Лекция 1. Кольца, поля, многочлены, конечные поля.

Определение 1. Множество $(R, +, \cdot)$ с двумя бинарными операциями (*сложением* и *умножением*) называется *кольцом*, если выполнены следующие условия (аксиомы кольца):
1. $\forall a, b, c \in R,\ \ (a + b) + c = a + (b + c)$;
2. $\forall a, b \in R,\ \ a + b = b + a$;
3. $\exists 0 \in R : \forall a \in R, a + 0 = 0 + a = a$;
4. $\forall a \in R, \exists(-a) \in R : (-a) + a = a + (-a) = 0$;
5. $\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$; 6. $(b + c) \cdot a = b \cdot a + c \cdot a$ (дистрибутивность слева и справа).
Если сверх того выполняется аксиома *ассоциативности умножения*,

$$\forall a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

то кольцо R называется *ассоциативным*;
если выполнена аксиома *коммутативности умножения*

$$\forall a, b \in R,\ \ a \cdot b = b \cdot a,$$

то кольцо R называется *коммутативным*;
если в кольце R имеется *нейтральный элемента по умножению*, или *единица*, 1, удовлетворяющий условию

$$\forall a \in R,\ 1 \cdot a = a \cdot 1 = a,$$

то кольцо R называется *кольцом с единицей*.

В наших лекциях, если прямо не указано противное, слово "кольцо" означает ассоциативное коммутативное кольцо с единицей.

Определение 2. Элемент a кольца R называется *обратимым*, если существует такой элемент a^{-1}, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
Элемент a кольца R называется *делителем нуля*, если $a \neq 0$ и существует такой элемент $b \in R$, что $b \neq 0$, но $a \cdot b = 0$.

Определение 3. *Полем* называется ассоциативное коммутативное кольцо с $1 \neq 0$, в котором каждый ненулевой элемент обратим.

Примеры: поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, кольцо целых чисел $\mathbb{Z}$ и кольцо $F[x]$ многочленов над полем F (которые не являются полями), некоммутативное кольцо $M_n(F)$ квадратных матриц порядка $n > 1$ над полем F.

Предложение 1. *В произвольном (возможно, неассоциативном и некоммутативном) кольце R выполнено условие $\forall a \in R, a \cdot 0 = 0 \cdot a = 0$.*

Доказательство. Из равенства $0 + 0 = 0$ следует, что $a \cdot 0 + a \cdot = a \cdot 0$, откуда

$$0 = (a \cdot 0) + (-(a \cdot 0)) = (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) = a \cdot 0 + (a \cdot 0 + (-(a \cdot 0)) = a \cdot 0 + 0 = a \cdot 0.$$

Равенство $0 \cdot a = 0$ доказывается аналогично. □

Из последнего предложения следует, что в любом кольце выполнены обычные правила арифметики

$$-(-a) = a,\ a \cdot (-b) = (-a) \cdot b = -(a \cdot b); (-a) \cdot (-b) = a \cdot b.$$

Сумму $a + (-b)$ будем обозначать через $a - b$. Отметим, что, как и в элементарной математике, знак умножения обычно опускают.

Предложение 2. *В кольце R с единицей делитель нуля не может быть обратимым элементом.*

Доказательство. Предположим, что a — обратимый элемент и $ab = 0$. Тогда

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b.$$

□

Определение 4. Пусть $n > 1$ — целое число. Для любого целого числа m обозначим через $\mathrm{rem}_n(m)$ остаток от деления m на n, т.е. такое число $r \in \{0, 1, \ldots, n-1\}$, что $m = nq + r$ для некоторого целого числа q. На множестве $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ определим операции $[a] + [b] = [\mathrm{rem}_n(a+b)]$, $[a][b] = [\mathrm{rem}_n(ab)]$. Легко проверить, что $\mathbb{Z}_n$ — ассоциативное и коммутативное кольцо с нулевым элементом $[0]$ и единицей $[1]$.

Теорема 1. *Следующие условия эквивалентны:*
(1) кольцо $\mathbb{Z}_n$ является полем;
(2) в кольце $\mathbb{Z}_n$ нет делителей нуля;
(3) n — простое число.

Доказательство. (1)⇒(2). По предложению 2.
(2)⇒(3) Если n — составное число, то $n = ab$ для некоторых натуральных $a, b < n$. Имеем

$$[a][b] = [\mathrm{rem}_n(ab)] = [0].$$

(3)⇒(1). Пусть n — простое число. Зафиксируем элемент $[a] \neq [0]$ в кольце $\mathbb{Z}_n$ и рассмотрим множество произведений $U = \{[a][b] : [b] \neq 0, [b] \in \mathbb{Z}_n\}$. Заметим, что если $[b_1] \neq [b_2]$, то $[a]([b_1] - [b_2]) \neq 0$, поэтому число элементов множества U равно $n-1$. Следовательно, $[1] \in U$, т.е. $[a][b] = [1]$ для некоторого $[b] \in \mathbb{Z}_n$. □

Итак, для простого числа p кольцо $\mathbb{Z}_p$ — пример *конечного поля*. Далее мы покажем и другие примеры конечных полей.

