малых простых делителей, разделив его на малые простые числа;
3) испытаем $N$ с помощью алгоритма со с. 135 достаточно много раз;
4) если выяснится, что $N$ — составное, то выберем новое значение $R$ и повторим вычисления.

Если $N$, выдерживает испытания данным алгоритмом, появляется надежда на то, что $N$ — простое чис-

ло, и следует попытаться доказать простоту с помощью более тонких известных тестов[17)].

На сегодняшний день созданы быстрые и эффективные алгоритмы для построения больших простых чисел.

**Факторизация** — нахождение примарного разложения натурального числа $n$

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

где $p_i$ — простые числа, $\alpha_i$ — натуральные, $i = \overline{1, s}$.

Стойкость к взлому многих криптосистем основывается на трудности факторизации (криптосистема RSA, некоторые схемы цифровой подписи и др.).

Полиномиальные алгоритмы факторизации неизвестны и, видимо, их вообще не существует. С появлением квантовых компьютеров задача FACT для такого числа может быть практически решена за реальное время[18)].

Далее для всех алгоритмов полагаем, что $n$ — нечётное составное, не являющееся степенью целого.

**$\rho$-алгоритм Полларда.** *Сплиттингом* натурального $n$ называют представление его в виде $n = a \cdot b$, $1 < a, b < n$, а числа $a$ и $b$ — *нетривиальными факторами* $n$.

---

[17)] см. теорему 4 на с. 102 книги *Введение в криптографию / Под общ. ред. В. В. Ященко. — М.: МЦНМО, 2012.*

[18)] Например, квантовый компьютер D-Wave канадской фирмы D-Wave Systems способен за секунду решать задачи, на выполнение которых у классического компьютера с одноядерным процессором ушло бы порядка 10 тыс. лет.

*ρ-алгоритм* сплиттинга составного целого $n$, которое не есть степень простого числа.

Шаг 0. Полагаем $a = 2$, $b = 2$, $f(x) = x^2 + 1$.

Шаг 1. Перевычисляем
$a := f(a)$, $b := f(f(b)) \pmod n$.

Шаг 2. Вычисляем $d = \text{НОД}(a - b, n)$.

Шаг 3. Если $d \in [\ 2,\ n - 1\ ]$, то вернуть $d$ как 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.

Предложенный Д. Поллардом в 1975 г. $\rho$-алгоритм строит числовую последовательность, элементы которой, начиная с некоторого номера $n$ образуют цикл, что иллюстрируется расположением чисел в виде греческой буквы $\rho$.

Основная идея $\rho$-алгоритма очень проста. Если период последовательности $x_i \pmod n$ может быть порядка $n$, то период последовательности $x_i \pmod p$ для простого делителя $p$ числа $n$ не превосходит $p$. Это значит, что $x_j$ и $x_k$ могут быть различными по модулю $n$, но совпадать по модулю $p$, т. е. $p \mid \text{НОД}(x_j - x_k, n)$.

$\rho$-алгоритм для сплиттинга числа $n$ требует $O\left(n^{1/4}\right)$ модулярных умножений и эффективен при поиске малых делителей.

*Пример* 4.4. 1. Пусть $n = 163\,829$.

Шаг 1. $a = 5$, $b = 26$.

Шаг 2. $a - b = 5 - 26 = -21 \equiv_{163\,829} = 163\,808$ и
$d = \text{НОД}\,(163\,808, 163\,829) = 23$.

Шаг 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 $\rho$-алгоритму Полларда приведены в следующей таблице.

| $a$ | $b$ | $d$ |
|---|---|---|
| 5 | 26 | 1 |
| 26 | 2871 | 1 |
| 677 | 179 685 | 1 |
| 2871 | 155 260 | 1 |
| 44 380 | 416 250 | 1 |
| 179 685 | 43 670 | 1 |
| 121 634 | 164 403 | 1 |
| 155 260 | 247 944 | 1 |
| 44 567 | 68 343 | 743 |

Следовательно, 743 и $455\,459/743 = 613$ есть два нетривиальных делителя $455\,459$; они оказываются простыми числами.

## $(p-1)$-алгоритм Полларда факторизации

*Определение* 4.2. Пусть $B$ — натуральное. Целое число $n$ называют *$B$-гладким*, или *гладким относительно границы $B$*, если все его простые делители не превосходят $B$.

$(p-1)$-алгоритм Полларда эффективно вычисляет *простой фактор* $p$ составного целого $n$, для которого $p-1$ есть *гладкое число* относительно некоторой сравнительно малой границы $B$.

$(p-1)$-*алгоритм*
вычисления простого фактора составного натурального $n$, которое не есть степень простого числа

Шаг 1. Выбрать гладкую границу $B < n$.

Шаг 2. Выбрать случайное целое $a \in [2, n-1]$, и вычислить $d = \text{НОД}(a, n)$.

Если $d \geqslant 2$, то вернуть $d$, как простой делитель $n$.

Шаг 3. Для каждого простого $q \leqslant B$ выполнить следующее.

Шаг 3.1. $l := \left\lfloor \dfrac{\ln n}{\ln q} \right\rfloor$.

Шаг 3.2. $a := a^{q^l} \pmod n$.

Шаг 4. $d := \text{НОД}(a-1, n)$.

Шаг 5. Если $1 < d < n$, то вернуть $d$ как простой делитель $n$.

Иначе алгоритм заканчивает работу и вопрос о нетривиальных факторах в $n$ остается открытым.

В случае отказа алгоритма можно попробовать испытать большее $B$.

*Пример* 4.5. Применим $(p-1)$-алгоритм Полларда для нахождения нетривиального фактора для $n = 19\,048\,567$.

Шаг 1. Выберем гладкую границу $B = 19$.

Шаг 2. Выберем целое $a = 3$ и вычислим $\text{НОД}(3, n) = 1$.

Шаг 3. В следующей таблице приведены значения $q, l, a$ после каждой итерации Шага 3 рассматриваемого алгоритма.

| $q$ | $l$ | $a$ |
|---|---|---|
| 2 | 24 | 2 293 244 |
| 3 | 15 | 13 555 889 |
| 5 | 10 | 16 937 223 |
| 7 | 8 | 15 214 586 |
| 11 | 6 | 9 685 355 |
| 13 | 6 | 13 271 154 |
| 17 | 5 | 11 406 961 |
| 19 | 5 | 554 506 |

Шаг 4. $d = \text{НОД}(554\,506 - 1, n) = 5\,281$.

Шаг 5. Два нетривиальных фактора $n$ есть $p = 5\,281$ и $q = n/p = 3\,607$ (эти факторы оказались простыми числами).

*Замечание.* Поскольку $p - 1 = 5\,280 = 2^5 \cdot 3 \cdot 5 \cdot 11$, то $p - 1$ есть 19-гладкое число (2, 3, 5, $11 \leqslant 19$ и $B = 19$ угадано верно). А $q - 1 = 3\,606 = 2 \cdot 3 \cdot 601$ — не есть 19-гладкое число.

## 4.4 Задача дискретного логарифмирования

**Дискретное логарифмирование. Криптосистема Эль-Гамаля.** 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 базируется ряд методов криптографии с отрытым ключом, например, рассмотренная ранее криптосистема Диффи–Хелмана и система Эль-Гамаля[19] ElGamal и др.

Рассмотрим вариант последней, когда $G$ есть мультипликативная группа простого поля $\mathbb{F}_p$, т. е. $|G| = n = p - 1$. Пусть также $\alpha$ — порождающий элемент $G$. Ясно, что мультипликативная группа $\mathbb{F}_p^*$ изоморфна группе $\mathbb{Z}_{p-1}$ по сложению. Например,

$$\mathbb{F}_{11}^* = \langle \{1, \ldots, 10\}, \cdot \rangle \cong \mathbb{Z}_{10} = \langle \{0, \ldots, 9\}, + \rangle.$$

Для организации обмена шифротекстами Алиса и Боб выбирают в $G$ каждый по своему секретному ключу — $x_A$ и $x_B$ из диапазона $[\,2,\ p-2\,]$ и вычисляют значения

[19] Тахер Эль-Гамаль (1955) — американский криптограф египетского происхождения.

$$d_A = \alpha^{x_A} \text{ и } d_B = \alpha^{x_B}.$$

Открытыми ключами, которыми обмениваются Алиса и Боб, являются тройки $(p, \alpha, d_A)$ и $(p, \alpha, d_B)$.

Пусть Алиса хочет передать Бобу сообщение $M \in \mathbb{F}_p^*$. Для этого она выбирает ещё одно случайное число $s \in [\,2,\, p-2\,]$, *называемое сеансовым ключом*, и вычисляет по $\bmod p$ пару чисел

$$a = \alpha^s \text{ и } b = M \cdot (d_B)^s,$$

которые передаёт по открытому каналу, то есть $(a, b)$ — шифртекст. Поэтому длина шифртекста в схеме Эль-Гамаля длиннее исходного сообщения $M$ вдвое.

Для расшифрования криптограммы Боб вычисляет по $\bmod p$

$$M = b \cdot (d_B)^{-s} = b \cdot (\alpha^{x_B})^{-s} = b \cdot (\alpha^s)^{-x_B} = b \cdot a^{p-1-x_B}.$$

Считается, что стойкость криптосистемы Эль-Гамаля равна стойкости системы RSA при той же длине ключа.

