Семинар 6

Возведение цикла в степень

Пусть $\rho = (1, 2, \ldots, k) \in \mathrm{S}_n$ – некоторый цикл длины k. Давайте найдем его произвольную степень $(1, 2, \ldots, k)^m$. Мы знаем, что результат будет какой-то перестановкой, а любая перестановка раскладывается в произведение независимых циклов. Оказывается, что все эти циклы будут иметь одну длину, точнее ответ такой

$$(1, 2, \ldots, k)^m = \rho_1 \cdot \ldots \cdot \rho_s$$

Где $s = (m, k)$, а длины всех циклов $k/(m, k)$. Тут надо сделать важное замечание, если $k|m$, то $s = k$. А это значит, что мы получаем k циклов длины 1 или другими словами тождественную перестановку. Потому эта формулировка корректна только для формальных циклов, где мы в перестановке все неподвижные точки считаем циклами длины 1. Вот пример

$$(1, 2, 3)^6 = (1)(2)(3)$$

Если же мы хотим сформулировать утверждение для настоящих циклов, то надо быть чуть аккуратнее и сказать следующее. Если $k|m$, то $(1, \ldots, k)^m$ вообще не содержит циклов, так как это тождественная перестановка. А если $k\nmid m$ то верна формула выше для обычных циклов. То есть при возведении в степень количество циклов:

1. либо не меняется
2. либо увеличивается
3. либо все циклы пропадают

А если мы говорим про формальные циклы, то формулировка говорит, что количество формальных циклов не уменьшится. В силу этого намного удобнее в таких задачах использовать формальные циклы, а не только настоящие циклы. Кроме того, формальные циклы помогают не забыть про все элементы, на которых мы действуем, даже если они неподвижные. Например, если $\sigma = (1, 2, 3) \in \mathrm{S}_3$ или $\sigma = (1, 2, 3) \in \mathrm{S}_4$, то их никак нельзя отличить по настоящим циклам и можно забыть, что у нас была еще точка 4. Однако запись $\sigma(1, 2, 3)(4)$ помогает не забыть про наличие этой точки. Тем не менее, бывают ситуации, когда наоборот удобнее не использовать формальные циклы.

Давайте проведем доказательство в два шага:

1. Покажем результат в двух частных случаях
2. Сведем общий случай к этим двум частным

Случай $(k, m) = 1$ В начале я хочу сделать полезное замечание. Если у вас есть цикл $\sigma = (1, 2, \ldots, k)$, то при возведении в степень он может только распасться на несколько независимых циклов. Если же у вас есть произведение независимых циклов $\rho_1 \ldots \rho_s$, то при возведении в степень каждый из них может только распасться на еще большее количество циклов, но они никогда не могут собраться в один больший цикл. Это я оставлю на осознать по методу пристального взгляда. Еще одно замечание $(1, 2, \ldots, k)^k = \mathrm{Id}$ – тождественная перестановка.

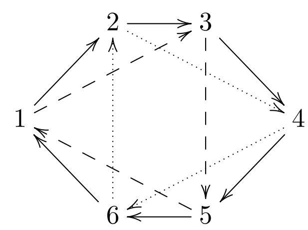
Теперь рассмотрим $\eta = (1, 2, \ldots, k)^m$. Нам надо показать, что то, что получится будет циклом длины k. Как это показать? Давайте для начала найдем такое число $a \in \mathbb{Z}$, что $\eta^a = (1, 2, \ldots, k)$. Тогда из этого будет следовать, что η – цикл. Действительно, если бы $\eta = \rho_1 \ldots \rho_s$ было произведение независимых циклов, то η^m будет состоять как минимум из s циклов по замечанию выше.

Теперь займемся поисками волшебного числа a. Для этого воспользуемся тем, что $(m, k) = 1$. Мы знаем, что НОД представляется в виде линейной комбинации, то есть найдутся такие числа $a, b \in \mathbb{Z}$, что $1 = am + bk$. Давайте рассмотрим

$$\eta^a = (1, 2, \ldots, k)^{am} = (1, 2, \ldots, k)^{1-bk} = (1, 2, \ldots, k)((1, 2, \ldots, k)^k)^{-b} = (1, 2, \ldots, k)$$

Ну и все. Значит в этом случае у нас цикл остается циклом.