Введём естественное обозначение $ka = \underbrace{a + a + \ldots + a}_{k \text{ раз}}$ для любого элемента a произвольного кольца и любого натурального числа k.

Теорема 2. *Пусть F — конечное поле с единицей 1. Тогда существует такое простое число p, что $p \cdot 1 = 0$, причем $k \cdot 1 \neq 0$ для любого $k \in \{1, 2, \ldots, p-1\}$.*

Доказательство. Рассмотрим множество всех элементов F вида $k \cdot 1$, где k пробегает множество всех натуральных чисел. Поскольку F конечно, для каких-то различных чисел k, l получим $k \cdot 1 = l \cdot 1$. Считая $k > l$, получим $(k-l) \cdot 1 = 0$, причём $k - l > 0$. Теперь пусть p — наименьшее натуральное число, для которого $p \cdot 1 = 0$ (такое число называется *характеристикой* поля F). Покажем, что p — простое число. Действительно, если $p = ab$, где $a < p$ и $b < p$, то $a \cdot 1 \neq 0$, $b \cdot 1 \neq 0$, но $(a \cdot 1)(b \cdot 1) = p \cdot 1 = 0$, что невозможно, так как в поле нет делителей нуля.

Второе утверждение теоремы следует из минимальности p. □

Теорема 3. *Пусть F — конечное поле, p — характеристика поля F. Тогда $|F| = p^r$ для некоторого натурального числа r.*

Доказательство. Сначала заметим, что элементы $0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1$ можно отождествить, соответственно, с элементами $[0], [1], \ldots, [p-1]$ поля $\mathbb{Z}_p$ (операции в обоих полях выполняются одинаково). Рассмотрим базис $b_1, \ldots, b_r$ поля F как векторного пространства над полем $\mathbb{Z}_p$. Тогда любой элемент поля F единственным образом представляется в виде линейной комбинации $\lambda_1 b_1 + \ldots + \lambda_r b_r$, где $\lambda_1, \ldots, \lambda_r \in \mathbb{Z}_p$, а число таких линейных комбинаций равно p^r, поскольку каждый коэффициент принимает p значений. □

Определение 5. Многочлен положительной степени над полем F называется *неприводимым*, если его нельзя разложить в произведение двух многочленов меньшей степени.

Теорема 4. *Любой многочлен положительной степени разлагается в произведение некоторого числа неприводимых многочленов.*

Доказательство. Действительно, если многочлен $f(x)$ неприводим, то доказывать нечего — $f(x)$ есть произведение из одного сомножителя. Если же $f(x)$ приводим, то $f(x) = g(x)h(x)$, где $g(x), h(x)$ — многочлены меньшей степени. Применяя то же рассуждение к каждому из сомножителей, получим либо искомое разложение, либо увеличим число сомножителей. Поскольку число сомножителей ограничено степенью многочлена $f(x)$, этот процесс остановится на некотором шаге. □

Через $\deg f(x)$ *мы будем обозначать степень многочлена* $f(x)$.

Теорема 5. *Пусть* $f(x), g(x) \in F[x]$ *и* $g(x) \neq 0$. *Тогда существуют единственные многочлены* $q(x)$ *и* $r(x)$ *такие, что*

$$f(x) = g(x)q(x) + r(x), \quad \text{где } r(x) = 0 \text{ или } \deg r(x) < \deg f(x). \tag{1}$$

Определение 6. Многочлен $r(x)$ из (1) называется *остатком* от деления $f(x)$ на $g(x)$. Мы будем использовать для остатка обозначение $\mathrm{rem}_g(f)$.

Замечание 1. Легко проверить тождества:

$$\mathrm{rem}_g(f_1 + f_2) = \mathrm{rem}_g(f_1) + \mathrm{rem}_g(f_2); \quad \mathrm{rem}_f(f_1 f_2) = \mathrm{rem}_g(\mathrm{rem}_g(f_1)\,\mathrm{rem}_g(f_2)).$$

Теорема 6. *Пусть* $0 \neq f(x), g(x) \in F[x]$. *Рассмотрим многочлен* $d(x)$ *наименьшей степени, представи́мый в виде суммы* $d(x) = u(x)f(x)+v(x)g(x)$. *Тогда* $d(x)$ *— наибольший общий делитель многочленов* $f(x)$ *и* $g(x)$.