*Пример* 4.6. Алиса передаёт Бобу своё сообщение $t = BUJ$, используя шифрсистему Эль-Гамаля.

Вычисление ключей. Боб

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 $(p,\, \alpha,\, d_B) = (2\,357,\ 2,\ 1\,185)$.

Зашифрование. Алиса

1) получает открытый ключ Боба;

2) представляет свой текст $t = BUJ$ в виде натурального числа из $[0,\, p-1]$ с помощью 27-ричной системы счисления числом
$$M = \underbrace{2}_{B}\cdot 27^2 + \underbrace{21}_{U}\cdot 27^1 + \underbrace{10}_{J} = 2\,035;$$

3) выбирает случайный сеансовый ключ $s = 1520 \in [2,\, p-2]$;

4) вычисляет по $\bmod 2\,357$ 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.

Расшифрование. Боб

1) получает криптограмму от Алисы;

2) вычисляет значение
$$a^{p-1-x_B} = 1\,430^{605} \equiv_{2\,357} 872$$
и получает $M = 872\cdot 697 \equiv_{2\,357} 2\,035$;

3) представляет $M$ в 27-ричной системе счисления: $M = 2\,035_{10} = (2\ 21\ 10)_{27}$ и получает исходный текст $t = BUJ$.

На практике для криптографической стойкости простое число $p$ задается двоичным числом с $1\,024$ и более бит.

**Алгоритм согласования.** Рассмотрим уравнение

$$a^x \equiv_p b \tag{4.6}$$

в мультипликативной группе простого поля Галуа $G = \mathbb{F}_p^*$, где $p$ — простое число. Будем предполагать, что $a$ — примитивный элемент группы $G$, т. е. $\operatorname{ord} a = p - 1$.

С помощью перебора можно решить уравнение (4.6) за $O(p)$ арифметических операций.

Известна формула

$$\log_a b \equiv \sum_{j=1}^{p-2} (1 - a^j)^{-1} \cdot b^j \qquad (\mathrm{mod}\ p-1),$$

однако сложность вычисления по ней хуже, чем для простого перебора.

*Алгоритм согласования* решения уравнения (4.6)

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 $c^u \equiv_p b \cdot a^v$ 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 $x \equiv_{p-1} Hu - v$, где $u \in [\ 1,\ H\ ]$, $v \in [\ 0,\ H\ ]$. Действительно, набор из $H(H+1)$ чисел вида

$$\begin{aligned} &H,\ H-1,\ H-2,\ \ldots,\ H-H=0,\\ &\qquad 2H,\ 2H-1,\ \ldots,\ 2H-H,\\ &\qquad\qquad H^2,\ H^2-1,\ \ldots,\ H^2-H \end{aligned}$$

содержит в себе, в частности, все числа $0,\ 1,\ \ldots,\ p-2$, поскольку $H^2 > p$.

Заметим, что на практике после выполнения Шагов 3 и 4 полезно проводить упорядочение таблиц по возрастанию выходных значений.

Поскольку набор из $N$ элементов можно упорядочить за $O\left(N \log N\right)$ операций, оценка сложности алгоритма согласования — $O\left(\sqrt{p} \cdot \log p\right)$ арифметических операций.

*Пример* 4.7. Решим уравнение

$$6^x \equiv_{11} 8.$$

Имеем $p = 11,\ a = 6,\ b = 8$.

1) $H = \left\lceil \sqrt{11} \right\rceil = 4$.

2) $6^4 = 1\,296 \equiv_{11} 9 = c \quad (1\,296 = 117 \cdot 11 + 9)$.

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) $v = 0, 1, \ldots, 4$

| $v$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $6^v$ | 1 | 6 | 36 | 216 | 1 296 |
| $8 \cdot 6^v$ | 8 | 48 | 288 | 1 728 | 10 152 |
| $8 \cdot 6^v \pmod{11}$ | 8 | 4 | 2 | 1 | 9 |

5) Совпал элемент 4 таблиц при $u = 2$ и $v = 1$. Отсюда $Hu - v = 4 \cdot 2 - 1 = 7 \pmod{10}$.

Ответ: $x = 7$. Убедимся: $6^7 = 279\,936 = \underbrace{25\,448 \cdot 11}_{279\,928} + 8$.

Известны некоторые усовершенствования алгоритма согласования, но все они также имеют экспоненциальную сложность. Разработаны и другие алгоритмы дискретного логарифмирования, основанные на различных идеях.

**Алгоритм Полига–Хеллмана.** В этом разделе будем пользоваться обозначением

$$\mathbb{Z}_n^* = \{\, a \in \mathbb{Z} \mid \text{НОД}(a, n) = 1 \,\},$$

то есть $\mathbb{Z}_n^*$ — множество элементов кольца $\mathbb{Z}_n$, обратимых по умножению.

Пусть $G = \mathbb{Z}_n^*$ и известно примарное разложение $n = |G|$. Для данного $b \in G = \langle a \rangle$ нужно вычислить $\log_a b = y$, то есть решить уравнение

$$a^y \equiv_n b.$$

*Алгоритм Полига–Хеллмана*

1) Для каждого простого $p$, делящего $n$, составляем таблицу чисел

$$a(p, j) = a^{j \frac{n}{p}}, \quad j = 0, \ldots, p-1. \qquad (*)$$

2) Для каждого простого $p_i \mid n$ находим $y_i = \log_a b \pmod{p_i^\alpha}$. Пусть $p_i = p$, $\alpha_1 = \alpha$ и

$$x = \log_a b = x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1} \pmod{p^\alpha},$$

где $0 \leqslant x_i \leqslant p-1$.

Если $y = x \pmod{p^\alpha}$, то $y = x + vp^\alpha$. Поэтому $b^{\frac{n}{p}} = (a^y)^{\frac{n}{p}} = a^{\frac{(x+vp^\alpha)n}{p}} = a^{\frac{xn}{p}}$ и

$$b_0^{\frac{n}{p}} = a^{\frac{x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1}}{p}} = a^{\frac{x_0 n}{p}}.$$

Теперь с помощью таблицы, полученной на первом шаге находим $x_0$. Положим $c_1 = ba^{-x_0}$. Далее рассмотрим соотношение

$$b_1^{\frac{n}{p^2}} = \left(ba^{-x_0}\right)^{\frac{x_1 n}{p}}.$$

По таблице $(*)$ находим $x_1$. Если уже вычислены $x_0, \ldots, x_{i-1}$ то положим

$$c_i = ba^{-x_0 - x_1 p - \ldots - x_{i-1} p^{i-1}}.$$

Далее вычисляем $c^{\frac{n}{p^{i+1}}}$ и по таблице $(*)$ определяем $x_i$. Таким образом, мы вычислим все компоненты $y_i$ дискретного логарифма элемента $b$ по модулю $p_i^{\alpha_i}$, $i = \overline{1,s}$.

3) Вычислив $y_i = \log_a b \pmod{p_i^{\alpha_i}}$, $i = \overline{1,s}$, находим $y = \log_a b \pmod{n}$ по китайской теореме об остатках из системы:

$$\left\{ y = y_i, \pmod{p_i^{\alpha_i}}, \quad i = 1, \ldots, s. \right.$$

*Пример* 4.8. Пусть $G = \mathbb{Z}_{81}^*$, $|G| = n = \varphi(3^4) = 2 \cdot 3^3 = 54$, $G = \langle 2 \rangle$. Требуется найти $\log_2 74$, то есть $a = 2$, $b = 74$.

Предварительно убеждаемся, что 2 — образующий элемент группы $G$.

1. Имеем $p_1 = 2$, $\alpha_1 = 1$, $p_2 = 3$, $\alpha_2 = 3$. Вычисляем

$$a(2,0) = 1,\ a(2,1) = 2^{27} \equiv_{81} -1,$$
$$a(3,0) = 1,\ a(3,1) = 2^{18} \equiv_{81} 28,$$
$$a(3,2) = 2^{36} \equiv_{81} 55.$$

2.1. $p = 2$. Находим $\lambda_0 = \log_2 74 \pmod 2$.

Имеем $\frac{n}{2} = 27 = 2^4 + 2^3 + 2^2 + 1$. Вычисляем

$$b^{\frac{n}{2}} = 74^{27} \cdot 74^8 \cdot 74^2 \cdot 74 \equiv -1 = a(2, \lambda_0)$$

Из Шага 1 следует, что $\lambda_0 = 1 = x_1$.

2.2. $p = 3$. Определяем
$\log_{3^3} 74 = \lambda_0 + \lambda_1 3 + \lambda_2 9 \pmod{27}$ и находим

$$b^{\frac{n}{3}} = 74^{18} \equiv_{81} 74^{16} \cdot 74^1 2 \equiv_{81} 70 \equiv_{81} 28 = a(3, \lambda_0).$$

Из Шага 1 получаем, что $\lambda_0 = 1$.

Далее, вычисляем

$$\left(b \cdot a^{-\lambda_0}\right)^{\frac{n}{p^2}} = (74 \cdot 2^{-1})^6 \equiv 37^6 =$$
$$= 37^2 \cdot 37^4 \equiv 55 = a(3, \lambda_1).$$

Из Шага 1 следует, что $\lambda_1 = 2$.

И наконец, вычисляем

$$\left(ba^{-\lambda_0-3\lambda_1}\right)^{\frac{n}{p^3}} = (74\cdot 2^{-7})^2 = (37\cdot 64^{-1})^2 = \\ = (37\cdot 19)^2 = 55^2 \equiv_{81} 28 = a(3,\lambda_2).$$

Из Шага 1 находим, что $\lambda_2 = 1$.

