Разбор билетов. Алгебра

(SE) Основная теорема арифметики. Малая теорема Ферма, функция Эйлера. Мультипликативность функции Эйлера. Теорема Эйлера.

Основная теорема арифметики.

Лемма. Если $x \cdot y$ делится на простое число p, то p делит x или y.

◀ Пусть x не делится на p, тогда найдутся числа u, v такие, что

$$xu + pv = 1.$$

Домножим обе части на y: $(xy)u + ypv = y$. Оба слагаемых в левой части делятся на p, поэтому y делится на p. Существование такой пары чисел u, v можно доказать с помощью алгоритма Евклида. ▶

Теорема. Основная теорема арифметики. Каждое натуральное число $n > 1$ представляется в виде $n = p_1 p_2 ... p_k$, где p_i — простое число. Такое представление единственно с точностью до порядка следования сомножителей.

◀ **Существование.** Пусть $n > 1$ — наименьшее число, неразложимое на простые множители. Тогда n не может быть простым, так как простое число очевидным образом раскладывается на простые. Если n — составное, то оно является произведением двух меньших натуральных чисел, каждое из которых можно разложить на простые множители. Тогда n можно представить как произведение всех простых. Противоречие.

Единственность. Пусть n — наименьшее натуральное число, допускающее два разных разложения на простые множители:

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_l.$$

Если множитель p_1 есть среди множества $\{q_1, ..., q_k\}$, то их можно сократить, тогда получим разные разложения меньшего числа. Противоречие. Если p_1 нет среди множителей $\{q_1, ..., q_k\}$, то левая часть не делится на p_1 по доказанной лемме. Противоречие. ▶

Функция Эйлера.

Определение. *Функция Эйлера* $\varphi(n)$ определяется как количество натуральных чисел, не превосходящих n и взаимно простых с n.

Формула для функции Эйлера.

Теорема. Функция Эйлера мультипликативна, то есть для любых двух взаимно простых чисел m, n выполняется соотношение $\varphi(nm) = \varphi(n)\varphi(m)$.

◄ Запишем $n \cdot m$ натуральных чисел в таблицу с n столбцами и m строками (см. ниже).

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{vmatrix}$$

Число, находящееся на месте (i, j) можно представить как $x = n(i - 1) + j$. Если x взаимно просто с n, то j взаимно просто с n. Значит весь столбец j взаимно прост с n. Так как внутри столбца остаток не меняется, то разные остатки при делении на n соответствуют разным столбцам, значит взаимно простых с n столбцов в таблице ровно $\varphi(n)$.

Числа внутри каждого столбца образуют геометрическую прогрессию с разностью $d = n$: $a,\ a + n,\ a + 2n,\ ...,\ a + (m - 1)n$. Если числа из одного столбца в строках k, l дают одинаковые остатки при делении на m, то $(k - l)n$ делится на m, при условии $(n, m) = 1$ это возможно только при $k = l$. Значит, числа в одном столбце образуют полную систему остатков по m. Таким образом, в каждом столбце ровно $\varphi(n)$ взаимно простых с m чисел. Следовательно, среди первых $n \cdot m$ чисел ровно $\varphi(n)\varphi(m)$ взаимно просты с $n \cdot m$. ►

Теорема Эйлера. Пусть n и a — взаимно простые, тогда

$$a^{\varphi(n)} \equiv 1\ (mod\ n).$$

Отношение сравнимости по модулю n — это отношение эквивалентности. Класс эквивалентности, содержащий число a называется *вычетом числа a по модулю n* и обозначается $[a]_n$. Вычет $[x]_n$ называется обратимым, если существует $[y]_n$ такой, что $[x]_n[y]_n \equiv 1\ (mod\ n)$. Решение уравнения $[x]_n[y]_n - 1 = mn$ существует только при $(n, x) = 1$. Тогда у числа n ровно $\varphi(n)$ обратимых вычетов.