Случай $m \mid k$ Давайте покажем, что в этом случае цикл $\sigma = (1, 2, \ldots, k)$ распадется в m циклов одинаковой длины. Давайте возьмем элемент 1 и подействуем на него σ m раз. Тогда он перейдет в $m+1$, после этого перейдет в $2m+1$ и так далее. Так как k делится на m, то после k/m итераций мы попадем в исходный элемент 1. Ниже картинка для $k = 6$ и $m = 2$:



Мы видим, что у нас есть m опций для начала нового цикла – это элементы с 1 по m. Значит у нас будет m циклов, а их длины равны, потому что процедура проходит одинаково, независимо от того, с какого элемента мы стартовали. В итоге получаем, что у нас m циклов длины k/m.

Общий случай Пусть теперь m и k произвольные и пусть $d = (m, k)$. Тогда

$$(1, 2, \ldots, k)^m = ((1, 2, \ldots, k)^d)^{\frac{m}{d}}$$

Тогда по второму случаю $(1, 2, \ldots, k)^d$ распадается в d циклов длины k/d. То есть

$$((1, 2, \ldots, k)^d)^{\frac{m}{d}} = (\rho_1 \ldots \rho_d)^{\frac{m}{d}} = \rho_1^{\frac{m}{d}} \ldots \rho_d^{\frac{m}{d}}$$

Но теперь каждый цикл ρ_i имеет длину k/d, а значит его длина взаимнопроста со степенью m/d. То есть $\rho_i^{m/d}$ остается циклом той же длины по первому случаю.

Извлечение корня из цикла по всем элементам

Рассмотрим цикл $(1, \ldots, n) \in \mathrm{S}_n$ и попробуем решить уравнение $\sigma^m = (1, \ldots, n)$ для $\sigma \in \mathrm{S}_n$. Обратите внимание, что в этой задаче важно, что σ действует на n элементах или другими словами, что цикл и в правой части уравнения проходит по всем элементам. Давайте рассмотрим два случая.

В начале сделаем общее замечание, которое годится для всех случаев, которые будут рассмотрены ниже. Если $\sigma^m = (1, \ldots, n)$, то σ сама является циклом по всем элементам $\{1, \ldots, n\}$ но быть может в другом порядке. Действительно, если бы $\sigma = \rho_1 \ldots \rho_k$ было бы произведением нескольких циклов, то $\sigma^m = \rho_1^m \ldots \rho_k^m$ будет произведением не менее k циклов (считая тривиальные). То есть не может быть циклом по всем элементам.

1. $(m, n) = 1$. В этом случае давайте докажем, что существует единственное решение и найдем его. В этом случае $1 = am + bn$ для некоторых $a, b \in \mathbb{Z}$. Рассмотрим любое решение $\sigma^m = (1, \ldots, n)$. Покажем, что $\sigma = (1, \ldots, n)^a$. Действительно, если $\sigma^m = (1, \ldots, n)$, то можно возвести обе части в степень a и получим

   $$(1, \ldots, n)^a = \sigma^{am} = \sigma^{1-bn} = \sigma(\sigma^n)^a$$

   Теперь воспользуемся тем, что σ – цикл длины n, а значит $\sigma^n = \mathrm{Id}$. Значит

   $$\sigma(\sigma^n)^a = \sigma(\mathrm{Id})^a = \sigma$$

   То есть мы показали, что для любого решения уравнения $\sigma^m = (1, \ldots, n)$ выполнено равенство $\sigma = (1, \ldots, n)^a$.

2. $(m, n) \neq 1$. В этом случае покажем, что решений нет. Так как в этом случае σ цикл длины n, то $\sigma^m = \rho_1 \ldots \rho_d$, где $d = (m, n) \neq 1$. То есть при возведении σ в степень m мы никогда не получим один цикл. А значит решений нет.