Таким образом, $x_2 \equiv_{27} \log_2 74 = 1+2\cdot 3+9 = 16$.

3. Вычисляем искомый логарифм $\log_2 74 \pmod{54}$. Для этого по китайской теореме об остатках находим решение системы:

$$\begin{cases} x \equiv 1 \pmod 2, \\ x \equiv 16 \pmod{27}. \end{cases}$$

Решение этой системы будет следующее:

$$\log_2 74 = 1\cdot 27\cdot 1 + 16\cdot 2\cdot 14 \equiv 43 \pmod{54},$$

что и является ответом.

*Пример* 4.9. Вычислить $\log_5 173$ в

$$G = \langle 5\rangle \subset \mathbb{Z}^*_{256}, \qquad |G| = 28^{8-2} = 64,$$
$$\log_5 173 = x_0 + x_1 2 + {}_2 2^2 + x_3 2^3 + x_4 2^4 + x_5 2^5,$$
$$x_i = ?,\ i = \overline{0,5}.$$

Шаг 1. Вычисляем $a(2,0) = 1$, $a(2,1) = 5^3 2 \equiv_{256} 129$.

Имеем

| $5^2$ | $5^4$ | $5^8$ | $5^{16}$ | $5^{32}$ |
|---|---|---|---|---|
| 25 | 113 | 225 | 1936 | 129 |

Шаг 2.0. Далее вычисляем $x_0$. Для этого вычислим

$$b^{\frac{n}{p}} = 173^{\frac{64}{2}} = 173^{32} \equiv_{256} 129.$$

Таблица промежуточных степеней числа 173 следующая:

| $173^2$ | $173^4$ | $173^8$ | $173^{16}$ | $173^{32}$ |
|---|---|---|---|---|
| -23 | 17 | 33 | 65 | 129 |

Таким образом, $a(2, x_0) = a(2, 1)$, то есть $x_0 = 1$.

Шаг 2.1. Далее вычисляем

$$b_1 = b \cdot a^{-x_0} = 173 \cdot 5^{-1} = 173 \cdot 205 \equiv_{256} 137$$

и

$$b_1^{\frac{n}{p^2}} = (137)^{16} \equiv_{256} 129 = a(2, x_1),$$

то есть $x_1 = 1$.

Шаг 2.2. Вычисляем

$$b_2 = ba^{-x_0 - px_1} = 173 \cdot 5^{-3} \equiv_{256} 137 \cdot 205^2 \equiv_{256} \equiv_{256} 137 \cdot 41 \equiv_{256} 241 \equiv_{256} -15$$

и

$$b_2^{\frac{n}{p^3}} = b_2^8 = (-15)^8 \equiv_{256} 225^4 = 129 = a(2, x_2).$$

Отсюда следует, что $x_2 = 1$.

Шаг 2.3. Вычисляем

$$b_3 = ba^{-x_0 - px_1 - p^2 x_2} = 173 \cdot 5^{-7} = (173 \cdot 5^{-3})5^{-4} \equiv_{256} 129$$

и $b_3^{\frac{n}{p^4}} = 129^4 \equiv_{256} = 1$.

Следовательно, $x_3 = 0$.

Шаг 2.4. Вычисляем

$$b_4 = ba^{-x_0 - px_1 - p^2 x_2 - p^3 x_3} \equiv_{256} b_3 \equiv_{256} 129$$

и

$$b_4^{\frac{n}{p^4}} \equiv_{256} 1, \; x_4 = 0.$$

Шаг 2.5.

$$b_5 = ba^{-x_0-px_1-p^2x_2-p^3x_3-p^4x_4} = b_3,$$

$$b_5^{\frac{n}{p^5}} \equiv_{256} 129.$$

Таким образом, $x_5 = 1$ и $\log_5 173 = 7 + 32 = 39$.

## 4.5 Задачи

4.1. Решить уравнения

а) $6^x \equiv_{11} 2$; б) $8^x \equiv_{11} 3$; в) $2^x \equiv_{13} 3$.

4.2. 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 $x_A = 5$, $x_B = 17$ и $x_C = 12$ соответственно.

Определить их открытые $X_A$, $X_B$ и $X_C$ и общие секретные ключи $K_{AB}$, $K_{AC}$ и $K_{BC}$.

4.3. 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 $y_2 = 03$.

4.4. Вычислить $\log_3 26$ в группе $G = \mathbb{Z}_{7^3}^*$.

4.5. В $\mathbb{Z}_{101}$ вычислить $\log_2 39$ двумя способами.

4.6. В $\mathbb{Z}_{37}$ вычислить $\log_2 24$.

# Решения задач

## 1. Группы, кольца, поля

1.1. (1) Да, (2) нет (противоположного элемента), (3) нет (устойчивости), (4) нет (ассоциативности), (5) нет (обратного у 0), (6) да, (7) да, (8) нет (ассоциативности), (9) да, (10) нет (обратных у всех), (11)–(16) да.

1.2. Любая циклическая 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.

1.7. *Ответ*: а) 200; б) 192; в) 432.

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

1.3. $\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k}\right) =$

$$= p_1^{\alpha_1 - 1}\varphi(p_1) \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_k) =$$
$$= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}\varphi(p_1) \cdot \ldots \cdot \varphi(p_k) =$$
$$= \frac{n}{p_1 \cdot \ldots \cdot p_k}(p_1 - 1) \cdot \ldots \cdot (p_k - 1) =$$
$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

1.4. (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.

1.5. По дистрибутивности

$$x \cdot (y+z) = x \cdot y + x \cdot z \Rightarrow x \cdot (0+0) = x \cdot 0 = x \cdot 0 + x \cdot 0 \Rightarrow$$
$$\Rightarrow x \cdot 0 = 0.$$

1.6. Нет! Хотя $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$, но $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$.

1.7. Множество векторов $V$ содержит нулевой вектор $\mathbf{0}$ и является, очевидно, абелевой группой по сложению, а операция $\times$ векторного умножения связана со сложением дистрибутивными законами

$$\boldsymbol{x}\times(\boldsymbol{y}+\boldsymbol{z})=\boldsymbol{x}\times\boldsymbol{y}+\boldsymbol{x}\times\boldsymbol{z},\ (\boldsymbol{y}+\boldsymbol{z})\times\boldsymbol{x}=\boldsymbol{y}\times\boldsymbol{x}+\boldsymbol{z}\times\boldsymbol{x}.$$

Кольцо $\langle V, +, \times, \mathbf{0}\rangle$ некоммутативно: $\boldsymbol{x}\times\boldsymbol{y}\neq\boldsymbol{y}\times\boldsymbol{x}$ и неассоциативно: $\boldsymbol{x}\times(\boldsymbol{y}\times\boldsymbol{z})\neq(\boldsymbol{x}\times\boldsymbol{y})\times\boldsymbol{z}$.

Однако в рассматриваемом кольце выполняются тождества, заменяющие, в некотором смысле коммутативность и ассоциативность:

$$\boldsymbol{x}\times\boldsymbol{y}=-\boldsymbol{y}\times\boldsymbol{x}\ \text{(антикоммутативность)},$$
$$(\boldsymbol{x}\times\boldsymbol{y})\times\boldsymbol{z}+(\boldsymbol{y}\times\boldsymbol{z})\times\boldsymbol{x}+(\boldsymbol{z}\times\boldsymbol{x})\times\boldsymbol{y}=\mathbf{0}\ \text{(тождество Якоби)}.$$

1.8. В кольце $\mathbb{Z}_6$ классы вычетов по идеалу $(3)=\{0,3\}$ суть

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

1.9. 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. *Ответ*: *a*) 1, *b*) 17, *c*) 382, *d*) 1.

2.2. Вычислять $x^{-1}$ в кольцах $\mathbb{Z}_n$ можно используя соотношение Безу (подбором коэффициентов или обобщённым алгоритмом Евклида). В некоторых очевидных случаях (напр. в пункте в)) можно обойтись без вычислений.

а) $1 = 2 \cdot 3 - 1 \cdot 5,\ 2 \cdot 3 = 1 + 1 \cdot 5,\ 2 \cdot 3 \equiv_5 1,\ 3^{-1} \equiv_5 2;$

Или

| | | | |
|---|---|---|---|
| 1 | 5 | 0 | |
| 2 | 3 | 1 | $q = 1$ |
| 3 | 2 | -1 | $q = 1$ |
| 4 | 1 | **2** | $q = 2 \quad (\ 2 \ldots)$ |
| 5 | 0 | | |

Таким образом, $3^{-1} = 2$.

б) $1 = 2 \cdot 14 - 3 \cdot 9,\ (-3) \cdot 9 = 1 - 2 \cdot 14,$
$(-3) \cdot 9 \equiv_{14},\ 9^{-1} = -3 = 11 \pmod{14};$

Или

| | | | |
|---|---|---|---|
| 1 | 14 | 0 | |
| 2 | 9 | 1 | $q = 1$ |
| 3 | 5 | -1 | $q = 1$ |
| 4 | 4 | 2 | $q = 1$ |
| 5 | 1 | **-3** | $q = 4 \quad (\ 4 \ldots)$ |
| 6 | 0 | | |

Таким образом, $9^{-1} = -3 \equiv_{14} = 11$.