Доказательство. Очевидно, что любой общий делитель многочленов $f(x)$ и $g(x)$ является делителем многочлена $d(x)$. Покажем, что $d(x)$ делит $f(x)$. Действительно, в противном случае $f(x) = d(x)q(x) + r(x)$, где $r(x) \neq 0$ и $\deg r(x) < \deg d(x)$. Но

$$r(x) = f(x) - q(x)d(x) = (1 - u(x)q(x))f(x) + (-q(x)v(x))g(x),$$

что противоречит минимальности степени многочлена $d(x)$. Аналогично, $d(x)$ делит $g(x)$. □

Определение 7. Если F и E — поля, причем F — подкольцо в E, то F называется *подполем* поля E, а E — *расширением* поля F. Если E имеет конечную размерность над F, то E называется *конечным* расширением поля F.

Теорема 7. *Если* F *— поле и* $f(x)$ *— многочлен положительной степени над* F, *то существует конечное расширение* E *поля* F, *в котором многочлен* $f(x)$ *имеет корень.*

Доказательство. Ясно, что достаточно доказать утверждение для случая, когда $f(x)$ — неприводимый многочлен со старшим коэффициентом 1. Если $\deg F(x) = 1$, доказывать нечего: такой многочлен имеет корень в F. Пусть $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$, где $n = \deg f(x) > 1$. Рассмотрим множество E всех многочленов вида $b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$, где $b_0, \ldots b_{n-1} \in F$. На этом множестве определено обычное сложение многочленов, а умножение определим новое:

$$a(x) * b(x) = \mathrm{rem}_f(ab).$$

Нетрудно проверить, что множество E является кольцом относительно этого нового умножения и что новое умножение совпадает с обычным, если один из сомножителей принадлежит F. Чтобы отличать элементы E от обычных многочленов, обозначим x как элемент E через α. Тогда α — корень многочлена $f(x)$:

$$f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \ldots + a_n = \mathrm{rem}_f(x^n + \ldots + a_n) = \mathrm{rem}_f(F) = 0.$$

Остаётся проверить, что E — поле, т.е. что каждый ненулевой элемент E обратим. Но каждый такой элемент имеет вид $g(\alpha)$, где $g(x)$ — ненулевой многочлен степени меньшей, чем n. Тогда $g(x)$

и $f(x)$, в силу неприводимости $f(x)$, не имеют общего делителя положительной степени, значит, по теореме 6, существуют такие многочлены $u(x)$ и $v(x)$, что

$$u(x)f(x) + v(x)g(x) = 1.$$

Соответственно, в E получаем равенство

$$1 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = u(\alpha) \cdot 0 + v(\alpha)g(\alpha) = v(\alpha)g(\alpha),$$

т.е. $g(\alpha)^{-1} = v(\alpha)$. □

Лемма 1. *Если F — поле характеристики p, и $a, b \in F$, то*

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

Доказательство. Воспользуемся формулой бинома Ньютона:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \ldots + \binom{p}{k} a^{p-k}b^k + \ldots + b^p. \tag{2}$$

Поскольку

$$\binom{p}{k} = \frac{p!}{(p-k)!k!},$$

при $0 < k < p$ знаменатель этой дроби не делится на простое число p, а числитель делится на p, значит, дробь делится на p. Но в поле характеристики p умножение на p отображает любой элемент в 0, значит, в сумме (2) остаются только первое и последнее слагаемые □

Очевидная индукция доказывает, что аналогичное утверждение справедливо для любого числа слагаемых, а из этого вытекает так называемая малая теорема Ферма*:*

Следствие 1. *Для любого $a \in \mathbb{Z}_p$ имеем $a^p = a$.*

Доказательство. Если $a = [0]$, утверждение очевидно. Если же $a = [k]$, где $k > 0$, то

$$[k]^p = (\underbrace{[1] + [1] + \ldots + [1]}_{k \text{ раз}})^p = \underbrace{[1]^p + [1] + \ldots + [1]^p}_{k \text{ раз}} = \underbrace{[1] + [1] + \ldots + [1]}_{k \text{ раз}} = [k].$$

□

Теорема 8. *Для любого простого числа p и любого натурального числа r существует поле из p^r элементов.*

Доказательство. Положим $q = p^r$ рассмотрим многочлен $x^q - x$ над полем $\mathbb{Z}_p$. Применяя многократно теорему 7, получим поле E, в котором многочлен $x^q - x$ разлагается на линейные множители. Но кратных корней у многочлена $x^q - x$ не может быть: кратный корень многочлена есть корень его формальной производной, а $(x^q - x)' = qx^{q-1} - 1$ не имеет корней в поле характеристики p. Значит, в поле E многочлен $x^q - x$ имеет разложение

$$x^q - x = (x - \alpha_1) \ldots (x - \alpha_q),$$

где $\alpha_1, \ldots, \alpha_q$ — корни этого многочлена.

