ЛЕКЦИЯ 5

ЧЕТНОСТЬ ПОДСТАНОВОК

АРИФМЕТИКА ЦЕЛЫХ ЧИСЕЛ

ВЕКТОРНЫЕ ПРОСТРАНСТВА

ЧЕТНОСТЬ ПОДСТАНОВОК

Лемма 1. *Каждая подстановка $\pi \in S_n$ является произведением транспозиций.*

Доказательство. В силу того, что любая подстановка раскладывается в произведение непересекающихся циклов, нам достаточно доказать, что любой цикл $(i_1\, i_2\, \ldots\, i_{k-1}\, i_k)$ раскладывается в произведение транспозиций.

Это разложение можно предъявить в явном виде:

$$(i_1\, i_2\, \ldots\, i_{k-1}\, i_k) = (i_1\, i_2)(i_2\, i_3)\ldots(i_{k-1}\, i_k).$$

□

Определение 1. У подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{pmatrix}$$

инверсией называется такая пара столбиков $\begin{pmatrix} l \\ i_l \end{pmatrix}$ и $\begin{pmatrix} k \\ i_k \end{pmatrix}$, что $l < k$, но $i_l > i_k$.

Определение 2. *Четностью* подстановки $\sigma \in S_n$ называется четность количества всех инверсий в этой подстановке.

Очевидно, что тождественная подстановка является четной, так как не содержит ни одной инверсии.

Транспозиция $(i\, j)$ всегда нечетна.

Теорема 1. *Умножение на транспозицию (слева или справа) меняет четность подстановки.*

Замечание 1. Предварительно заметим, что умножение на транспозицию слева или справа меняет у подстановки ровно два элемента во второй строчке.

Доказательство. Соответственно сформулированному замечанию нам надо показать, что если в подстановке поменять два элемента во второй строчке, то ее четность изменится на противоположную.

Пусть для начала эти элементы являются соседними, то есть

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots n \\ i_1 & i_2 & \dots & i_k & i_{k+1} & \dots & i_n \end{pmatrix},$$

после умножения на транспозицию

$$\sigma' = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots n \\ i_1 & i_2 & \dots & i_{k+1} & i_k & \dots & i_n \end{pmatrix}.$$

Все инверсии, которые существовали между столбцами с номерами меньше k или больше $k+1$, либо между одним из таким столбцов и либо k-м, либо $k+1$-м, сохранятся (так как порядок следования между этими парами столбцов не изменится. Если между столбцами с номерами k и $k+1$ не было инверсии, то они появится, если же инверсия была, то она исчезнет.

Таким образом, число инверсий в подстановке σ' на одну отличается (на одну больше или на одну меньше), чем число инверсий в подстановке σ.

Значит, эти две подстановки имеют различную четность.

Если же мы поменяли в подстановке σ не соседние столбики, а столбики, которые находились на расстоянии m друг от друга, то это означало бы, что мы делаем сначала $m-1$ перестановку соседних столбиков (после чего они становятся соседними), далее меняем эти два столбика местами и за $m-1$ шаг возвращаем

столбик на место. На это уйдет $2m-1$ операция, в которой мы меняем местами элементы в соседних столбиках, то есть произойдет нечетное число изменений четности подстановки.

Таким образом, постановка σ поменяет четность. □

Следствие 1. *Если подстановку σ разложить в произведение транспозиций двумя способами, то четность числа транспозиций в разложениях будет одинаковой.*

Следствие 2. *Четность подстановки равна четности числа транспозиций в ее разложении.*

Лемма 2. *Четность цикла длины k равна четности числа $k-1$.*

Доказательство. Очевидно следует из разложения цикла длины k в произведение $k-1$ транспозиции. □

Теорема 2. *Если подстановка $\sigma = \tau_1\tau_2\ldots\tau_m$ разложена в произведение m независимых циклов длин $l_1, l_2, \ldots, l_m$ соответственно, то ее четность равна*

$$(-1)^{\sum\limits_{i=1}^{m}(l_i-1)}.$$

Доказательство. Очевидно следует из предыдущих леммы и следствий. □

Теорема 3. *Множество всех четных перестановок (обозначаемое через A_n) замкнуто относительно операций умножения и взятия обратной перестановки (то есть является группой).*

Доказательство. Очевидно следует из предыдущих теорем. □

Так как все подстановки делятся на четные и нечетные, рассмотрим разбиение

$$S_n = A_n \cup \overline{A}_n, \quad \overline{A}_n = S_n \setminus A_n.$$

Установим биективное соответствие между множествами A_n и $\overline{A}_n$, сопоставляя каждой подстановке $\sigma \in A_n$ подстановку $\sigma \cdot (1\,2) \in \overline{A}_n$.