в) $x \cdot 1 \equiv 1 \Rightarrow 1^{-1} = 1$ по любому модулю;
$1^{-1} \equiv_{118} 1;$

г) $1 = 2 \cdot 4 - 1 \cdot 7,\ 2 \cdot 4 = 1 + 1 \cdot 7,\ 2 \cdot 4 \equiv_7 1,$
$4^{-1} \equiv_7 2,\ 3 \cdot 4^{-1} = 3 \cdot 2 = 6 \pmod{7};$

д) $-3 \equiv_7 4$, в пункте г) вычислено $4^{-1} \equiv_7 2$, значит, $(-3)^{-1} = 4^{-1} = 2 \pmod 7$;

е) $1 = 2 \cdot 6 - 1 \cdot 11,\ 2 \cdot 6 = 1 + 1 \cdot 11,\ 2 \cdot 6 \equiv_{11} 1,$ $6^{-1} \equiv_{11} 2,\ 6^{-2} = (6^{-1})^2 = 2^2 = 4 \pmod{11}$;

ж) $1 = 3 \cdot 3 - 8,\ 3 \cdot 3 = 1 + 8,\ 3 \cdot 3 \equiv_8 1,$ $3^{-1} \equiv_8 3,\ 3^{-3} = (3^{-1})^3 = 3^3 = 27 = 3 \pmod 8$.

2.3. 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. Имеем

$$F = \mathbb{F}_2[x]/\big(x^2 + x + 1\big) = \{\, 0, 1 = \alpha^3, \alpha, \alpha + 1 = \alpha^2 \,\},$$

где $\alpha$ — порождающий элемент мультипликативной группы $F^*$. Поэтому

$$P = \prod_{i=1}^{3} (x - \beta_i) = (x+1)(x+\alpha)(x+\alpha+1) =$$
$$= (x+1)\left(x^2 + \alpha x + x + \alpha x + \alpha^2 + \alpha\right) =$$
$$= (x+1)\left(x^2 + x + \alpha^2 + \alpha\right) =$$

$$= \big(x^3 + (\alpha+1)x^2 + (\alpha+1)x^2 + (\alpha^2+\alpha+1)x + \\ + \alpha^2 + \alpha\big) = x^3 + 1,$$

и по теореме 2.4:

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

2.5. 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. 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. Это поле $\mathbb{F}_2^2$, оно может быть построено как факторкольцо $\mathbb{F}_2[x]/\,(a(x))$, где $a(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$ степени 2. Но такой многочлен только один: $x^2+x+1$.

Следовательно, $\mathbb{F}_2^2 = \{\,0,\,1,\,x,\,x+1\,\}$ и $x^2 = x+1$ (черту над элементами не пишем).

Таблицы сложения и умножения в построенном поле (операции с 0 опускаем):

| $+$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|
| $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x$ | $1$ | $0$ |

| $\times$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|
| $1$ | $1$ | $x$ | $x+1$ |
| $x$ | $x$ | $x+1$ | $1$ |
| $x+1$ | $x+1$ | $1$ | $x$ |

2.8. 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. Поле $F = \mathbb{F}_2[x]/\left(x^3+x+1\right)$ содержит 8 элементов: 0 и степени $1, \ldots, 7$ порождающего элемента $\alpha$. 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. 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. 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 $\frac{2\pi}{p}$, $2\frac{2\pi}{p}$, …, $2\pi$ 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. 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. 1) $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$, $(x-2) \equiv_5 (x+3)$

2)

$$\begin{array}{r|l} x^3 + 2x^2 + 4x + 1 & x + 3 \\ \cline{2-2} x^3 + 3x^2 & x^2 + 4x + 2 \\ \cline{1-1} \quad 4x^2 + 4x & \\ \quad 4x^2 + 2x & \\ \cline{1-1} \quad\quad 2x + 1 & \\ \quad\quad 2x + 1 & \\ \cline{1-1} \quad\quad\quad 0 & \end{array}$$

3) Перебором убеждаемся, что многочлен $x^2+4x+2$ неприводим в $\mathbb{F}_5$.

*Ответ*: $x^3 + 2x^2 + 4x + 1 = (x+3)\left(x^2 + 4x + 2\right)$.

2.14. 1) $0, 1, 2$ — не корни $f(x) \Rightarrow f(x)$ линейных делителей не содержит.

2) Неприводимые многочлены над $\mathbb{F}_3$ степени 2:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2.$$

3) Подбором получаем
*Ответ*: $f(x) = x^4 + x^3 + x + 2 = \left(x^2 + 1\right)\left(x^2 + x + 2\right)$.

2.15. 1. $f(x) \neq 0$ ни при каком $x = 0, 1, 2, 3, 4$, то есть $f(x)$ не имеет линейных делителей.

2. Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем

*Ответ*: $f(x) = \big(x^2 + x + 1\big)\,\big(x^2 + 2x + 4\big)$.

2.16. 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. Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0$.

$$\begin{aligned} f_1(x) &= x^3 + 2x + 1, \\ f_2(x) &= x^3 + 2x + 2, \\ f_3(x) &= x^3 + x^2 + 2, \\ f_4(x) &= x^3 + 2x^2 + 1, \\ f_5(x) &= x^3 + x^2 + x + 2, \\ f_6(x) &= x^3 + x^2 + 2x + 1, \\ f_7(x) &= x^3 + 2x^2 + x + 1, \\ f_8(x) &= x^3 + 2x^2 + 2x + 2. \end{aligned}$$

2.18. 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. $a(x) = x^2+x-1$, $a(0)=6$, $a(1)=1$, $a(2)=5$, $a(3)=4$, $a(4)=6$, $a(5)=1$, $a(6)=6$, то есть многочлен $a(x)$ — *неприводим* в $\mathbb{F}_7$ и $F$ — поле ($\cong \mathbb{F}_7^2$).

2. $\mathbb{F}_7^2 = \big\{\, ax+b \mid a,b \in \mathbb{F}_7,\ x^2 = 1-x = 6x+1 \,\big\}$

$$(ax+b)\cdot(6x+1) = \ldots = (2a+6b)x + (6a+b) = 1$$

$$\begin{cases} 6a+b &= 1 \\ a+3b &= 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

*Ответ*: $(1-x)^{-1} = x+2$ в $F$.

2.20. $\beta = x + x^2 = x(x+1)$.

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. $\underline{x^4 = x+1}$

$$\beta^2 = x^2(x+1)^2 = x^4 + x^2 = x^2 + x + 1,$$
$$\beta^3 = x(x+1)\left(x^2+x+1\right) = x\left(x^3+1\right) = x^4 + x = x + 1 + x = 1.$$

*Ответ*: В поле $F_1$ $\operatorname{ord}\beta = 3$.

2. $\underline{x^4 = x^3 + 1}$

$$\begin{aligned}
\beta^2 &= x^4 + x^2 = x^3 + x^2 + 1,\\
\beta^3 &= x(x+1)\left(x^3 + x^2 + 1\right) =\\
&= x\left(x^4 + x^2 + x + 1\right) = x\left(x^3 + x^2 + x\right) =\\
&= x^4 + x^3 + x^2 = x^2 + 1 \neq 1,\\
\beta^5 &= x^2 x^3 = \left(x^3 + x^2 + 1\right)\left(x^2 + 1\right) =\\
&= \left(x^5 + x^4 + x^2 + x^3 + x^2 + 1\right) = \ldots\\
\ldots &= \left(x^3 + 1\right) x = x^4 + x = x^3 + x + 1 \neq 1.
\end{aligned}$$

*Ответ*: В поле $F_2$ $\operatorname{ord}\beta = 15$.

2.21. Мультипликативная группа поля

$$\mathbb{F}_2[x]/\left(x^6 + x^3 + 1\right)$$

состоит из $2^6 - 1 = 63$ элементов.

Простые делители $63 = 3^2 \cdot 7$ суть 3 и 7, поэтому равенство $x^d = 1$ нужно проверить только для $d = 21 = \frac{63}{3}$ и $d = 9 = \frac{63}{7}$.

В рассматриваемом поле $x^6 = x^3 + 1$ и

$$x^9 = x^6 x^3 = \left(x^3 + 1\right) x^3 = x^6 + x^3 = \not{x}^3 + 1 + \not{x}^3 = 1.$$

Т.о. $\operatorname{ord} x = 9 \neq 63$ и многочлен $f(x)$ *не примитивен.*

2.22.

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

1. $\underline{((7)) \text{ над } \mathbb{F}_2}$

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

$((1)) = 2$: 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. $\operatorname{char} F = 3$, поэтому $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

$F = \mathbb{F}_3^2$, $F^*$ содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1,8}$ примитивного элемента $\alpha$.

Если элемент $x$ окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в $\mathbb{F}_3^2$ проводятся по $\bmod a(x)$, будем иметь

$$x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1.$$

Найдём порядок элемента $x$: т. к. $8 = 2^3$, $\frac{8}{2} = 4$, проверим равенство $x^4 = 1$:

$$x^4 = \left(x^2\right)^2 = (2x+1)^2 = x^2 + x + 1 = \cancel{2}x + 1 + \cancel{x} + 1 = 2 \neq 1,$$

то есть $x$ — примитивный элемент $F$: $\operatorname{ord} x = 8$, $x^8 = 1$.

*Повезло*: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над $\mathbb{F}_3$, иначе примитивный элемент поля $F$ пришлось бы искать.