Теперь мы покажем, что множество корней $P = \{\alpha_1, \ldots, \alpha_q\}$ есть поле. Действительно, произведение двух элементов $\alpha, \beta \in P$ принадлежит P: $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$. Сумма таких элементов также принадлежит P в силу леммы 2. Из этого следует, что $-\alpha = (p-1) \cdot \alpha$ является корнем многочлена $x^q - x$, а если $\alpha \neq 0$, то из $\alpha^q - \alpha = \alpha(\alpha^{q-1} - 1) = 0$ следует, что $\alpha^{q-1} = 1$, т.е. $\alpha^{-1} = \alpha^{q-2} \in P$. Значит, P — искомое поле. □

Лекция 2. Элементы алгебраической теории кодов.

Пусть Ω — конечное множество (алфавит), $q = |\Omega| > 1$, Ω^n — множество *слов* длины n, т.е. строк $(a_1, a_2, \ldots, a_n)$, где $a_i \in \Omega, i = 1 \ldots, n$.

Определение 8. *Кодом* длины n над алфавитом Ω называется любое непустое подмножество C множества строк Ω^n.

Элементы множества C называются *кодовыми словами* кода C.

Размерностью (комбинаторной) кода C называется (действительное) число $\log_q |C|$.

Расстоянием Хэмминга между словами $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$ называется число $d(a, b) = |\{i : a_i \neq b_i, 1 \leqslant i \leqslant n\}|$.

Расстоянием кода C называется число

$$d(C) = \min\{d(a, b) : a, b \in C \text{ и } a \neq b\}$$

.

Код длины n над алфавитом из q элементов, имеющий размерность k и расстояние d, называется $[n, k, d]_q$-*кодом.*

Предложение 3 (Свойства расстояния Хэмминга)**.** *Для любых слов $a, b, c \in \Omega^n$ справедливы следующие утверждения:*
1) $d(a, b) = d(b, a)$*;*
2) $d(a, b) = 0$ *тогда и только тогда, когда* $a = b$*;*
3) (неравенство треугольника) $d(a, c) \leqslant d(a, b) + d(b, c)$*.*

Доказательство. Первые два утверждения очевидны. Докажем неравенство треугольника. Для этого запишем слова a, b, c одно под другим:

$$\begin{array}{l} a = (a_1, \ \ldots \ , \ a_i, \ \ldots \ , a_n) \\ b = (b_1, \ \ldots \ , \ b_i, \ \ldots \ , b_n) \\ c = (c_1, \ \ldots \ , \ c_i, \ \ldots \ , c_n) \end{array}$$

и заметим, что неравенство $a_i \neq c_i$ возможно только в случае выполнения хотя бы одного из неравенств $a_i \neq b_i$ или $b_i \neq c_i$, значит, количество таких позиций i не превосходит $d(a, b)+d(b, c)$. □

Теорема 9 (Исправление ошибок)**.** *Пусть d — расстояние Хэмминга кода C и $2r < d$. Тогда для любого слова $a \in \Omega^n$ существует не более одного слова $c \in C$, для которого выполнено неравенство $d(a, c) \leqslant r$.*

□ Действительно, пусть $c_1, c_2 \in C$, $d(a, c_1) \leqslant r$ и $d(a, c_2) \leqslant r$. Тогда
$d(c_1, c_2) \leqslant d(c_1, a) + d(a, c_2) \leqslant 2r < d$, откуда $c_1 = c_2$. □

Принцип максимального правдоподобия. Если известно, что переданное слово a принадлежит коду C, а полученное слово b ему не принадлежит, то слово b заменяется на такое слово $c \in C$, что $d(b, c)$ минимально. Если при передаче искажено менее чем $d/2$ знаков, то $c = a$.

Теорема 10 (Граница Синглтона)**.** *Если C — код длины n размерности k с расстоянием d, то $d + k \leqslant n + 1$.*

Доказательство. Пусть $m = |C| = q^k$. Выпишем все слова кода C в виде матрицы и разделим ее столбцы

$$\begin{array}{c|c} (a_{1,1} \ldots a_{1,d-1} & a_{1,d} \ldots a_{1,n}) \\ \ldots & \ldots \\ (a_{i,1} \ldots a_{i,d-1} & a_{i,d} \ldots a_{i,n}) \\ \ldots & \ldots \\ (a_{j,1} \ldots a_{j,d-1} & a_{j,d} \ldots a_{j,n}) \\ \ldots & \ldots \\ (\underbrace{a_{m,1} \ldots a_{m,d-1}}_{d-1} & \underbrace{a_{m,d} \ldots a_{m,n}}_{n-(d-1)}) \end{array} \qquad \begin{array}{c} (a_{i,d} \ldots a_{i,n}) = (a_{j,d} \ldots a_{j,n}) \\ \Downarrow \\ i = j \end{array}$$