Очевидно, что такое соответствие является биективным, откуда получаем, что четные подстановки составляют ровно половину от всех подстановок.

АРИФМЕТИКА ЦЕЛЫХ ЧИСЕЛ

Дадим краткое описание простейших свойств делимости целых чисел, которые понадобятся нам в дальнейшем.

ОПРЕДЕЛЕНИЕ 3. Целое число s называется *делителем* целого числа n, если $n = st$ для некоторого $t \in \mathbb{Z}$. В свою очередь n называется *кратным* s. Делимость обозначается символом $s|n$, отсутствие делимости — $s \not| n$. Делимость — транзитивное отношение на $\mathbb{Z}$. Если $m|n$ и $n|m$, то $n = \pm n$ и числа n, m называются *ассоциированными*. Целое число p, все делители которого исчерпываются числами $\pm 1, \pm p$, называют *простым*.

Теорема 4 (основная теорема арфиметики)**.** *Каждое положительное целое число $n \neq 1$ может быть записано в виде произведения простых чисел: $n = p_1 p_2 \dots p_s$. Эта запись единственна с точностью до порядка множителей.*

Собрав вместе одинаковые простые множители и изменив обозначения, получим

$$n = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k}, \quad \varepsilon_i > 0, \quad 1 \leqslant i \leqslant k.$$

Заметим, что множество P всех простых чисел бесконечно (теорема Евклида). Действительно, если бы существовало только конечное множество простых чисел $p_1, p_2, \dots, p_t$, то по основной теореме число $c = p_1 p_2 \dots p_t + 1$ делилось бы хотя бы на одно p_i. Пусть, например, $c = p_1 c'$. Тогда $p_1(c' - p_2 \dots p_t) = 1$, что невозможно, так как делителями единицы являются только ± 1.

Любые два целых числа n и m можно записать в виде произведения степеней одних и тех же простых чисел

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad m = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

если условиться допускать нулевые показатели.

Введем в рассмотрение два целых числа:

$$\text{НОД}(n, m) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}, \quad \gamma_i = \min(\alpha_i, \beta_i), \quad i = 1, \dots, k,$$

и

$$\text{НОК}(n, m) = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}, \quad \gamma_i = \max(\alpha_i, \beta_i), \quad i = 1, \dots, k.$$

Очевидным образом выполняются следующие утверждения:
(1) $\text{НОД}(n, m) | n$; $\text{НОД}(n, m) | m$, и если $d | n$, $d | m$, то $d | \text{НОД}(n, m)$.
(2) $n | \text{НОК}(n, m)$, $m | \text{НОК}(n, m)$, и если $n | u$, $m | u$, то $\text{НОК}(n, m) | u$.

Свойства (1) и (2) оправдывают сокращенные обозначения НОД и НОК наибольшего общего делителя и наименьшего общего кратного чисел n, m. При $n, m > 0$ выполнено соотношение

$$\text{НОД}(n, m) \cdot \text{НОК}(n, m) = nm.$$

Целые числа n, m называются *взаимно простыми*, если $\text{НОД}(n, m) = 1$.

Алгоритм деления в $\mathbb{Z}$.