Теперь вычислим значение заданного выражения. Имеем $2^8 = 256 \equiv_3 1$, $x + 2 = -x^2$, $x^4 = 2$ и далее:

$$S = \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} + \frac{x^7}{x^9x^2} = \frac{x^8}{x^2} + \frac{x^7x^8}{x^{11}} =$$
$$= x^6 + x^4 = \left(x^2\right)^3 + 2 = (2x+1)^3 + 2 = 2x^3 + \not{1} + \not{2} =$$
$$= 2x(2x+1) = x^2 + 2x = 2x + 1 + 2x = x + 1.$$

2.24. В данном 9-элементном поле

$$x^2 + 1 = 0 \;\Rightarrow\; x^2 = -1 \equiv_3 2.$$

1. Найдём порядок элемента $x$, для чего проверим равенство $x^4 = 1$ (т. к. $9 - 1 = 8 = 2^3$, $\frac{8}{2} = 4$):

$$x^4 = \left(x^2\right)^2 = 4 \equiv_3 1.$$

Следовательно $\operatorname{ord} x = 4$ и элемент $x$ не является генератором группы $F^*$ (и $x^2 + 1$ — не есть примитивный многочлен над $\mathbb{F}_3$:
$x^4 - 1 = x^4 + 2 = \left(x^2 + 1\right)\left(x^2 + 2\right)$).

2. Проверим на примитивность элемент $x + 1$:

$$(x+1)^4 = (x+1)(x+1)^3 = (x+1)\left(x^3+1\right) =$$
$$= (x+1)(2x+1) = 2x^2 + \not{x} + \not{2}x + 1 = 4 + 1 = 2 \neq 1$$

то есть $\alpha = x + 1$ оказался примитивным элементом. Его степени:

$$\alpha^1 = x + 1, \qquad \alpha^5 = 2(x+1) = 2x + 2,$$
$$\alpha^2 = x^2 + 2x + 1 = 2x, \qquad \alpha^6 = \alpha^2 \cdot \alpha^4 = 4x = x,$$
$$\alpha^3 = 2x(x+1) = 2x + 1, \qquad \alpha^7 = x(x+1) = x + 2,$$
$$\alpha^4 = 4x^2 = x^2 = 2, \qquad \alpha^8 = (\alpha^4)^2 = 4 = 1.$$

*Замечание*: вычисление очередной степени $\alpha^{i+j}$ часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

2.25. 1. Сначала проверим, является ли многочлен $f(x) = x^2 + x + 2$ делителем $x^4 + 1$?

$$x^4 + 1 \;=\; \big(x^2 + x + 2\big) \cdot \big(x^2 + 2x + 2\big) \quad \text{— да, является}$$

Поэтому искомый идеал составят многочлены из $R$, кратные $f(x)$:

$$\big(x^2 + x + 2\big) = \left\{ \big(x^2 + x + 2\big)\,(ax + b) \mid a, b \in \mathbb{F}_3, x^4 = 1 \right\}.$$

2. Проведём умножение:

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

Теперь, перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $\big(x^2 + x + 2\big)$:

| $a$ | $b$ | $ax^3 + (a+b)x^2 + (2a+b)x + 2b$ |
|---|---|---|
| 0 | 0 | $0$ |
| 0 | 1 | $x^2 + x + 2$ |
| 0 | 2 | $2x^2 + 2x + 1$ |
| 1 | 0 | $x^3 + x^2 + 2x$ |
| 1 | 1 | $x^3 + 2x^2 + 2$ |
| 1 | 2 | $x^3 + x + 1$ |
| 2 | 0 | $2x^3 + 2x^2 + x$ |
| 2 | 1 | $2x^3 + 2x + 2$ |
| 2 | 2 | $2x^3 + x^2 + 1$ |

А если бы $f(x) \not| a(x)$? Тогда в $R$ существует идеал, порождённый элементом НОД $(f(x), a(x))$.

2.26. Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ с учётом $x^2 = 2x + 2$:

$$\begin{aligned} \det M &= (3x+4)(3x+2) - (x+2)(x+3) = \\ &= 4x^2 + 3x + 3 - x^2 - 1 = \\ &= 3x^2 + 3x + 2 = 3(2x+2) + 3x + 2 = 4x + 3. \end{aligned}$$

2. Найдём обратный к $4x + 3$ элемент, решая соотношение Безу

$$\left(x^2 + 3x + 3\right) a(x) + (4x+3)b(x) = 1$$

с помощью обобщённого алгоритма Евклида:

Шаг 0. // *Инициализация*

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

Шаг 1. // *Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком*

$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x) + r_0(x), \\ q_0(x) &= 4x + 4, \\ r_0(x) &= 1, \ // \ \deg r_0 = 0 \Rightarrow \mathit{OCTAHOB} \\ y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = \\ &= -q_0(x) = -4x - 4 = x + 1. \end{aligned}$$

3. Вычислим обратную матрицу

$$M^{-1} = (x+1)\begin{pmatrix} 3x+2 & 4x+2 \\ 4x+3 & 3x+4 \end{pmatrix} = \begin{pmatrix} x+2 & 1 \\ 4x & 3x \end{pmatrix}.$$

2.27. 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

$$f(x) = \big(x^2 + x + 1\big) \times \\ \times (\underbrace{x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1}_{g(x)}).$$

Делим частное $g(x)$ на $x^2 + x + 1$:

$$g(x) = x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ = \big(x^2 + x + 1\big) \cdot \big(x^7 + x^4 + x^3 + x^2 + x + 1\big) + x$$

— не делится нацело, то есть $x^2 + x + 1$ — делитель $f(x)$ кратности 1.

3. Неприводимых многочленов 3-й степени над $\mathbb{F}_2$ только два: $x^3 + x + 1$ и $x^3 + x^2 + 1$.
Пробуем поделить $g(x)$ на $x^3 + x + 1$:

$$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ = \big(x^3 + x + 1\big)\,(\underbrace{x^6 + x^5 + x^3 + x^2 + 1}_{h(x)}) \quad \text{— делится!}$$

Производя далее попытки деления $h(x)$ на неприводимые многочлены 3-й степени, получаем

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

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

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. 1. Найдём разложение многочлена $f(x)$ на *неприводимые* множители над $\mathbb{F}_3$.

- Ищем корни: $f(0)=2,\ f(1)=1,\ f(2)=0$. Поскольку $x-2 \;\equiv_3\; x+1$, то $f(x) = (x+1)\left(x^2+2x+2\right)$.
- Многочлен $g(x)=x^2+2x+2$ не имеет корней в $\mathbb{F}_3$, его степень 2, т. е. он неприводим.
- Окончательно: $f(x)=(x+1)\left(x^2+2x+2\right)$.

2. Известно, что если $g(x)$ — неприводимый многочлен степени $n$ над $\mathbb{F}_p$, то он:

- в поле своего расширения $F=\mathbb{F}_p[x]/(g(x))$ раскладывается на $n$ линейных множителей —

$$g(x) \;=\; (x-\alpha)\cdot(x-\alpha^p)\cdot\left(x-\alpha^{p^2}\right)\cdot\ldots\cdot\left(x-\alpha^{p^{n-1}}\right),$$

  где $\alpha$ – 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 $\alpha$ — корень $g(x)$, то и $\alpha^3$ — тоже его корень. Вычисляем:

$$\begin{aligned}\alpha^2 &= -2\alpha - 2 = \alpha + 1,\\ \alpha^3 &= \alpha(\alpha+1) = \alpha^2 + \alpha = 2\alpha + 1\end{aligned}$$

Построенное поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ содержит найденный ранее корень 2, поэтому многочлен $f(x)$ в этом поле раскладывается на следующие линейные множители:

$$f(x) = x^3 + x + 2 = (x-2)(x-\alpha)(x-2\alpha-1) = (x+1)(x+2\alpha)(x+\alpha+2).$$

4. Определить корни многочлена

$$g(x) = (x-\alpha)(x-2\alpha-1)$$

в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ легко: всегда можно взять $\alpha = x$, откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

*Ответ*: многочлен $f(x) = x^3 + x + 2$ имеет корни 2, $x$, $2x + 1$ в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right) = GF(3^2)$.

2.29. $\beta \in \{\, 0,\, 1,\, \alpha,\, \ldots,\, \alpha^{14} \,\} = F, \quad x^4 = x + 1.$

$\beta = 0$: $m_0(x) = x$.

$\beta = 1$: $m_1(x) = x + 1$.

$\beta = \alpha$: сопряжённые с $\alpha$ элементы — $\alpha^2$, $\alpha^4$, $\alpha^8$ 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 $\alpha^3$ элементы суть $\alpha^6$, $\alpha^{12}$, $\alpha^{24} = \alpha^9$, их м. м. —

$$m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = \\ = x^4 + \left(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\right)x^3 + \\ + \left(\alpha^3\alpha^6+\alpha^3\alpha^9+\alpha^3\alpha^{12}+\alpha^6\alpha^9+\alpha^6\alpha^{12}+\alpha^9\alpha^{12}\right)x^2 + \\ + \left(\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^9\alpha^{12}+\alpha^6\alpha^9\alpha^{12}\right)x + \\ + \left(\alpha^3\alpha^6\alpha^9\alpha^{12}\right) = x^4 + \left(\alpha^3 + (\alpha^3+\alpha^2) + (\alpha^3+\alpha) + \right. \\ \left. + (\alpha^3+\alpha^2+\alpha+1)\right)x^3 + (\ldots)\,x^2 + (\ldots)\,x + \alpha^{30} = \\ = x^4 + x^3 + x^2 + x + 1.$$

$\beta = \alpha^5$: единственный сопряжённый с $\alpha^5$ элемент — $\alpha^{10}$ (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 $\alpha^7$ элементы — $\alpha^{14}$, $\alpha^{28} = \alpha^{13}$, $\alpha^{56} = \alpha^{11}$, 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. 1. Любой многочлен в поле характеристики 5 вместе с корнем $\alpha^3$ содержит все сопряжённые с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т. д.

