Math 155 (Lecture 1)

August 30, 2011

This course is meant to serve as an introduction to the study of combinatorics. We might therefore begin by asking the question: what is combinatorics? According to Wikipedia, combinatorics is "a branch of mathematics concerning the study of finite or countable discrete structures." Of course, this definition is very broad, and encompasses many more topics than we can discuss in a one-semester course. After canvassing some experts, I've come to the conclusion that there is no real consensus as to what should be taught in a course like this one.

What can we say about finite mathematical structures? One answer is obvious: if a set is finite, we can ask how many elements it has. This leads to the subject of *enumerative combinatorics*, which is concerned with counting problems.

Example 1. Let $S = \{1, \ldots, m\}$ and $T = \{1, \ldots, n\}$ be finite sets. How many functions are there from S to T? Since there are m choices for where each element of S can go, the answer is n^m.

Example 2. Let $S = \{1, \ldots, n\}$ be a set with m elements. Then there are precisely n^n functions from S to itself. How many of these functions are permutations of S? Recall that a permutation of S is a bijective map $\pi : S \to S$. Since there are n choices for $\pi(1)$, $(n-1)$ remaining choices for $\pi(2)$, and so forth, we see that the number of permutations is

$$n! = n(n-1)(n-2)\cdots(3)(2)(1)$$

Example 3. Let $S = \{1, \ldots, n\}$ be a set with n elements. A *derangement* of S is a permutation of S with no fixed points: that is, a permutation π such that $\pi(i) \neq i$ for $1 \leq i \leq n$. How many derangements does the set S has? What is the probability that a randomly chosen permutation is a derangement? (This question has an interesting and perhaps surprising answer. We will later see that as n grows, the probability approaches $\frac{1}{e}$, where e is Euler's constant.)

Example 1 is a completely elementary observation. Nevertheless, with a little bit of cleverness, one can extract some interesting consequences.

Theorem 4 (Fermat's Little Theorem)**.** *Let n be an integer and let p be a prime number. Then*

$$n^p \equiv n \ (mod\ p).$$

Theorem 4 is an absolutely fundamental result in number theory. It has many proofs; we will sketch one that uses Example 1 and some other basic counting principles.

Proof. We might as well assume that n is nonnegative (otherwise, replace n by $-n$). We wish to show that the difference $n^p - n$ is divisible by p: in other words, that $n^p = n + pd$ for some integer d. Let X denote the collection of all functions from the set $\{1, \ldots, p\}$ to the set $\{1, \ldots, n\}$. We will denote the number of elements of X by $|X|$, so that $|X| = n^p$.

Now let us observe that the set X has some *symmetry*: there is a translation map $T : X \to X$, given by the formula

$$(Tf)(i) = \begin{cases} f(i-1) & \text{if } i > 1 \\ f(p) & \text{if } i = 1. \end{cases}$$

We can therefore partition the set X into two subsets:

- Let X_0 denote the collection of functions $f : \{1, \ldots p\} \to \{1, \ldots, n\}$ which are *translation invariant*: that is, which satisfy $Tf = f$. This means that $f(i) = f(i+1)$ for $0 < i < p$, so that the function f is necessarily constant. There is one element of X_0 for every element of $\{1, \ldots, n\}$, so that $|X_0| = n$.

- Let X_1 be the collection of all functions $f : \{1, \ldots, p\} \to \{1, \ldots, n\}$ which are *not* translation invariant: that is, which satisfy $Tf \neq f$. It then follows (since p is a prime number) that the functions $Tf, T^2 f, \ldots, T^{p-1} f, T^p f = f$ are all distinct (and also belong to X_1). It follows that the set X_1 can be partitioned into finitely many subsets, each of which has size exactly p, so that the number of elements of X_1 is divisible by p.

We now conclude the proof by noting that

$$n^p = |X| = |X_0| + |X_1| = n + pd.$$

□

Let us now isolate some of the principles at work in the proof of Theorem 4.

(a) One way to prove that two numbers are equal is to try to solve a counting problem in two different ways.

(b) If a set S is given as a disjoint union of subsets S_0 and S_1, then $|S| = |S_0| + |S_1|$. Using this, we can often break a complicated counting problem down into simpler constituents.

(c) Studying symmetries can give lots of useful information.

We will meet many other counting principles (some of which are quite a bit more sophisticated) later in this course.

Of course, combinatorics is not just about counting problems: there are all sorts of other questions one can ask about finite mathematical structures. To give another example, it will be useful to introduce a definition.

Definition 5. A *graph* consists of a set V (whose elements are called *vertices*) together with a collection E of 2-element subsets of V (whose elements are called *edges*).

If G is a graph, it is helpful to think of the collection of edges of G as a *relation* on the set V of vertices: we say that a pair of vertices v and w are *adjacent* if the set $\{v, v'\}$ is an edge of G. This relation is symmetric (if v is adjacent to w, then w is also adjacent to v) and antireflexive (no vertex is adjacent to itself).

Example 6. For every integer n, there is a graph K_n whose vertex set is given by $V = \{1, \ldots, n\}$, and whose edge set is given by the collection of all two-element subsets of V (in other words, every pair of distinct vertices of V is connected by an edge). The graph K_n is called the *complete graph on n vertices*.

If G is a graph, then a *clique* of size n is an embedding $K_n \hookrightarrow G$. In other words, a clique of size n is a collection of n vertices of G, every one of which is adjacent to each of the others. A typical question might read something like the following:

(Q) Given a graph G, how large a clique can we find? If G is sufficiently large, is it guaranteed to have large cliques?

Of course, the answer to this question is "no" in general: if G is a graph with no edges, then it has no cliques of size ≥ 2. However, such a graph will generally have very large *anti-cliques*: an anti-clique is a collection of vertices, every one of which is *not* adjacent to any of the others.

Here is an example of one of the theorems we will prove in this class:

Theorem 7 (Ramsey's Theorem). *Let $k \geq 0$ be an integer. Then there exists an integer n such that, for any graph G with at least n vertices, either G contains a clique of size k or G contains an anti-clique of size k.*