MATH 565 Spring 2019 - Class Notes

2/27/19

Scribe: Alyssa Eller

0.1 Combinatorics

0.1.1 Basic Combinatorial Principle

If α can be selected from a set S in m ways and β can be selected from a set T in n ways then the number of pairs α, β is nm.

Let r denote permutations. Count the number of ways to choose r things from a set of size n. Denote this by

$$^{n}P_{r} = n(n-1)(n-2)...(n-r+1)$$

Proof. Define k to be $n - r$ +1.

Base Case: r=1

$$^{n}P_{r} = {}^{n}P_{1}$$

counts the ways to pick one object from n things.

$$n - 1 + 1 = n$$

$$n = n$$

Induction Hypothesis: Assume that the theorem holds for $^{m}P_{(}r-1)$ so the number of ways to pick $r-1$ things from a set of size m is

$$m(m-1)...(m-(r-1)+1)$$

Now we want to count $^{n}P_{r}$. We can pick the first object in n ways. Now there are $r-1$ more choices that need to be made. These can be picked from $(n-1)$ things. This is counted by $^{n}P_{-}1r-1$.

Our induction hypothesis tells us this is

$$(n-1)(n-2)(...)((n-1)-(r-1)+1)$$

$$(n-1)(n-2)(...)(n-r+1)$$

Now we use the basic combinatory principle to say that the total number is

$$
\begin{aligned}
{}^{n}P_{r} &= n * {}^{(}P_{n} - 1)(r-1) \\
&= n((n-1)...(n-(r-1))) \\
&= n((n-1)...(n-r+1))
\end{aligned}
$$

□

Note: Order matters in permutations. Picking 2 things from a set of size 5:

$$(a, c) \neq (c, a) \tag{1}$$

A combination is the number of ways to pick r things from n objects if order doesn't matter. Write this as ${}^{n}C_{r}$, "n choose r."

Pick r-permutations of n, each r combination shows up $r!$ different times.

$$\binom{n}{r}$$

$$*r! = {}^{n}P_{r}$$

$$\binom{n}{r}$$

$$= \frac{{}^{n}P_{r}}{r!} = \frac{n!}{(n-r)!r!} = \frac{n(n-1)...(n-r+1)}{r(r-1)...(1)}$$

Theorem 1. *The product of any n consecutive integers is divisible by the product of the first n integers.*

Example: $7 * 8 * 9$ is divisible by $6 = 1 * 2 * 3$.

Proof. Let N be the largest of the numbers in the product of consecutive integers.

$$N * (N-1) * (N-2)...(N-n+1)$$

Want to prove this is divisible by n! Count the number of ways to pick n things from a set of size N.

$$\binom{N}{n}$$

$$= \frac{N!}{(N-n)!n!} = \frac{N(N-1)...(N-n+1}{n!}$$

But

$$\binom{N}{n}$$

has to be an integer because it's counting something.

$$N(N-1)...(N-n+1) = n!$$

* $\binom{N}{n}$

so this product is divisible by n!

□

0.1.2 Fermat's Little Theorem

Theorem 2. *If $a > 1$ and in integer and p is prime then*

$$p \mid (a^p - a)$$

.

Examples:

$p = 3, a = 2$
$a^3 - a = 2^3 - 2 = 8 - 2 = 6 \implies 3 \mid 6$

$p = 7, a = 2$
$a^7 - a = 2^7 - 2 = 126 \implies 7 \mid 126$

$p = 5, a = 3$
$3^5 - 3 = 240 \implies 5 \mid 240$

Proof. Count bracelets that can be made out of p beads and a choices of colors.

Note: Let R=red, B=blue, Y=yellow and G=green

Make bracelets by putting beats on a string and tying the two ends together.

Monochromatic: R-R-R or B-B-B

Multi-colored: R-B-R is the same bracelet as R-R-B, but they are two different strands. When connected, the blue bead is in between two red beads.

Note that you are not allowed to flip a bracelet R-G-B-Y $\neq Y - B - G - R$.

Count strands: a choices for the first bead, a choices for the second, third, ...

There are a^p possible strands, with $a = 2$ possibilities and $p = 3$ choices to make, giving us 8 strands in total:

R-R-R, R-R-B, R-B-B, R-B-R, B-R-B, B-R-R, B-B-R, B-B-B.

Notice that there is 1 bracelet with all red beads, 1 bracelet with all blue beads, 3 bracelets with 2 red beads and 1 blue bead, and 3 bracelets with 2 blue beads and 1 red bead.

Of these a^p strands, exactly a of them are monochromatic $a^p - a$ multicolored strands.

How many times does each multicolor bracelet get produced by different strands? Take a strand and move k beads from the top to the bottom without changing their order, then we product the same bracelet.

Pick a multicolor strand and let q be the least number of beads we can move from top to bottom to get the same strand. If we do this with $2q, 3q, 4q, ...$ beads, we still get the same strand. Moving all p beads from the top to the bottom is the same strand.

So $p = iq$ for some i so q is either 1 or p. If $q = 1$, the strand is monochromatic so if we have a multicolor strand, $q = p$. So each strand is part of a family of $p = q$ different strands that all produce the dame bracelet.

So our $a^p - a$ muticolor strands can be divided evenly into families of size p so $p \mid (a^p - a)$. $\square$