2. В поле $F$ имеем $\alpha^{5^2-1} = \alpha^{24} = 1$, и сопряжённым с $\alpha^3$ будет только элемент $\alpha^{15}$, т. к. $\alpha^{75} = \alpha^3$. Поэтому минимальный многочлен элемента $\alpha^3$ — 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. 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 $|F_2^*| = 2^4-1 = 15 = 3\cdot5$, то для определения значения $\operatorname{ord} x$ нужно проверить на равенства $x^3 = 1$ и $x^5 = 1$.

Первое равенство явно не имеет места, поэтому вычисляем с учётом $x^4 = x^3+x^2+x+1$:

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

Это означает, что $\operatorname{ord} x = 5 \neq 15$, $x$ — *не есть примитивный элемент* $F$, а м.м. $a(x)$ не примитивен.

2.32. 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 $f_1(x) = x - 3$ (или на $x+2$), получим $x^3+3x^2+4x+4 = (x-3)\cdot\left(x^2 + x + 2\right)$.

Перебором элементов $x \in GF(5)$ убеждаемся, что $f_2(x) = x^2 + x + 2$ — неприводимый многочлен.

В поле $\mathbb{F}_5[x]/\left(x^2 + x + 2\right)$ корни многочлена $f_2(x) = 0$ суть $\left\{ x,\, x^5 \right\}$ 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*: $\{\, 3,\, x,\, 4x + 4 \,\}$.

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

2.34. Поскольку $n = 40 = 5 \cdot 8$, то корни бинома $x^{40}-1$ суть все корни $x^8-1$ (они все различны), но 5-й кратности.

Рассмотрим разложение многочлена $x^8-1$ над $\mathbb{F}_5$. Относительно умножения на 5 вычеты по модулю 8 $\{\,\overline{0}, \overline{1}, \ldots, \overline{7}\,\}$ разбиваются на орбиты:

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

Пояснение: $5 \cdot 5 = 25 \equiv_8 1$, $2 \cdot 5 = 10 \equiv_8 2$ и т. д.

Поэтому:

- бином $x^8-1 \in \mathbb{F}_5[x]$ разлагается в произведение четырёх линейных и двух неприводимых квадратных многочленов;
- бином $x^{40}-1 = \left(x^8-1\right)^5$ разлагается в произведение двадцати многочленов степени 1 (четырёх кратности 5 каждый) и десяти неприводимых многочленов степени 2 (двух кратности 5 каждый);
- максимальная степень неприводимых делителей-многочленов есть 2, следовательно полем расширения данного бинома будет $\mathbb{F}_5^2$.

*Замечание.* В данном случае разложение бинома $x^8-1 \in \mathbb{F}_5[x]$ на неприводимые множители легко находится (первые три равенства справедливы в любом кольце):

$$x^8-1 = \left(x^4-1\right)\left(x^4+1\right),$$
$$x^4-1 = \left(x^2-1\right)\left(x^2+1\right),$$
$$x^2-1 = (x-1)(x+1),$$
$$x^2+1 \equiv_5 x^2-4 = (x-2)(x+2),$$
$$x^4+1 \equiv_5 x^4-4 = \left(x^2-2\right)\left(x^2+2\right).$$

Итого в $\mathbb{F}_5[x]$ :

$$x^8-1 = (x+1)(x-1)(x+2)(x-2)\left(x^2+2\right)\left(x^2-2\right).$$

И далее

$$x^{40}-1 = (x+1)^5(x-1)^5(x+2)^5(x-2)^5\left(x^2+2\right)^5\left(x^2-2\right)^5.$$

2.35. $\deg f(x) = 2$ 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 $x^5$.

2.36. Вычисляем значения $f(x)$ для всех $x$ из $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$: $f(0) = 4$, $f(1) = 1$, $f(2) = 0$ и т. о. $x = 2$ — корень $f(x)$.

Деля «уголком» $f(x)$ на $f_1(x) = x-2 = x+3$, получим $2x^4+x^3+4x^2+4 = (x+3)\cdot(2x^3+4x+3)$.

Для удобства нормируем частное $2x^3+4x+3$: т. к. $2^{-1}=3$, то вместо уравнения $2x^3+4x+3=0$ можно решать уравнение

$$f_2(x) \;=\; 3\cdot(2x^3+4x+3) \;=\; x^3+2x+4 \;=\; 0.$$

Перебором элементов $x\in\mathbb{F}_5$ —

$$f(0)\;=\;4,\;\; f(1)\;=\;2,\;\; f(2)\;=\;1,\;\; f(3)\;=\;2,\;\; f(4)\;=\;1,$$

убеждаемся, что $f_2(x)=x^3+2x+4$ — неприводимый многочлен[20)].

В поле $\mathbb{F}_5[x]/\big(x^3+2x+4\big)$ корнями многочлена $f_2(x)=0$ будут $x,\;x^5,\;x^{25}$.

Вычисляем — с учётом $x^3=-2x-4=3x+1$:

$$\begin{aligned} x^5 \;&=\; x^2(3x+1) \;=\; 3x^3+x^2 \;=\; 4x+3+x^2 \;= \\ &=\; x^2+4x+3; \\ x^{25} \;&=\; \big(x^5\big)^5 \;=\; \big(x^2+4x+3\big)^5 \;=\; x^{10}+4^5x^5+3^5 \;= \\ &=\; x^{10}+4\big(x^2+4x+3\big)+3 \;=\; x^{10}+4x^2+x. \end{aligned}$$

(поскольку $4^5=2^{10}=102\underline{4}$ и $3^5=81\cdot3=24\underline{3}$).

Найдём отдельно $x^{10}$:

$$\begin{aligned} x^{10} \;&=\; \big(x^5\big)^2 \;=\; \big(x^2+4x+3\big)^2 \;= \\ &=\; x^4+x^2+3^2+3x^3+4x+x^2 \;= \\ &=\; x^4+3x^3+2x^2+4x+4 \;= \\ &=\; 3x^2+\not{x}+\not{4}x+3+\not{2}x^2+4x+4 \;=\; 4x+2. \end{aligned}$$

Продолжаем:

[20)] а если бы это был многочлен 4-й степени?

$$x^{25} = x^{10} + 4x^2 + x = \not{4}x + 2 + 4x^2 + \not{x} = 4x^2 + 2.$$

*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 $2 \in F$).

2.37. В таблицах неприводимых многочленов данный многочлен отсутствует.

Подбором находим, что $f(x)$ разлагается в произведение двух неприводимых над $\mathbb{F}_2$ многочленов:

$$x^8+x^4+x^2+x+1 = \underbrace{\big(x^4 + x^3 + 1\big)}_{f_1(x)} \cdot \underbrace{\big(x^4 + x^3 + x^2 + x + 1\big)}_{f_2(x)}.$$

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

$x$, $x^2$, $x^3$, $x^3 + x^2 + x + 1$

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 $(=4)$ и поля $F_1$ и $F_2$ изморфны, т. о. все 8 корней уравне-ния $f(x) = 0$ лежат в поле $GF(2^4)$.

Для записи данных корней выберем представление $F_1$ поля $GF(2^4)$. Тогда запись корней $f_1(x)$ останется без изменений, а корни $f_2(x)$ надо представить как элементы $F_1$.

Приравнивая многочлены, порождающие данные поля, получим

$$x^4+x^3+1 = x^4+x^3+x^2+x+1 \;\Rightarrow\; x^2+x = x(x+1) = 0.$$

Ясно, что при подстановке $x \mapsto x+1$ полученное равенство останется справедливым. Применим данную подстановку для изоморфного преобразования полей $F_1 \leftrightarrow F_2$.

Находим представления корней многочлена $f_2(x)$ в поле $F_1$:

$$\begin{gathered} x \mapsto x+1, \\ x^2 \mapsto (x+1)^2 = x^2+1, \\ x^3 \mapsto (x+1)^3 = x^3+x^2+x+1, \\ x^3+x^2+x+1 \mapsto \left(x^3+x^2+x+1\right)+\left(x^2+1\right)+ \\ +(x+1)+1 = x^3. \end{gathered}$$

Проверим, что, например, $x^2+1$ — корень $f(x)$:

$$\begin{aligned} f\left(x^2+1\right) &= \left(x^2+1\right)^8+\left(x^2+1\right)^4+\left(x^2+1\right)^2+\left(x^2+1\right)+1 = \\ &= \left(x^{16}+1\right)+\left(x^8+1\right)+\left(x^4+1\right)+x^2. \end{aligned}$$

Очевидно $x^{16} = x$, $x^4 = x^3+1$ и $x^8 = \left(x^3+1\right)^2 = x^6+1$.

Поскольку $x^5 = x^4+x = x^3+x+1$, то $x^6 = x^4+x^2+x = x^3+x^2+x+1$ и $x^8 = x^3+x^2+x$.

