Chapter 5: Picking and choosing.

Recall last time: total number of usernames like “ss518” (two letters (a-z) followed by three numbers (0-9)) is
$26 \times 26 \times 10 \times 10 \times 10$.
Let’s formalise the technique we just used.

Multiplication principle.

Let P be a process with n steps, and suppose that for $1 \leq r \leq n$ the number of choices for the rth step is a_r, independent of which choices are made in the first $r-1$ steps. Then the process can be done in $a_1 a_2 a_3 \cdots a_n$ ways.

Depending on your point of view, this is either completely obvious, or can be proved by induction on n.

Example. how many even 2-digit numbers are there whose digits are distinct elements of the set $\{1, 2, 3, 4, 5, 6\}$?

Example. how many even 2-digit numbers are there whose digits are distinct elements of the set $\{1, 2, 3, 4, 5, 6\}$?
We need to design a process for which we can apply the multiplication principle.
Idea: choose the second digit first.

Our process can be: in step 1, choose the second digit – the "units digit" (three choices), and then in step 2 choose the "tens digit" (five choices).

Note: the *actual choices available to us* for the tens digit will depend on what we choose for the units digit. For example, if we choose 4 for the units digit, then our choices for the tens digit are $\{1, 2, 3, 5, 6\}$, but if we choose 6 then our choices are $\{1, 2, 3, 4, 5\}$.

However, the multiplication principle works, because the *number* of choices for the second step is always 5.
The multiplication principle says that the total number of choices is $3 \times 5 = 15$.

Say S is a set with $n \in \mathbb{Z}_{\geq 0}$ elements. How many ways are there of "linearly ordering S"? In other words, how many ways can we re-arrange the elements of S into a list $s_1, s_2, \ldots, s_n$?

For example, if $S = \{A, B, C\}$ then there are six ways:
A, B, C
A, C, B
B, A, C
B, C, A
C, A, B
C, B, A

Recall that $n! := \prod_{i=1}^{n} i = 1 \times 2 \times \cdots \times (n-1) \times n$.
(note that 0! is the empty product, which is the unit for multiplication, which is 1).

Multiplication principle.
Let P be a process with n steps, and suppose that for $1 \leq r \leq n$ the number of choices for the rth step is a_r, independent of which choices are made in the first $r-1$ steps. Then the process can be done in $a_1 a_2 a_3 \cdots a_n$ ways.

Proposition 5.1. There are $n!$ ways of linearly ordering a set of size n.

Proof. We order S using the following n-step process: for the first step, we choose the first element, in the second step we choose the second element, and so on.

By the multiplication principle, the number of ways of doing this is $n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!$.

$\square$

Definition 5.2. If $r, n \in \mathbb{Z}_{\geq 0}$ with $0 \leq r \leq n$, define the *binomial coefficient* $\binom{n}{r}$ to be the number of r-element subsets of a set of size n.

Example. $\binom{4}{2} = 6$, because if S is the four-element set $\{A, B, C, D\}$ then the full list of two-element subsets are $\{A, B\}$, $\{A, C\}$, $\{A, D\}$, $\{B, C\}$, $\{B, D\}$, $\{C, D\}$.

In the below examples, let S be a set of size n.

Example. If $0 \leq r \leq n$ then $\binom{n}{r} = \binom{n}{n-r}$. Why? There is a *bijection* (a one-to-one and onto correspondence) between the r-element subsets of S and the $(n-r)$-element subsets of S – if T is an r-element subset then its complement $S \backslash T$ is an $n-r$-element subset.

Example. If $n \in \mathbb{Z}_{\geq 1}$ then $\binom{n}{1} = n$ (choosing a one-element subset of a set of size n is the same as choosing an element, and there are n elements). Similarly $\binom{n}{n-1} = n$ (because of the previous example).

Example. If $n \in \mathbb{Z}_{\geq 0}$ then $\binom{n}{0} = 1$ (there is only one zero-element subset of S, namely the empty set) and $\binom{n}{n} = 1$ (there is only one n-element subset of S, namely S).

Proposition 5.3. $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

Proof. Let S be a set with n elements. We saw in Proposition 5.1 an n-step process which ordered it. Here is a different process – a three-step process – which also orders it.

Step 1. Choose a subset T of S of size r (this will be the "first r elements of the ordering").

Step 2. Order T, and put these first.

Step 3. Order $S \backslash T$ (the $n - r$ elements of S which are not in T), and put these elements after those in T.

Process to order an n-element set S:

Step 1. Choose a subset T of S of size r (this will be the “first r elements of the ordering”).
Step 2. Order T, and put these first.
Step 3. Order $S \setminus T$ (the $n - r$ elements of S which are not in T), and put these elements after those in T.

By definition there are $\binom{n}{r}$ ways of doing Step 1.

By Proposition 5.1 there are $r!$ ways of doing Step 2, and $(n - r)!$ ways of doing Step 3.

Hence by the multiplication principle there are $\binom{n}{r} r!(n - r)!$ ways of ordering a set with n elements. However by Proposition 5.1 there are $n!$ ways of doing this. Hence $n! = \binom{n}{r} r!(n - r)!$, and the result follows.

$\square$

The *binomial theorem* is a way of expanding $(a+b)^n$. Apparently you all know what it is already. **Happy?** Question: what *are* a and b in the binomial theorem?
The formalist would say that a and b are "commuting elements of an arbitrary ring". This is not much help for a generic M1F student of course! Exercise: Is the binomial theorem true if a and b are arbitrary 2×2 matrices? So let's say a and b are real or complex numbers, or commuting square matrices, or polynomials, or… [commuting elements in an arbitrary ring].

Proposition 5.4. [The Binomial Theorem] If a and b are real numbers (or complex numbers, or polynomial variables, or…, then

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Proposition 5.4. [The Binomial Theorem] If a and b are real numbers (or complex numbers, or polynomial variables, or..., then $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$.

Proof. Do a thought experiment, where you expand out all of the n brackets in $(a+b)^n = (a+b)(a+b)(a+b)\cdots(a+b)$. Clearly a “random” term when you expand it out will be of the form $a^r b^s$ with $r+s=n$. In other words, every term is of the form $a^r b^{n-r}$.

How many times does the term $a^r b^{n-r}$ show up in the product? Well, from each of the n brackets we have to choose a or b, and we need to choose a exactly r times and b the remaining $n-r$ times.

This means that the coefficient of $a^r b^{n-r}$ will be the number of ways to choose r brackets from the n brackets, which is $\binom{n}{r}$ by definition!

$\square$

I think this proof uses "human intuition" and I believe there will be a more formal proof by induction presented in room 342 later on today.
But anyway, we now all believe $(a+b)^n = \sum_{r=0}^n \binom{n}{r} a^r b^{n-r}$.

Corollary 5.5. Say $n \in \mathbb{Z}_{\geq 0}$.

a) $(x+1)^n = \sum_{r=0}^n \binom{n}{r} x^r$.

b) $\sum_{r=0}^n \binom{n}{r} = 2^n$.

c) $\sum_{r=0}^n (-1)^r \binom{n}{r} = 0$ if $n \geq 1$.

Proof. First part: $a = x$ and $b = 1$. Second part: $x = 1$. Third part: $x = -1$ and note that $0^n = 0$ if $n \geq 1$.

$\square$

Multinomial coefficients.

Four students show up late at night at a hotel, and ask for a room for the night. But there are only three rooms left: room 1 is a double room (two students), and room 2 and room 3 are single rooms. How many ways can the students arrange themselves? (just to be clear, switching the students in room 2 and room 3 counts as a different arrangement.)

Definition 5.6 [multinomial coefficient] Say $n, d \in \mathbb{Z}_{\geq 0}$ and we have d non-negative integers r_1, r_2, r_3, ..., r_d with $r_1 + r_2 + \cdots + r_d = n$. The *multinomial coefficient* $\binom{n}{r_1, r_2, \ldots, r_d}$ is defined to be the number of ways we can partition a set S of size n up into d disjoint subsets X_1 of size r_1, X_2 of size r_2, ..., X_d of size r_d.

Example. $\binom{4}{2,1,1} = 12$.

Example. $\binom{n}{r, n-r} = \binom{n}{r}$. Note that the bracket on the left is a multinomial bracket, and the one on the right is a binomial bracket. They are indistinguishable to the naked eye.

Example. Four students play a game of bridge. The way bridge works is that 52 (different!) playing cards are dealt out to the players so they get 13 each. How many ways can we deal the cards out to the four players? (note that if two students decide to swap all their cards with each other, that counts as a different deal).

The answer is $\binom{52}{13,13,13,13}$;-) By definition! Yeah, but what *is* that number?

Theorem 5.7. Say $n, d \in \mathbb{Z}_{\geq 0}$ and $r_1, r_2, \ldots, r_d \in \mathbb{Z}_{\geq 0}$ satisfy $\sum_{i=1}^{d} r_i = n$. Then $\binom{n}{r_1, r_2, \ldots, r_d} = \frac{n!}{r_1! r_2! \cdots r_d!}$.

Proof. Let S be a set of size n, and let's order S using a $d+1$-step process.

Theorem 5.7. Say $n, d \in \mathbb{Z}_{\geq 0}$ and $r_1, r_2, \ldots, r_d \in \mathbb{Z}_{\geq 0}$ satisfy $\sum_{i=1}^{d} r_i = n$. Then $\binom{n}{r_1, r_2, \ldots, r_d} = \frac{n!}{r_1! r_2! \cdots r_d!}$.

Proof. Let S be a set of size n, and let's order S using a $d+1$-step process.

Step 1. Break up S into subsets X_1 of size r_1, X_2 of size r_2, $\ldots$.

How does the proof now go?

Steps 2, 3, $\ldots$, $d+1$: put X_1, X_2, $\ldots$, X_d into an order.

Then put S into an order by first using X_1 then X_2 then $\ldots$ then X_d.

By the multiplication principle, the number of ways of ordering S is hence $\binom{n}{r_1, r_2, \ldots, r_d} r_1! r_2! \cdots r_d!$. But it's also equal to $n!$ by Proposition 5.1. The result now follows.

$\square$

Theorem 5.8. [the multinomial theorem]
$(a_1 + a_2 + \cdots a_d)^n = \sum \binom{n}{r_1, r_2, \ldots, r_d} a_1^{r_1} a_2^{r_2} \cdots a_d^{r_d}$, where the sum is over the ordered d-tuples $(r_1, r_2, \ldots, r_d)$ of non-negative integers such that $\sum_{i=1}^{d} r_i = n$.

Proof. How does this proof go? The same proof as the binomial theorem works. We expand out the brackets, and see that the total number of a_i in each of the terms will be n, so a general term is $a_1^{r_1} a_2^{r_2} \cdots a_d^{r_d} = \prod_{i=1}^{d} a_i^{r_i}$ with $\sum_{i=1}^{d} r_i = n$. And the number of times each of these terms occurs is equal to the number of ways that you can take n brackets and choose a_1 from r_1 of them, a_2 from r_2 of them and so on, and this is $\binom{n}{r_1, r_2, \ldots, r_d}$ by definition!

$\square$