При заданных $a, b \in \mathbb{Z}$, $b > 0$, всегда найдутся такие $q, r \in \mathbb{Z}$, что

$$a = bq + r, \quad 0 \leqslant r < b.$$

Доказательство. В самом деле, множество

$$S = \{a - bs \mid s \in \mathbb{Z}, a - bs \geqslant 0\},$$

очевидно, непусто. Значит, множество S содержит наименьший элемент; обозначим его $r = a - bq$. По условию $r \geqslant 0$. Предположим, что $r \geqslant b$, тогда получим, что элемент

$$r - b = a - b(q + 1) \in S$$

меньше r. Таким образом, $r < b$. □

Теперь при заданных числах n, m, одновременно не равных нулю, положим

$$J = \{nu + mv \mid u, v \in \mathbb{Z}\}.$$

Выберем в J наименьший положительный элемент $d = nu_0 + mv_0$. Используя деление с остатком, запишем $n = dq + r$, $0 \leqslant r < d$. Ввиду выбора d включение

$$r = n - dq = n - (nu_0 + mv_0)q = n(1 - u_0q) + m(-v_0q) \in J$$

влечет равенство $r = 0$. Значит, $d|n$. Аналогично доказывается, что $d|m$.

Пусть теперь d' — любой делитель чисел n и m. Тогда

$$d'|n, d'|m \Longrightarrow d'|nu_0, d'|mv_0 \Longrightarrow d'|(nu_0 + mv_0) \Longrightarrow d'|d.$$

Итак, d обладает всеми свойствами наибольшего общего делителя, поэтому $d = \text{НОД}(n, m)$. Мы приходим к следующему утверждению:

Теорема 5. *Наибольший общий делитель двух целых чисел, не равных одновременно нулю, всегда записывается в виде*

$$НОД(n, m) = nu + mv, \quad u, v \in \mathbb{Z}.$$

В частности, целые числа n, m взаимно просты тогда и только тогда, когда

$$nu + mv = 1$$

для некоторых $u, v \in \mathbb{Z}$.

ВЕКТОРНЫЕ ПРОСТРАНСТВА СТРОК И СТОЛБЦОВ

Пусть n — какое-то фиксированное натуральное число. *Векторным пространством строк длины* n над $\mathbb{R}$ называется множество $\mathbb{R}^n$ (его элементами являются векторы-строки или просто векторы), рассматриваемое вместе с операциями сложения векторов и умножения их на скаляры — вещественные числа.

Скаляры обычно обозначаются строчными буквами латинского или греческого алфавита, а векторы — заглавными латинскими буквами, как матрицы.

По существу на вектор $X = (x_1, x_2, \ldots, x_n)$ можно смотреть как на матрицу размера $1 \times n$. Пусть $Y = (y_1, y_2, \ldots, y_n)$ — еще один вектор, λ — скаляр. По определению

$$X + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$
$$\lambda X = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n).$$

Нулевой вектор $(0, 0, \ldots, 0)$ будем просто обозначать символом 0. Прямую $\mathbb{R}^1$ принято отождествлять с $\mathbb{R}$.

Свойства введенного пространства распространяются и на абстрактные пространства (множества) с операциями сложения и умножения на числа.

Покажем, что принято понимать под *абстрактным векторным пространством.*

Векторным пространством называется множество с операциями сложения и умножения (слева) на числа, обладающее следующими восемью свойствами:

1. $X + Y = Y + X$ для любых векторов X, Y (закон коммутативности);

2. $(X+Y)+Z) = X+(Y+Z)$ для любых трех векторов X, Y, Z (закон ассоциативности);

3. существует специальный (нулевой) вектор 0 такой, что $X + 0 = X$ для всех X;

4. для каждого X существует противоположный вектор $-X$, для которого $X + (-X) = 0$;

5. $1 \cdot X = X$ для всех X;

6. $(\alpha\beta)X = \alpha(\beta X)$ для всех чисел α, β и векторов X;

7. $(\alpha + \beta)X = \alpha X + \beta X$ для всех чисел α, β и векторов X;

8. $\alpha(X + Y) = \alpha X + \alpha Y$ для всех чисел α и векторов X, Y.

Единственность векторов 0 и $-X$ можно легко вывести. Например, если есть 0_1 и 0_2, то

$$0_1 = 0_1 + 0_2 = 0_2,$$

если $X + Y = 0$, $X + Z = 0$, то

$$Z = 0 + Z = (Y + X) + Z = Y + (X + Z) = Y + 0 = Y.$$

Наряду с векторным пространством строк рассматривают и векторное пространство столбцов высоты n.