Подставляя в выражение для $f\left(x^2+1\right)$ полученные полиномиальные представления степеней $x$, получим

$$f(x^2+1) \;=\; (x+1)+\left(x^3+x^2+x+1\right)+x^3+x^2 \;=\; 0.$$

*Ответ*: многочлен $f(x) = x^8+x^4+x^2+x+1 \in \mathbb{F}_2[x]$ имеет в поле $\mathbb{F}_2[x]/\left(x^4+x^3+1\right)$ корни $x$, $x^2$, $x^2+1$, $x^3$, $x^3+1$, $x^3+x^2+x$, $x+1$, $x^3+x^2+x+1$.

2.38. Поскольку $f(0) = f(1) = 2$, $f(2) = 1$, то $f(x)$ линейных делителей не имеет.

Проверим существование квадратичных:

$$f(x) = x^4+2x+2 = \left(x^2+ax+b\right)\left(x^2+cx+d\right) = \\ = x^4+cx^3+dx^2x+ax^3+acx^2+adx+bx^2+bcx+bd = \\ = x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd.$$

Отсюда

1) $c = -a$ и коэффициент при $x^2$ есть $b-a^2+d = 0$;
2) из $bd = 2$ следует, что либо $b = 1$ и $d = 2$, либо $b = 2$ и $d = 1$, то есть в любом случае $b+d = 3 = 0$;
3) но тогда из п. (1) $a^2 = 0$, то есть $a = c = 0$ и коэффициент при $x$ равен $0 \Rightarrow$ противоречие.

Т.о. полином $f(x)$ над $\mathbb{F}_3$ *неприводим*.

Теперь рассмотрим поле $\mathbb{F}_3[x]/\left(x^4+2x+2\right)$.

В нём $f(x) = x^4+2x+2 = 0$, то есть $x^4 = x+1 = 0$, и корни $f(x)$ суть $x$, $x^3$, $x^{3^2}$, $x^{3^3}$.

Вычислим $x^9$ и $x^{27}$:

$$x^9 = \left(x^4\right)^2 x = (x+1)^2x = x^3+2x^2+x;$$
$$x^{27} = \left(x^9\right)^3 = \left(x^3+2x^2+x\right)^3 = x^9+2x^6+x^3 = \\ = \ldots = x^3+x^2+x.$$

*Ответ*: полином $f(x) = x^4+2x+2$ имеет корни $x$, $x^3$, $x^3+2x^2+x$, $x^3+x^2+x$ в поле $\mathbb{F}_3[x]/(f)$.

2.39. Поскольку $f(0) = f(1) = 1$, полином $f(x)$ линейных делителей не имеет. Кроме того,

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

то есть полином $f(x)$ не имеет и (единственного) квадратичного неразложимого делителя и, поскольку его степень равна 5, то он *неприводим*.

Рассмотрим теперь поле $\mathbb{F}_2[x]/\left(x^5 + x^2 + 1\right)$. В нём $f(x) = x^5 + x^2 + 1 = 0$, то есть $x^5 = x^2 + 1 = 0$ и его корни суть $x$, $x^2$, $x^{2^2}$, $x^{2^3}$, $x^{2^4}$.

Вычислим $x^8$ и $x^{16}$:

$$\begin{aligned} x^8 \;&=\; x^5x^3 \;=\; \left(x^2+1\right)x^3 \;=\; x^5 + x^3 \;=\; x^3 + x^2 + 1; \\ x^{16} \;&=\; \left(x^8\right)^2 \;=\; \left(x^3 + x^2 + 1\right)^2 \;=\; x^6 + x^4 + 1 \;= \\ &=\; x^5x + x^4 + 1 \;=\; (x^3 + x) + x^4 + 1 \;= \\ &=\; x^4 + x^3 + x + 1. \end{aligned}$$

*Ответ*: в поле $\mathbb{F}_2[x]/\left(x^5 + x^2 + 1\right)$ уравнение

$$f(x) = x^5 + x^2 + 1 = 0$$

имеет корни $x$, $x^2$, $x^4$, $x^3 + x^2 + 1$, $x^4 + x^3 + x + 1$.

# 3. Коды, исправляющие ошибки

3.1. Проверочная матрица $H$ имеет размерность $3\times 7$, и код при длине $n=7$ содержит $m=3$ проверочных и $k=7-3=4$ информационных бит.

Порождающая матрица кода $G$, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_4 \end{bmatrix}$.

Матрицу $P$ можно получить, если привести проверочную матрицу $H$ к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, преобразуя *строки*:

$$\begin{bmatrix} 0&0&1&0&1&1&1 \\ 0&1&0&1&1&1&0 \\ 1&0&1&1&1&0&0 \end{bmatrix} \xrightarrow{(1)\leftrightarrow(3)} \begin{bmatrix} 1&0&1&1&1&0&0 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{bmatrix} \rightarrow$$

$$\xrightarrow{(1)+(3)\mapsto(1)} \begin{bmatrix} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{bmatrix}$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\boldsymbol{u}_1=[1101]^T$ и $\boldsymbol{u}_2=[1001]^T$:

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

Очевидно был задан $(7,4)$-код Хэмминга.

3.2. Для определения кодового расстояния найдём все кодовые слова:

$$v(x) = g(x)(ax^2+bx+c) = \left(x^6+x^3+1\right)\left(ax^2+bx+c\right) = \\ = ax^8+bx^7+cx^6+ax^5+bx^4+cx^3+ax^2+bx+c.$$

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 $u(x)$:

$$u(x) \;\mapsto\; v(x) = x^6u(x) + r(x),$$
$$x^6u(x) = x^6\left(x^2+x\right) = x^8+x^7.$$

Находим остаток $\deg r(x)$ от деления $x^6u(x)$ на $g(x)$:

$$\begin{array}{rr|l} x^8+x^7 & & x^6+x^3+1 \\ \cline{3-3} x^8 \quad +x^5 \quad +x^2 & & x^2+x \\ \cline{1-2} \quad x^7+x^5 \quad +x^2 & & \\ \quad x^7 \quad +x^4 \quad +x & & \\ \cline{1-2} \quad x^5+x^4+x^2+x & & \end{array}$$

Т. о. $r(x) = x^5+x^4+x^2+x$ и

$$v(x) = x^8+x^7+x^5+x^4+x^2+x \;\leftrightarrow\; [0\,1\,1\,0\,1\,1\,\underline{0\,1\,1}]^T.$$

3.3. Декодирование систематического кода Хэмминга можно провести делением принятого полинома на

порождающий: остаток от деления определяет синдром $s$ с учётом таблицы соответствий между полиномиальным и степенным представлением элементов рассматриваемого поля со с. 162):

Находим позицию $j$ ошибки.

1) $x^6+x^2+x \;=\; \bigl(x^3+x+1\bigr)^2+\underline{x+1},\; j=3.$

Действительно,

$$w(\alpha) \;=\; \alpha^6+\alpha^2+\alpha \;=\; (\alpha^3)^2+\alpha^2+\alpha \;= \\ =\; \alpha^2+1+\alpha^2+\alpha \;=\; \alpha+1.$$

2) $x^6+x^5+x^3+x^2+x \;= \\ =\; \bigl(x^3+x^2+x+1\bigr)\bigl(x^3+x+1\bigr) \;+ \\ \underline{x^2+x+1},\; j=5;$

Действительно,

$$w(\alpha) \;=\; \alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha \;= \\ =\; \alpha^2+1+\alpha^5+\alpha+1+\alpha^2+\alpha \;=\; \alpha^5.$$

3) $x^6+x^3+x^2+x \;=\; \bigl(x^3+x\bigr)\bigl(x^3+x+1\bigr)+\underline{0},$
т. е. ошибки не произошло.

3.4. Имеем $\alpha^{31}=1$ и разложение $F^*$ над $\mathbb{F}_2$ есть

$$\{1\},\{\alpha,\alpha^2,\alpha^4,\alpha^8\,\alpha^{16}\},\\ \{\alpha^3,\alpha^6,\alpha^{12},\alpha^{24},\alpha^{17}\},\{\alpha^5,\alpha^{10},\alpha^{20},\alpha^9,\alpha^{18}\},\\ \{\alpha^7,\alpha^{14},\alpha^{28},\alpha^{25},\alpha^{19}\},\{\alpha^{11},\alpha^{22},\alpha^{13},\alpha^{26},\alpha^{21}\},\\ \{\alpha^{15},\alpha^{30},\alpha^{29},\alpha^{27},\alpha^{23}\}.$$

3.5. Будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов данного поля со с. 47.

С её помощью вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \\
&= (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + (\alpha + 1) = \\
&= \alpha^3 + \alpha + 1 = \alpha^7, \\
s_2 &= w(\alpha^2) = \left(w(\alpha)\right)^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = \left(w(\alpha^2)\right)^2 = \alpha^{28} = \alpha^{13}.
\end{aligned}$$

Синдромный полином —

$$s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1.$$

Решим удовлетворяет соотношению Безу

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \quad \deg\lambda(x) \leqslant 2.$$

с помощью обобщённого алгоритма Евклида:

$$\begin{aligned}
\text{Шаг 0.}\quad & r_{-2}(x) = x^5, \\
& r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1, \\
& \sigma_{-2}(x) = 0, \\
& \sigma_{-1}(x) = 1. \\
\text{Шаг 1.}\quad & r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x), \\
& q_0(x) = \alpha^2 x, \\
& r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x, \\
& \sigma_0(x) = \sigma_{-2}(x) - \sigma_{-1}(x)q_0(x) = \\
& \qquad = -q_0(x) = \alpha^2 x.
\end{aligned}$$

Шаг 2.
$$\begin{aligned} r_{-1}(x) &= r_0(x)q_1(x) + r_1(x),\\ q_1(x) &= \alpha^{12}x + \alpha^5,\\ r_1(x) &= \alpha^{14}x^2 + 1,\\ &\deg r_1(x) = 2 \leqslant r,\\ \sigma_1(x) &= \sigma_{-1}(x) - \sigma_0(x)q_1(x) = \\ &= 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) = \\ &= \underbrace{\alpha^{14}x^2 + \alpha^7 x + 1}_{\text{полином локаторов ошибок}} = \sigma(x). \end{aligned}$$

3.6. Найдём корни (их 2, полином квадратный) полинома локаторов ошибок полным перебором.

