utopia
Math Blog

A Combinatorial Proof for Fermat's Little Theorem

Posted on May 24, 2015 by keriimov

Fermat's Little Theorem states that if p is a prime number and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$. There exist many proofs for this theorem but among the proofs, there is the one which is more interesting for me. The following proof uses Burnside's Lemma which is an important theory in Combinatorics.

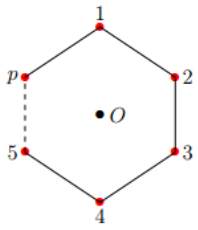
Burnside's Lemma. If G is a finite group of permutations of a finite set X, then the number of orbits of G on X is

$$\frac{1}{|G|}\sum_{\phi \in G} |\mathrm{fix}(\phi)|,$$

where $\mathrm{fix}(\phi) = \{x \in X \mid \phi(x) = x\}$.

For combinatorial purposes, we may consider G as a rotation group and orbits as equivalance classes for rotationally distinct colorings of X. For instance, one can define a rotation group on a cube and find the number of rotationally distinct colorings of the faces of a cube using Burnside's Lemma. Actually, it can be shown that the number of rotationally distinct colorings of the faces of a cube with k different colors is $\frac{1}{24}(k^6 + 3k^4 + 12k^3 + 8k^2)$, where the rotations are defined in a natural manner.

The combinatorial proof for Fermat's Little Theorem proceeds as follows: Consider the following p-gon where p is a prime number:



The natural way to define the rotation group is considering the rotations with respect to the center of the polygon, which is denoted by O in the figure above. Thus, the elements of G has form $(k\frac{360}{p})^\circ$ for $k = 0, 1, 2, ..., p-1$ and it immediately follows that $|G| = p$. Suppose that we want to find the number of rotationally distinct colorings of the corners of a p-gon with a different colors. Notice that, we automatically assume $p > 2$ and $a \in \mathbb{N}$. But once we prove Fermat's Little Theorem for $a \in \mathbb{N}$, we directly have the theorem for $a \in Z$. Now, in order to apply Burnside's Lemma, we need to find $|\mathrm{fix}(\phi)|$ for each $\phi \in G$.

For $k = 0$, the corresponding group element fixes all possible colorings of the polygon, that is a^p.

Now let $k = 1$. It is clear that in order to keep the same color configuration after the action of this rotation, all the colors of corners must be the same. Thus, this rotation fixes a elements.

It is also easy to see that the other rotations corresponding to $k = 2, 3, ..., p-1$ fix a elements each as well. It follows from the fact that p is prime. Then by Burnside's Lemma, the number of rotationally distinct colorings of the corners of a p-gon with a different colors is

$$\frac{1}{|G|}\sum_{\phi\in G}|\mathrm{fix}(\phi)| = \frac{1}{p}(a^p + \underbrace{a+a+\ldots+a}_{p-1 \text{ times}}) = \frac{1}{p}(a^p+(p-1)a).$$

Since the last expression gives the number of colorings, $a^p+(p-1)a$ must be divisible by p. That is, $a^p+(p-1)a \equiv 0 \pmod{p} \Rightarrow a^p - a \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$.

About keriimov
Senior at Bilkent University Department of Mathematics.
View all posts by keriimov →

This entry was posted in Combinatorics. Bookmark the permalink.