Следовательно, $m = q^k \leqslant q^{n-(d-1)} \Rightarrow k \leq n - d + 1$. □

Определение 9. Код C длины n размерности k с расстоянием d называется *МДР-кодом* (или, полностью, *разделимым кодом с максимальным достижимым расстоянием*), если

$$d + k = n + 1.$$

Простейшие примеры:
1) *Код констант* $C = \{(c, c, \ldots, c) : c \in \Omega\}$ — $[n, 1, n]_q$-код.
2) Код Ω^n — $[n, n, 1]_q$-код.
3) *Код проверки на чётность*, состоящий из слов $(a_1, \ldots, a_n)$ над алфавитом $\mathbb{Z}_q$, для которых $a_1 + \ldots + a_n = [0]$ — $[n, n-1, 2]_q$-код.

Перечисленные МДР-коды называют *тривиальными*.

Нерешенная задача. Для заданных значений q и k найти максимальную возможную длину $n(k, q)$ МДР-кода размерности k над алфавитом из q элементов.

Ответ не найден даже при $k = 2$ и $q = 10$: известно лишь, что $5 \leqslant n(2, 10) \leqslant 11$. При $k = 2$ и $q < 10$ ответ даётся следующей таблицей:

q	2	3	4	5	6	7	8	9
$n(2, q)$	3	4	5	6	3	8	9	10

Вообще, вопрос об МДР-кодах размерности 2 непосредственно связан с вопросом о латинских квадратах, которые мы рассмотрим в следующей лекции.

Больше известно о линейных МДР-кодах

Определение 10. *Линейным кодом* длины n над конечным полем F из q элементов называется подпространство пространства строк F^n, т.е. подмножество множества строк, замкнутое относительно операций сложения строк и умножения строки на элемент поля F.

Ясно, что если C — линейный код, то в C можно выбрать базис, скажем из k элементов, поэтому число элементов кода C равно q^k и его комбинаторная размерность равна обычной размерности: $\log_q(q^k) = k$.

Следующая конструкция позволяет строить линейные МДР-коды над заданным полем F любой размерности k и длины n, где $2 \leqslant k \leqslant n \leqslant q = |F|$.

Определение 11. Пусть F — поле из q элементов, $\alpha_1, \ldots, \alpha_n$ — различные элементы поля F, $u_1, \ldots, u_n$ — произвольные обратимые элементы поля F.

Для произвольных элементов $\lambda_0, \ldots, \lambda_{k-1}$ поля F положим $g(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{k-1} x^{k-1}$ и определим слово

$$w(\lambda_0, \ldots, \lambda_{k-1}) = (u_1 g(\alpha_1), \ldots, u_n g(\alpha_n).$$

Ясно, что совокупность всех слов вида $w(\lambda_0, \ldots, \lambda_{k-1})$ есть линейный код над F длины n. Этот код называется *обобщённым кодом Рида–Соломона* и обозначается через $GRS(k, n)$ или, более подробно, через $GRS(k; \alpha_1, \ldots, \alpha_n; u_1, \ldots, u_n)$.

Теорема 11. *Пусть F — конечное поле и $2 \leqslant k \leqslant n \leqslant q = |F|$. Тогда любой обобщённый код Рида–Соломона $GRS(k; \alpha_1, \ldots, \alpha_n; u_1, \ldots, u_n)$ является МДР-кодом размерности k.*

Доказательство. Пусть d' и k' — соответственно расстояние и размерность кода $C = GRS(k; \alpha_1, \ldots, \alpha_n; u_1, \ldots, u_n)$. Заметим, что число слов кода C не превосходит числа задающих слова наборов $\lambda_0, \ldots, \lambda_{k-1}$, следовательно, $|C| \leqslant q^k$ и $k' = \dim C \leqslant k$.

Покажем, что расстояние d' кода C не меньше числа $d = n - k + 1$. Предположим противное: пусть найдутся различные слова $a, b \in C$, для которых $d' = d(a, b) < d$. Рассмотрим слово $c = a - b$. Ясно, что $c \neq 0$ и $c \in C$, значит, $c = w(\lambda_o, \ldots, \lambda_{k-1})$, причём $g(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{k-1} x^{k-1}$ — ненулевой многочлен степени меньше k. Но только d' из элементов $\alpha_1, \ldots, \alpha_n$ не являются корнями этого многочлена, а остальные $n - d'$ элементов — корни многочлена $g(x)$. Однако, $n - d' > n - d = n - (n + 1 - k) = k - 1$, а степень многочлена $g(x)$ не больше $k - 1$. По теореме Безу, это невозможно. Итак, расстояние d' кода C удовлетворяет неравенству $d' \geqslant n - k + 1 \geqslant n - k' + 1$. В то же время из теоремы 10 следует, что $d' \leqslant n - k' + 1$, значит, все выведенные неравенства превращаются в равенства, откуда $k = k'$ и $d' = d = n + 1 - k$. □

Лекция 3. Квазигруппы и латинские квадраты

Определение 12. *Латинским квадратом* над конечным множеством M называется матрица размера $|M| \times |M|$, в каждом столбце и каждой строке которого содержатся все элементы из M (по одному разу каждый).