◄ Достаточно доказать теорему Эйлера только для вычетов. Рассмотрим вычеты по модулю n. Если $(a, n) = 1$, то вычет $[a]$ обратим. Пусть $[b_1], ..., [b_{\varphi(n)}]$ — все обратимые вычеты по модулю n. Тогда вычет $[b] = [b_1 \cdot ... \cdot b_{\varphi(k)}]$ тоже обратим. Тогда $[ab_1][ab_2]...[ab_{\varphi(n)}] = a^{\varphi(n)}[b] = [b]$,

так как умножение всех вычетов $[b_i]$ на a просто меняет их порядок. Домножим обе части на $[b]^{-1}$, получим требуемое равенство $a^{\varphi(n)} \equiv 1$. ▶

Малая теорема Ферма после теоремы Эйлера доказывается легко. Очевидно, что $\varphi(p) = p - 1$ для любого простого p. Тогда для взаимно простых a и p справедливо соотношение $a^{\varphi(p)} \equiv 1 \ (mod\ p) \Rightarrow$

$$a^{p-1} \equiv 1 \ (mod\ p).$$

(YA, SE) Понятие линейного пространства (ЛП). Линейная зависимость и независимость. Базис и размерность ЛП, их связь. Координаты элемента ЛП в базисе. Замена базиса, матрица перехода, преобразование координат при замене базиса.

Определение. Пусть $\Re$ — произвольное поле. Векторным (или линейным) пространством над $\Re$ называется множество V, элементов (векторов), удовлетворяющее следующим аксиомам:

а) На V задана бинарная операция $V \times V \to V$, наделяющая V строением абелевой группы. Стало быть:

1. $x + y = y + x$ (*коммутативность*);
2. $(x + y) + z = x + (y + z)$ (*ассоциативность*);
3. в V существует *нулевой* вектор 0 такой, что $x + 0 = x$ для любого $x \in V$;
4. для каждого вектора x из V существует *обратный* $-x$ такой, что $x + (-x) = 0$;

б) На множестве $\Re \times V$ задано умножение векторов на скаляры из $\Re$ обладающее свойствами

1. $1 \cdot x = x$ (*унитарность*);
2. $(\alpha\beta)x = \alpha(\beta x)$ для всех $\alpha, \beta \in \Re$, и $x \in V$ (*ассоциативность*);
3. $(\alpha + \beta)x = \alpha x + \beta x$ (*дистрибутивность*);
4. $\alpha(x + y) = \alpha x + \alpha y$ (*дистрибутивность*).

Пусть имеется конечный набор скаляров $\lambda_1, ..., \lambda_n \in \Re$ и векторов $x_1, ..., x_n \in V$. Тогда выражение

$$\lambda_1 x_1 + ... + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i$$

называется *линейной комбинацией* векторов x_i с коэффициентами λ_i. При этом множество $\langle M \rangle_{\Re}$ всевозможных линейных комбинаций векторов $x_i \in M$ замкнуто относительно операций сложения векторов и умножения их на скаляры:

$$\lambda \in \Re,\ x, y \in \langle M \rangle \Rightarrow x + y \in \langle M \rangle,\ \lambda x \in \langle M \rangle.$$

Принято говорить, что $\langle M \rangle$ — *линейная оболочка* множества $M \subset V$.

Определение. Пусть V — векторное пространство над $\Re$, $U \subset V$ — его подмножество, являющееся аддитивной подгруппой V и переходящее в себя при умножении на скаляры. Тогда ограничение на U операций, определенных в V, наделяет U строением векторного пространства. Оно называется *векторным* (или *линейным*) *подпространством* в V.

Определение. Векторы $v_1, ..., v_n$ пространства V называются *линейно зависимыми*, если некоторая их нетривиальная линейная комбинация равна нулю, то есть найдутся такие скаляры $\alpha_1, ..., \alpha_n$, не все равные нулю, что

$$\alpha_1 v_1 + ... + \alpha_n v_n = 0.$$

В противном случае система векторов называется *линейно независимой*.

Определение. Число векторов, содержащихся в любой максимальной (не допускающей расширения до линейно независимой системы систем из большего числа векторов) линейно независимой подсистеме данной системы векторов, называется *рангом* системы.

Определение. Линейное пространство V, в котором существует n линейно независимых векторов, но нет линейно независимых систем большего ранга, называется *n-мерным* ($\dim V = n$). Если такого числа n нет, то векторное пространство называется *бесконечномерным*. Пример бесконечномерного пространства — множество всех непрерывных функций. Из него всегда можно выделить бесконечное число линейно независимых векторов $1,\ x,\ x^2, ..., x^n, ...$

Определение. Пусть V — n-мерное векторное пространство над полем $\Re$. Любая система из n независимых векторов $e_1, ..., e_n \in V$ называется (конечным линейным) *базисом* пространства V.

Теорема. Пусть V — векторное пространство над полем $\Re$ с базисом $(e_1, ..., e_n)$ тогда имеют место следующие утверждения:

1. каждый вектор $v \in V$ можно представить, и притом единственным образом, в виде линейно комбинации векторов $e_1, ..., e_n$;

2. всякую систему из $s \leq n$ линейно независимых векторов можно дополнить до базиса.

◀ 1) Присоединим к базису вектор v. По определению базиса система из векторов $(v, e_1, ..., e_n)$ линейно зависима, поэтому найдутся скаляры λ_i, $\lambda_0 \neq 0$ такие, что

$$\lambda_0 v + \lambda_1 e_1 + ... + \lambda_n e_n = 0,$$

тогда

$$v = (-\frac{\lambda_1}{\lambda_0})e_1 + ... + (-\frac{\lambda_n}{\lambda_0})e_n.$$

Если вектор v допускает два разложения по базису, то

$$\alpha_1 e_1 + ... + \alpha_n e_n = v = \beta_1 e_1 + ... + \beta_n e_n,$$

значит

$$(\alpha_1 - \beta_1)e_1 + ... + (\alpha_n - \beta_n)e_n = 0,$$

что по определению базиса возможно лишь при $\alpha_i = \beta_i$.

2) Пусть $f_1, ..., f_s$ — система линейно независимых векторов. Рассмотрим систему $f_1, ..., f_s, e_1, ..., e_n$. Удалим из нее все векторы, которые выражаются через предыдущие. Тогда по условию все векторы f_i останутся. Получаем

$$f_1, ..., f_s, e_{i_1}, ..., e_{i_t}.$$

Если теперь

$$\alpha_1 f_1 + ... + \alpha_s f_s + \beta_1 e_{i_1} + ... + \beta_t e_{i_t} = 0,$$

то существовал бы $\beta_k \neq 0$ с наибольшим номером k, значит e_{i_k} можно выразить через предыдущие, что исключено по построению. Значит такая система линейно независима. Очевидно, что через нее выражается любой вектор. Значит она максимальна, следовательно $f_1, ..., e_{i_k}$ образуют базис. ▶

В силу теоремы о единственности разложения вектора ЛП по базису имеет место следующее

Определение. Пусть $(e_1, ..., e_n)$ — базис векторного пространства V над $\Re$. Скаляры $\lambda_1, ..., \lambda_n \in \Re$, входящие в разложение

$$v = \lambda_1 e_1 + ... + \lambda_n e_n$$

называются *координатами* вектора $v \in V$ в данном базисе.

Если $x = \alpha_1 e_1 + ... + \alpha_n e_n$, $y = \beta_1 e_1 + ... + \beta_n e_n$, то $x + y = (\alpha_1 + \beta_1)e_1 + ... + (\alpha_n + \beta_n)e_n$ (коммутативность + дистрибутивность). При этом $\lambda x = \lambda(\alpha_1 e_1 + ... + \alpha_n e_n) \Rightarrow$ (дистрибутивность) $\Rightarrow \lambda x = \lambda\alpha_1 e_1 + ... + \lambda_n \alpha_n e_n$.

Замена базиса.

