Worksheet 6

Math 391, Abstract Algebra

Monday, October 12, 2020

In lecture we gave a proof of Proposition 3.3, called Fermat's little theorem: if p is prime and n is any (positive) integer then

$$n^p \equiv n \pmod{p}.$$

Here's an outline of another proof. Work through it together, convincing yourselves that each claim is correct.

1. Consider a necklace with p beads, and all the ways of labeling each bead with a number between 1 and n. There are n^p different ways to do this.

2. Within that set of n^p labeled necklaces, we consider two different kinds: the "constant" necklaces, where every bead is labeled with the same number, and the "non-constant" necklaces. There are n of the former and $n^p - n$ of the latter.

3. Divide the non-constant necklaces into groups as follows: two necklaces belong to the same group if you can fasten the clasps and rotate them so that they match up. Then each group has p necklaces in it.

   (Here it's important that p is prime!)

4. Thus $n^p - n$ is a multiple of p, so $n^p \equiv n \pmod{p}$.

5. Draw the picture for $n = 2$ and $p = 3$: write down all eight necklaces, cross off the two constant necklaces, and put the six non-constant necklaces into two groups of three.

6. See where the proof breaks if p is not prime, by drawing the picture for $n = 2$ and $p = 4$.