Пример — латинский квадрат над множеством $\{0, 1, 2, 3, 4\}$:

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

Впервые латинские квадраты (4-го порядка) были опубликованы в книге «Шамс аль Маариф» («Книга о Солнце Гнозиса»), написанной Ахмадом аль-Буни в Египте приблизительно в 1200 году.

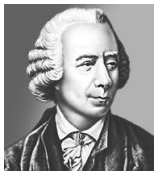
Занумеруем строки и столбцы латинского квадрата L элементами множества M и элемент квадрата L, лежащий в строке x и столбце y, обозначим через $L[x, y]$. Тогда L можно рассматривать как таблицу бинарной операции $*$ на M, считая, что $L[x, y] = x * y$.

Определение 13. *Квазигруппой* называется множество M с одной бинарной операцией $*$, удовлетворяющей аксиоме

$$\forall \quad a, b \in M \quad \exists!\ x, y \in M : a * x = b \quad \& \quad y * a = b.$$

Легко видеть, что построение латинского квадрата над M равносильно заданию операции на M, превращающей M в квазигруппу.

Например, приведённый выше латинский квадрат порядка 5 соответствует операции $x * y = 2x + y$ в кольце $\mathbb{Z}_5$ (здесь и далее мы опускаем квадратные скобки в обозначении вычетов).

Задача о 36 офицерах. 

Л. Эйлер (1707 – 1783) сформулировал следующую задачу (Euler L. Recherches sur une nouvelle espèce de quarrés magiques. — Middelburg, 1782):

“Этот вопрос касается совокупности 36 офицеров шести разных званий, взятых из шести разных полков, которых выстраивают в каре таким образом, чтобы в каждом ряду, как по горизонтали, так и по вертикали, находилось шесть офицеров различных званий и из разных полков. Однако после всех трудов, затраченных на решение этой задачи, я вынужден был признать, что такое размещение абсолютно невозможно, хотя и не удалось дать строгого доказательства этому.”

Задача о 9 офицерах (греко-латинский квадрат). Пусть
a, b, c обозначают полки — уланский, драгунский, гусарский,
α, β, γ обозначают звания — корнет, штабс-ротмистр, ротмистр.
Пара $a\alpha$ обозначает улана-корнета и т.д., до пары $c\gamma$, которая обозначает гусара-ротмистра.

Решение

$a\alpha$	$b\gamma$	$c\beta$
$b\beta$	$c\alpha$	$a\gamma$
$c\gamma$	$a\beta$	$b\alpha$

a	b	c
b	c	a
c	a	b

α	γ	β
β	α	γ
γ	β	α

Ортогональные латинские квадраты. Латинские квадраты L и L' над множеством M называются *ортогональными*, если отображение $(x, y) \mapsto (L[x, y], L'[x, y])$ биективно на $M \times M$. Иными словами, любая пара элементов из M единственный раз встречается в одинаково расположенных клетках этих квадратов.

В терминах операций: квадраты L и L', заданные, соответственно, операциями $*$ и $\circ$ на множестве M, ортогональны тогда и только тогда, когда

$$\forall \quad a,b \in M \quad \exists!\, x,y \in M : x * y = a \quad \& \quad x \circ y = b.$$

Гипотеза Эйлера. Л.Эйлер доказал существование пар ортогональных латинских квадратов любого нечётного порядка и любого "чётно-чётного" (т.е. кратного 4) порядка (мы дадим алгебраическое доказательство для квадратов нечётного порядка, использующее кольца вычетов).

Он также предположил, что ортогональных латинских квадратов "чётно-нечётного" порядка (т.е. порядка вида $n = 4k + 2$, $k = 0, 1, 2, \ldots$) не существует.

Для $n = 2$ это очевидно.

Для $n = 6$ это доказано только спустя 100 с лишним лет Г.Тарри (1900).

Однако уже при $n = 10$ пары ортогональных латинских квадратов порядка n существуют (R. C. Bose, S. S. Shrikhande and E. T. Parker, 1960, для построения использовался компьютер). Способ "ручного" построения таких пар предложил Чжу Ле (1982).

0	2	4	6	9	8	7	5	3	1
7	3	5	0	2	9	8	1	6	4
8	7	6	1	3	5	9	4	2	0
9	8	7	2	4	6	1	0	5	3
4	9	8	7	5	0	2	3	1	6
5	0	9	8	7	1	3	6	4	2
6	1	3	9	8	7	4	2	0	5
1	4	0	3	6	2	5	7	8	9
2	5	1	4	0	3	6	8	9	7
3	6	2	5	1	4	0	9	7	8

0	7	8	9	4	5	6	1	2	3
2	3	7	8	9	0	1	4	5	6
4	5	6	7	8	9	3	0	1	2
6	0	1	2	7	8	9	3	4	5
9	2	3	4	5	7	8	6	0	1
8	9	5	6	0	1	7	2	3	4
7	8	9	1	2	3	4	5	6	0
5	1	4	0	3	6	2	7	8	9
3	6	2	5	1	4	0	9	7	8
1	4	0	3	6	2	5	8	9	7

Теорема 12. *Пусть n — нечётное число, $n > 1$. Один латинский квадрат определим с помощью операции сложения в кольце $G = \mathbb{Z}_n$.*

Второй латинский квадрат определим новой *операцией на множестве G: $x * y = 2x + y$.*

Тогда полученные квадраты ортогональны.

Доказательство. Первая операция определяет латинский квадрат, потому что

$$a + x = b \Leftrightarrow x = a - b.$$

Вторая операция определяет латинский квадрат, потому что вычет 2 по нечётному модулю n является обратимым элементом кольца $\mathbb{Z}_n$: обратный вычет можно определить как $2^{-1} = \dfrac{n+1}{2}$. Следовательно,

$$a * x = b \Leftrightarrow x = b - 2a, \quad y * a = b \Leftrightarrow \ = 2^{-1}(b - a).$$

Теперь проверим, что данные квадраты ортогональны. Для этого обычным образом для любых $a, b \in G$ решим систему уравнений $\begin{cases} x + y = a \\ 2x + y = b \end{cases}$. Из первого уравнения $y = a - x$, из второго $2x + a - x = b \Leftrightarrow x = b - a$, откуда $y = 2a - b$. □

Системы попарно ортогональных латинских квадратов

Теорема 13. *Пусть M — конечное множество. Существование множества из n попарно ортогональных латинских квадратов равносильно существованию МДР-кода длины $n + 2$ и размерности 2 над алфавитом M.*

Доказательство. Пусть попарно ортогональные латинские квадраты задаются операциями $*_1, *_2, \ldots, *_n$. Рассмотрим код C длины $n + 2$, состоящий их всех слов вида

$$(x, y, x *_1 y, x *_2 y, \ldots, x *_n y).$$

Очевидно, что $|C| = |M|^2$, т.е. (комбинаторная) размерность кода C равна 2. Покажем, что расстояние кода C равно $n+2+1-2 = n+1$. Для этого рассмотрим два слова $a = (a_1 \dots, a_{n+2})$ и $b = (b_1, \dots, b_{n+2})$, символы которых различаются менее чем в $n+1$ позициях. Значит, символы в некоторых двух позициях $i < j$ должны совпадать (т.е. $a_i = b_i$ и $a_j = b_j$). Если $i = 1$ и $j = 2$, то слова a и b равны по построению. Если, скажем, $i = 1$, а $j > 1$, то как a_2 так и b_2 удовлетворяют уравнению $a_1 *_{j-2} x = a_j \Leftrightarrow b_1 *_{j-2} x = b_j$, поэтому $a_2 = b_2$ и $a = b$. Аналогично при $i = 2$ и $j > 2$ получаем равенство $a_1 = b_1$, и снова имеем $a = b$. Наконец, при $i > 2$ пары a_1, a_2 и b_1, b_2 являются решением системы уравнений $x *_{i-2} y = a_i = b_i$ и $x *_{j-2} y = a_j = b_j$. В силу ортогональности квадратов с номерами $i-2$ и $j-2$ снова получаем $a_1 = b_1$ и $a_2 = b_2$, откуда $a = b$.

