Math 68 - Algebraic Combinatorics

Nadia Lafrenière

Necklaces

10/18/2019

A necklace of length ℓ is a circular arrangement of ℓ colored beads, and two necklaces are considered equivalent if they are the same up to a cyclic rotation

Here, the group that acts on the necklace is $\mathbb{Z}_\ell$.

Problem

Given a set of uncolored beads, how many inequivalent necklaces can we build out of it, if we have n colors?

We know from the previous class that this number is

$$N_{\mathbb{Z}_\ell}(n) = \frac{1}{\# \mathbb{Z}_\ell} \sum_{\sigma \in \mathbb{Z}_\ell} n^{c(\sigma)},$$

where $c(\sigma)$ is the number of cycles in σ

How many cycles does it have?

Proposition

Let π be the rotation of angle $2\pi/\ell$ (so a primitive element of $\mathbb{Z}_\ell$). The number of cycles in π^k is $\gcd(k,\ell)$.

Proof

If $\gcd(k,\ell)=d$, then the cycles of π^k are $(0, d, 2d, \ldots, \underbrace{(\frac{\ell}{d}-1)d}_{\ell-d})$, $(1, d+1, 2d+1, \ldots, \ell-d+1), \ldots, (d-1, 2d-1, \ldots, \ell-1)$. These cycles are disjoint.

So we can rewrite

$$N_{\mathbb{Z}_\ell}(n) = \frac{1}{\ell} \sum_{1 \le k \le \ell} n^{\gcd(k,\ell)}$$

$$= \frac{1}{\ell} \sum_{d \mid \ell} \sum_{\substack{1 \le k \le \ell \\ \gcd(k,\ell)=d}} n^d$$

$$= \frac{1}{\ell} \sum_{d \mid \ell} n^d \cdot \# \{ 1 \le k \le \ell \mid \gcd(k,\ell) = d \}$$

$$= \frac{1}{\ell} \sum_{d \mid \ell} n^d \cdot \# \{ 1 \le \tfrac{k}{d} \le \tfrac{\ell}{d} \mid \gcd(\tfrac{k}{d}, \tfrac{\ell}{d}) = 1 \}$$

$$= \frac{1}{\ell} \sum_{d \mid \ell} n^d \cdot \phi(\ell/d)$$

Euler-Phi function:
$\phi(n) = \#$ of integers smaller than and coprime with n.

Theorem

The number of inequivalent necklaces of length ℓ with n colors is

$$N_{\mathbb{Z}_\ell}(n) = \frac{1}{\ell} \sum_{d \mid \ell} n^d \phi(\ell/d).$$

The generating function of inequivalent necklaces of length ℓ with i_j beads of color r_j is

$$F_{\mathbb{Z}_\ell}(r_1, \ldots, r_n) = \frac{1}{\ell} \sum_{d \mid \ell} \phi(d) (r_1^d + r_2^d + \ldots + r_n^d)^{\ell/d}$$

Proof of the second part.

We first need to compute the cycle indicator.

$$Z_{\mathbb{Z}_\ell} = \frac{1}{\ell} \sum_{1 \le k \le \ell} z_1^{c_1} z_2^{c_2} \cdots z_k^{c_k} = \frac{1}{\ell} \sum_{d \mid \ell} z_{\ell/d}^{d} \phi(\ell/d)$$

③

Then, we can use Pólya's theorem to get

$$F_{\mathbb{Z}_\ell}(r_1,\dots,r_n) = \frac{1}{\ell}\sum_{d\mid \ell} \phi(\ell/d)\,(r_1^{\ell/d} + r_2^{\ell/d} + \dots + r_n^{\ell/d})^d$$

$$= \frac{1}{\ell}\sum_{d\mid \ell} \phi(d)\,(r_1^{d} + r_2^{d} + \dots + r_n^{d})^{\ell/d}$$

by substituting d by ℓ/d. d divides ℓ iff ℓ/d divides ℓ.

Notice that this definition of necklace should be considered as a necklace that is currently worn by someone, since no symmetry is allowed (we must remove the necklace from someone's neck to be able to apply a symmetry). A necklace to which we can apply symmetries is a dihedral necklace.

What if the number of beads is a prime number?

Then $N_{\mathbb{Z}_p}(n) = \frac{1}{p}\sum_{d\mid p} n^d \phi(p/d) = \frac{1}{p}\left(n\cdot\phi(p) + n^p\phi(1)\right) = \frac{1}{p}\left((p-1)n + n^p\right)$

A primitive necklace is a necklace with no symmetries (i.e. no non-identity rotation preserves it).

How many primitive necklaces of length ℓ are there?

If ℓ is prime, then these corresponds to the necklaces whose beads are not all the same color: $\frac{1}{p}(n^p - n)$

Otherwise, we need more sophisticated techniques.

First, observe that a non-primitive necklace is a sequence of length $d \mid \ell$ $(d \neq \ell)$ that is repeated ℓ/d times.

Let $M_\ell(n)$ be the number of primitive necklaces of length ℓ. Then,

$$N_{\mathbb{Z}_\ell}(n) = \sum_{d\mid \ell} M_d(n)$$

To solve this equation, one can think of the divisors' lattice, and then use Möbius inversion

$$M_\ell(n) = \sum_{d|\ell} \underbrace{\mu(d,\ell)}_{\mu(\ell/d)} N_{\mathbb{Z}_d}(n)$$

$\mu(\ell/d)$, because the interval of D_ℓ starting at d is isomorphic to $D_{\ell/d}$.

Plugging the value of $N_{\mathbb{Z}_d}(n)$, and by computations, one can get the following:

Theorem

The number of primitive necklaces of length ℓ is
$$M_\ell(n) = \frac{1}{\ell}\sum_{d|\ell} \mu(\ell/d)\, n^d.$$

Example

With p prime, we recover what we first computed: $\frac{1}{p}(n^p - n)$.

$$M_p(n) = \frac{1}{p}\sum_{d|p} \mu(p/d)\, n^d$$
$$= \frac{1}{p}\left(\mu(p)\, n + \mu(1)\, n^p\right)$$
$$= \frac{1}{p}(n^p - n).$$

References: Richard P. Stanley Algebraic Combinatorics §7.