Для вычислений удобно пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной в предыдущей задаче.

$$\begin{aligned} \sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3,\\ \sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\ \sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\ \sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\ \sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = \mathbf{0},\\ \sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\ \sigma(\alpha^7) &= \alpha^{16} + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\ \sigma(\alpha^8) &= \alpha^{18} + \alpha^{14} + 1 = \mathbf{0}. \end{aligned}$$

Дальше можно не вычислять: оба корня $\sigma(x)$ найдены. Итак, данный полином локаторов ошибок имеет корни $\alpha^5$ и $\alpha^8$. Определяем позиции ошибок:

$$-5 \equiv_{15} 10, \qquad -8 \equiv_{15} 7.$$

3.7. Имеем $n = 31 = 2^5 - 1$, $q = 5$, $d_c - 1 = 2r = 6$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни $\alpha$, $\alpha^2$, $\alpha^3$, $\alpha^4$, $\alpha^5$, $\alpha^6$, где $\alpha$ — 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 о разложение $F^*$ на классы на с. 188 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. 34 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[21)] есть соответствующие таблицы. В этих таблицах указано, что все эти многочлены являются примитивными, то есть все они могут быть выбраны в качестве порождающего поле полинома $a(x)$.

Положим $a(x) = x^5 + x^3 + 1$ (многочлен № 2) и тогда $g(x) = a(x)$, $\alpha^5 = \alpha^3 + 1$, $\alpha^{31} = 1$.

Определим, какие из остальных многочленов соответствуют циклотомическим классам для $\alpha^3$ и $\alpha^5$.

Имеем:

[21)] например, [2], Том 1, Таблица С.

*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,
$g_2(x) = x^5+x^3+x^2+x+1,\ g_{\alpha^5}(x) = x^5+x^4+x^3+x+1$
и порождающий многочлен для $(31, 16, 7)$-кода БЧХ есть

$$g(x) = g_1(x)\cdot g_2(x)\cdot g_3(x) =$$
$$= x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1,$$
$$\deg g(x) = m = 15,\ k = n-m = 16.$$

3.8. Для вычислений в поле $F$ нам понадобится таблица, уже построенная на с. 47.

Перебором найдём корни полинома ошибок

$$\sigma(x) = \alpha^6 x+\alpha^{15} = (\alpha^3+\alpha^2)\,x+1:$$
$$\sigma(\alpha) = \alpha^4+\alpha^3+1 = \alpha+1+\alpha^3 \neq 0;$$
$$\sigma(\alpha^2) = \alpha^5+\alpha^4+1 = \alpha^2+\alpha+\alpha+1+1 = \alpha^2 \neq 0;$$
$$\ldots\ldots$$
$$\sigma(\alpha^9) = \alpha^{12}+\alpha^{11}+1 =$$
$$= (\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+1 = \mathbf{0}.$$

Линейный полином $\sigma(x)$ имеет один корень $\alpha^9$, и поэтому позиция единственной ошибки есть $-9 \equiv_{15} 6$.

# 4. Алгебраические основы криптографии

4.1. Используем алгоритм согласования из п. 4.4.

(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) $8^4 = 4\,096 \equiv_{11} 4 = c$.

3) $u = 1, 2, 3, 4$

| $u$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $4^u$ | 4 | $4 \cdot 4 = 16$ | $5 \cdot 4 = 20$ | $9 \cdot 4 = 36$ |
| $4^u \pmod{11}$ | 4 | 5 | 9 | 3 |

4) $v = 0, \ldots, 4$

| $v$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $8^v$ | 1 | 8 | 64 | 512 | 4096 |
| $3 \cdot 8^v$ | 3 | | | | |
| $3 \cdot 8^v \pmod{11}$ | 3 | | | | |

5) Совпал элемент 4 таблиц при $u = 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 4 = 16 \equiv_{10} 6$.

Ответ: $x = 6$.

(в) $2^x \equiv_{13} 3$. Имеем $p = 13$, $a = 2$, $b = 3$.

1) $H = 4$.

2) $2^4 = 16 \equiv_{13} 3 = c$.

3) $u = 1, 2, 3, 4$

| $u$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $c^u$ | 3 | 9 | 27 | 3 |
| $c^u \pmod{13}$ | 3 | 9 | 1 | 3 |

4) $v = 0, \ldots, 4$

| $v$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $2^v$ | 1 | | | | |
| $3 \cdot 2^v$ | 3 | | | | |
| $3 \cdot 2^v \pmod{11}$ | 3 | | | | |

5) Совпал элемент 3 таблиц при $u = 1, 4$ и $v = 0$. Отсюда $Hu - v = 4 \cdot 1 = 4$, или $4 \cdot 4 \equiv_{12} 4$.

Ответ: $x = 4$.

4.2. Вычислить $\log_3 26$ в группе $G = \mathbb{Z}_{7^3}^*$

$7^3 = 343$.
Порядок $|G| = \varphi(7^3) = 6 \cdot 7^2 = 2 \cdot 3 \cdot 7^2 = 294$.
Определяем $a(p, i)$, для $p = 2, 3, 7$.

1. Для вычисления $a(p, i)$ предварительно вычисляем следующие величины по модулю 343:

$$3^2 = 9,\ 3^4 = 81,\ 3^8 = 44,\ 3^{16} = 221,\ 3^{32} = 135,$$
$$3^{64} = 46,\ 3^{128} = 58.$$

Получаем (все сравнения по mod 343):

$$a(2,0) = 1,\ a(2,1) = 3^{\frac{294}{2}} \equiv -1,$$
$$a(3,0) = 1,\ a(3,1) = 3^{98} \equiv 324,\ a(3,2) = 324^2 \equiv 18,$$
$$a(7,0) = 1,\ a(7,1) = 3^{42} \equiv 295,\ a(7,2) = 3^{84} \equiv 246,$$
$$a(7,3) \equiv 197,\ a(7,4) \equiv 148,\ a(7,5) \equiv 99,\ a(7,6) \equiv 50.$$

2.1. Находим $\log_3 26 \equiv_2 \lambda_0$.

Для этого вычисляем $b^{\frac{n}{2}} \equiv_2 -1$. Из Шага 1 следует, что $\lambda_0 = 1$.

2.2. Находим $\mu_0 \equiv_3 \log_3 26$.

Для этого вычисляем $b^{\frac{n}{3}} = a(3, \mu_0) \equiv 18$. Откуда следует, что $\mu_0 = 2$ (см. Шаг 1).

2.3 Находим $\log_3 26 \equiv_{7^2} \delta_0 + \delta_1 74$.

Для определения $\delta_0$ вычисляем $a(7, \delta_0) = 197$. Из этого сравнения вытекает, что $\delta_0 = 3$ (см. Шаг 1).

Вычисляем (сравнения по mod 343):

$$b_1 = ba^{-\delta_0} = 26 \cdot 27^{-1} \equiv 216 \cdot 26 \equiv 128.$$

Далее определяем $\delta_1$ из сравнения $a(7, \delta_1) = 99$. Из шага 1 следует, что $\delta_1 = 5$.

Таким образом, $\log_3 26 = 3 + 5 \cdot 7 = 38$.

3. Находим искомый логарифм $\log_3 26$ в группе $\langle 3 \rangle = \mathbb{Z}_{7^3}^*$ (сравнения по mod 294):

$$\log_3 26 \equiv 1 \cdot 147 \cdot 1 + 2 \cdot 98 \cdot 2 + 38 \cdot 6 \cdot 41 \equiv 185.$$

4.3.

$$X_A = 2^5 = 32 \equiv_{23} 9;$$
$$X_B = 2^{17} = 131\,072 \equiv_{23} 18;$$
$$X_C = 2^{12} = 4\,096 \equiv_{23} 2;$$
$$K_{AB} = X_A^{17} = 9^{17} = 16\,677\,181\,699\,666\,569 \equiv_{23} 3;$$
$$K_{AC} = X_A^{12} = 9^{12} = 282\,429\,536\,481 \equiv_{23} 9;$$
$$K_{BC} = X_B^{12} = 18^{12} = 1\,156\,831\,381\,426\,176 \equiv_{23} 18.$$

4.4. Определим модуль $n = pq = 11 \cdot 17 = 187$. При этом $e = 13$ взаимно просто с $p-1 = 10$ и $q-1 = 16$. Открытый ключ есть пара $(187, 13)$.

Определим секретный ключ $d$. 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** | $q = 4$ | ( 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. *Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н.* Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.

2. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. — М.: Мир, 1988.

3. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2006.

4. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

5. Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.

6. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.

7. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.