Обратно, пусть C есть МДР-код длины $n+2$ и размерности 2 над M. Тогда, как легко заметить, вспоминая доказательство границы Синглтона, первые координаты слов из C образуют произвольные пары элементов M, причём каждая пара встречается один раз. Значит, можно определить операции $*_1, *_2, \dots, *_n$ следующим образом: для любых $x, y \in M$ найдем в C слово $a = (x, y, a_3, \dots, a_{n+2})$ и положим $x *_i y = a_{i+2}$. Остаётся проверить, что каждая операция из $*_1, *_2, \dots, *_n$ определяет латинский квадрат и что эти квадраты попарно ортогональны. Но из того, что расстояние кода C равно $n+1$, следует, что если 2 слова имеют одинаковые символы на в двух позициях $i < j$, то они совпадают. Значит, множество пар (a_i, a_j), выбранных из всех слов кода C, равно M^2, причём каждая пара встречается один раз. Это и означает, что $*_{j-2}$ определяет латинский квадрат при $j > 2$ (выбираем $i = 1$ и $i = 2$ для проверки каждого из двух условий, определяющих квазигруппу), и что операции $*_{i-2}$ и $*_{j-2}$ ортогональны (при $i > 2$). □

Теорема 14. *Если $q = p^r$, где p — простое число, а r — натуральное число, то существует система из $q-1$ попарно ортогональных латинских квадратов порядка q.*

Доказательство. Пусть F — поле из q элементов, и $\{\alpha_1, \dots, \alpha_{q-1}\} = F \setminus \{0\}$ — множество всех ненулевых элементов поля F. Рассмотрим множество из $q-1$ операций на F, заданных формулами $x *_i y = \alpha_i x + y$, $i = 1, \dots, q-1$. Поскольку α_i — обратимый элемент поля F, каждая операция определяет квазигруппу ($a *_i x = b \Leftrightarrow x = b - \alpha_i a$, $y *_i a = b \Leftrightarrow y = \alpha_i^{-1}(b-a)$). Далее, система уравнений $x *_i y = a$, $x *_j y = b$ равносильна системе линейных уравнений $\alpha_i x + y = a$, $\alpha_j x + y = b$. Определитель этой системы $\begin{vmatrix} \alpha_i & 1 \\ \alpha_j & 1 \end{vmatrix} = \alpha_i - \alpha_j \neq 0$ при $i \neq j$, значит, эта система имеет единственное решение, следовательно, соответствующие латинские квадраты ортогональны. □

Предложение 4. *Для любого q выполнено неравенство $n(2, q) \leqslant q+1$.*

Доказательство. Для удобства занумеруем элементы алфавита Ω числами $1, 2, \dots, q$. Допустим, что C есть МДР-код размерности 2, длина которого n больше чем $q+1$. Как мы уже видели, в первых двух позициях слов кода C встречаются любые пары (i, j) чисел от 1 до q. Обозначим через $a^{(1)}, \dots, a^{(q)}$ слова кода C, начинающиеся, соответственно, с символов $(1,1), \dots, (1,q)$. Заметим, что в позициях $3, \dots, n$ слова $a^{(1)}, \dots, a^{(q)}$ содержат различные символы (иначе расстояние между ними было бы меньше $n-1$), следовательно, для любого $i > 2$ и любого числа k найдётся слово a^j, $j = j(i, k)$, содержащее в позиции i символ k. Пусть теперь b — слово, начинающееся с пары $(2, 1)$. Тогда слово b содержит общий символ со словом $a^{(1)}$ в позиции 2 и поэтому не может содержать в позициях $3, \dots, n$ общего символа со словом $a^{(1)}$. Меняя, если надо, нумерацию слов $a^{(1)}, \dots, a^{(q)}$, можем считать, что слово b имеет общий символ со словом $a^{(2)}$ в позиции 3, (и не имеет больше общих символов с этим словом). Получается, что в позиции $q+2$ все символы окажутся "занятыми", т.е. слова b с данными свойствами не существует. Противоречие доказывает предложение. □

Следствие 2. *При $q = p^r$, где p — простое число и $r \in \mathbb{N}$, $n(2, q) = q+1$.*

Рекомендуемая литература для дальнейшего чтения

1. Р. Лидл, Г. Нидеррайтер. Конечные поля (в двух томах). Москва, “Мир”, 1988.

2. Ф. Дж. МакВильямс, Н. Дж. А. Слоэн, Теория кодов, исправляющих ошибки. Москва, “Связь”, 1979.

3. Э. Р. Берлекамп, Алгебраическая теория кодирования, Москва, “Мир”, 1971.

4. М. Холл. Комбинаторика. Москва, “Мир”, 1970.

5. И. И. Валуцэ, В. Д. Белоусов, Г. Б. Белявская. Квазигруппы и латинские квадраты. Кишинёв, “Штиинца”, 1983.

6. М. М. Глухов. О применениях квазигрупп в криптографии. Прикладная дискретная математика, 2008, № 2, 28–32
(http://www.mathnet.ru/php/getFT.phtml?jrnid=pdm&paperid=29&what=fullt&option_lang=rus).

7. А. Е. Малых, В. И. Данилова, Об историческом процессе развития теории латинских квадратов и некоторых их приложениях. Вестник Пермского университета, N4 (2010), 95–104 (http://vestnik.psu.ru/files/articles/199_38700.p).