Exercise 1 (Exercise 1)**.** Prove that addition and multiplication of cardinalities satisfies the distributive law, that is, that

$$|A|(|B| + |C|) = |A|\cdot|B| + |A|\cdot|C|,$$

using the definition of addition and multiplication of cardinalities that we defined in class.

Answer

To prove the equality using the definition of cardinalities, we would like to exhibit a bijection from a set whose size is the amount on the left to a set whose size is the amount on the right.
Consider any sets A, B and C. The following table summarizes the information we are working with

Set	Cardinality	Elements
$A \times (B \cup C)$	$\|A\|(\|B\| + \|C\|)$	$(a,(x,n))$
$(A \times B) \cup (A \times C)$	$\|A\|\cdot\|B\| + \|A\|\cdot\|C\|$	$((a,x),n)$

with $n \in \{0,1\}$ and $n = 0 \Rightarrow x \in B$, while $n = 1 \Rightarrow x \in C$. This is because the disjoint union can be constructed in the following way

$$B \cup C = (B \times \{0\}) \cup (C \times \{1\}).$$

Because of this construction it doesn't matter if B and C share elements since they will be labeled.
Now the function

$$f : A \times (B \cup C) \to (A \times B) \cup (A \times C),\ (a,(x,n)) \mapsto ((a,x),n)$$

can be proven to be well-defined, injective and surjective. It is therefore bijective and its inverse is the function that follows the rule $((a,x),n) \mapsto (a,(x,n))$.
Since we have found the bijection in question, it follows that both sets have the same cardinalities and thus the quantities in question are equal.

Exercise 2 (Exercise 2)**.** Prove the binomial theorem using a combinatorial argument as follows.

i) Show that, for all positive integers s, t, and n, we have

$$\sum_{k=0}^{n} \binom{n}{k} s^k t^{n-k} = (s+t)^n.$$

In particular, do not treat s and t as variables; rather, interpret $(s+t)^n$ as counting something parameterized by the integers s, t, n and show that the right hand side counts the same thing.

ii) Defining the polynomials $p(x) = (x+1)^n$ and $q(x) = \sum_{k=0}^{n} \binom{n}{k} x^k$, we have that $p(s) = q(s)$ for all positive integers s. Use the fact that polynomials in one variable that agree on infinitely many values must be the same to conclude that $p(x) = q(x)$ as polynomials.

iii) Finally, plug in x/y and clear the denominators on both sides of the equation $p(x/y) = q(x/y)$ to show that the binomial theorem holds.

Answer

(a) Consider a string[a] of length n, an alphabet S with s characters, and an alphabet T with length t.[b]

The quantity $(s+t)^n$ counts the number of strings of length n that we can build with our alphabets S and T. We can count this amount in another way.

Suppose that $k \leqslant n$ is fixed, we can break up the string in two parts: the k spots where we put a character from alphabet S and the $n-k$ spots where we put a character from alphabet T. There's s^k ways to pick a character from alphabet S and t^{n-k} ways to take a character from T. So in total there's $s^k t^{n-k}$ ways to construct a string with such a restriction.

However, the k spots are indifferent to the placement of the characters, we can *choose* our k spots in $\binom{n}{k}$ ways. So there are $\binom{n}{k} s^k t^{n-k}$ ways to construct a length n string with k characters from alphabet S and the rest from T. Summing up all over k gives us the desired result.

(b) Consider the polynomial p and q. Suppose $s \in \mathbb{N}$, then replacing $t = 1$ in our binomial formula we obtain $p(s) = q(s)$ for every $s \in \mathbb{N}$.

This means that the polynomial $q - p$ has infinitely many zeros, so it must be identically zero. Therefore $p = q$ as polynomials.

(c) Since $p = q$ we have that

$$p\left(\frac{x}{y}\right) = q\left(\frac{x}{y}\right) \Rightarrow \left(\frac{x}{y}+1\right)^n = \sum_{k=0}^{n}\binom{n}{k}\left(\frac{x}{y}\right)^k$$
$$\Rightarrow y^n\left(\frac{x}{y}+1\right)^n = y^n\sum_{k=0}^{n}\binom{n}{k}\left(\frac{x}{y}\right)^k$$
$$\Rightarrow (x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k\frac{y^n}{y^k} = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

[a] A password, for example

[b] The idea to count strings came from **yourself**, but when you told me I only thought about strings with 0's and 1's. I asked **Kyle** about the strings and so he recommended using more than two characters, and that the terms in the sum were the ways to separate the string in two parts.

Exercise 3 (Exercise 3, Stanley 1.3.e)**.** Give a combinatorial proof of the identity $2\binom{2n-1}{n} = \binom{2n}{n}$.

Answer

The quantity $\binom{2n}{n}$ counts the number of committees of length n which can be formed from a group of $2n$ people. From our select group we can choose one president in $\binom{n}{1} = n$ ways. So the amount of ways we can choose a committee with a president is $n\binom{2n}{n}$.
We can also choose the president first, and then select the rest of the committee members. This is done as follows:

- There are $\binom{2n}{1} = 2n$ ways to choose the president from the whole group of people without the restriction of being in the committee first.
- With the president out, there are $\binom{2n-1}{n-1}$ ways to pick the rest of the committee's members.

In total there would be $2n\binom{2n-1}{n-1}$ ways to form a committee with a president. Since both quantities count the same thing it follows that

$$n\binom{2n}{n} = 2n\binom{2n-1}{n-1} \Rightarrow \binom{2n}{n} = 2\binom{2n-1}{n-1}$$

and by symmetry of the binomial coefficient we get

$$\binom{2n}{n} = 2\binom{2n-1}{n}.$$

Exercise 4 (Exercise 5, Stanley 1.13)**.** Let p be a prime and $a \in \mathbb{N}$. Show *combinatorially* that $p \mid a^p - a$.[1]

Answer

Consider an alphabet A with a characters and a string of length p. We can construct a^p possible strings. However, there are a very special strings[a] which are the strings which only contain one character from our alphabet. This means we have $a^p - a$ strings which contain two or more different characters.
Let's now wrap around this strings to form *necklaces*. We will say two strings are equivalent if any rotation of the necklace formed by the first string gives us the necklace formed by the second string. This is an equivalence relation:

- ◇ Every string is equivalent to itself by the identity rotation.
- ◇ Rotating has an inverse operation which makes the relation symmetric.
- ◇ And the composition of rotations guarantees that the relation is transitive.

The set of strings is therefore partitioned into a certain number[b] of equivalence classes with p equivalent necklaces each. It follows that $p \mid a^p - a$.

[a] Very unsafe passwords.
[b] Which is, of course, an integer

[1] This is Fermat's Little Theorem.