Пусть V — линейное пространство и $(e_1, ..., e_n)$, $(e'_1, ..., e'_n)$ — его базисы. Векторы одного базиса выражаются через векторы другого:

$$\begin{cases} e'_1 = a_{11}e_1 + a_{21}e_2 + ... + a_{n1}e_n \\ \dots \\ e'_n = a_{1n}e_1 + a_{2n}e_2 + ... + a_{nn}e_n. \end{cases}$$

Коэффициенты $a_{ij} \in \Re$ определяют матрицу

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Важно! Координаты вектора e'_j составляют j-ый **столбец** матрицы A. Матрица A называется *матрицей перехода от базиса* $(e_1, ..., e_n)$ *к базису* $(e'_1, ..., e'_n)$.

Если вектор v задан в старом базисе координатами $[\lambda_1, ..., \lambda_n]$, то есть

$$v = \lambda_1 e_1 + ... + \lambda_n e_n,$$

то можно выразить его координаты через новый базис. Для этого нужно решить уравнение

$$X = AX'. \tag{1}$$

Здесь $X = [\lambda_1, ..., \lambda_n]$ — координаты вектора в старом базисе, A — матрица перехода от старого базиса к новому, $X' = [\lambda'_1, ..., \lambda'_n]$ — координаты вектора в новом базисе.

Данное уравнение не сложно получить, заменив старые базисные векторы на новые

$$v = \lambda'_1(a_{11}e_1 + ... + a_{n1}e_n) + ... + \lambda'_n(a_{1n}e_1 + ... + a_{nn}e_n) = \lambda_1 e_1 + ... + \lambda_n e_n.$$

Уравнение (1) можно переписать в виде $A^{-1}X = X'$. Итак, справедлива

Теорема. При переходе от базиса $(e_1, ..., e_n)$ пространства V к базису $(e'_1, ..., e'_n)$, определяемом матрицей A, координаты вектора в **новом** базисе выражаются через **старые** координаты при помощи обратимого линейного преобразования с матрицей A^{-1}.

Важно отметить, что старые координаты выражаются через новые естественным образом (зная X' легко получить X), в то время как получение новых координат через старые требует трудоемкой операции обращения матрицы перехода.

(SE) Системы линейных алгебраических уравнений. Теорема Кронекера-Капелли. Общее решение системы алгебраических уравнений.

(YA, SE) Понятие линейного пространства (ЛП). Линейная зависимость и независимость. Базис и размерность ЛП, их связь. Координаты элемента ЛП в базисе. Замена базиса, матрица перехода, преобразование координат при замене базиса.

(YA) Матрицы. Транспонированная матрица. Обратная матрица. Ранг матрицы. Специальные виды матриц. Линейные и нелинейные операции над матрицами: сложение, умножение матрицы на число, умножение матриц, транспонирование матриц. Их свойства.

(YA) Евклидовы и унитарные пространства. Свойства скалярного произведение, неравенство Коши-Буняковского. Норма, ортонормированный базис. Разложение пространства в прямую сумму подпространства и его ортогонального дополнения.

(YA) Понятие линейного оператора, матрицы линейного оператора, нормы. Преобразование матрицы при замене базиса, характеристический многочлен. Собственные векторы и собственные значения, геометрический смысл.

(YA) Квадратичные формы, их знакоопределенность и канонический вид. Унитарные и нормальные операторы.

Вопросы из программы НОД-ВШЭ.

Линейная зависимость системы векторов. Базис линейного пространства. Скалярное произведение.

Определитель квадратной матрицы. Вычисление определителей. Разложение определителя по строке и по столбцу.

Транспонированная матрица. Обратная матрица. Ранг матрицы. Специальные виды матриц.

Системы линейных уравнений. Метод Крамера. Метод Гаусса. Фундаментальная система решений.

Линейные преобразования векторных пространств и их матрицы. Изменение матриц линейного пространства и квадратичной формы при смене базиса.

Собственные числа и собственные векторы матрицы. Собственные и инвариантные подпространства.

Характеристический многочлен. Аннулирующий и минимальный многочлены. Теорема Гамильтона-Кэли.

Квадратичные формы. Матрица квадратичной формы. Условие положительной (отрицательной) определенности квадратичной формы. Критерий Сильвестра. Индексы инерции квадратичных форм.