## EECS 70 Discrete Mathematics and Probability Theory Spring 2014 Anant Sahai Discussion 10A

## 1. ANAGRAMS

An anagram of a word is any re-ordering of the letters of the word, in any order. It does not have to be an English word.

- (a) How many different anagrams of FLORIDA are there?
- (b) How many different anagrams of ALASKA are there?
- (c) How many different anagrams of MONTANA are there?

## 2. Fermat's necklace: a combinatorial proof

Let p be a prime number and let k be a positive integer. We have an endless supply of beads. The beads come in k different colors. All beads of the same color are indistinguishable.

- (a) We have a piece of string. We want to make a pretty decoration by threading p beads onto the string. How many different ways are there construct such a sequence of p beads of k different colors?
- (b) Now, there's a restriction. All the beads cannot be of just one color. Now, how many different sequences exist? (Your answer should be a simple function of k and p.)
- (c) Now we tie the two ends of the string together, forming a circular necklace which lets us freely rotate the beads around the necklace. We'll consider two necklaces equivalent if the sequence of colors on one can be obtained by rotating the beads on the other. (For instance, if we have k = 3 colors—red (R), green (G), and blue (B)—then the length p = 5 necklaces RGGBG, GGBGR, GBGRG, BGRGG, and GRGGB are all equivalent, because these are cyclic shifts of each other.) How many non-equivalent sequences are there now? Again, the *p* beads must not all have the same color. (Your answer should be a simple function of *k* and *p*.)
  [Hint: What follows if rotating all the beads on a necklace to another position produces an identical looking necklace?]
- (d) Use your answer to part (c) to prove Fermat's little theorem. (Recall that Fermat's little theorem says that if p is prime and  $a \neq 0 \pmod{p}$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .)