Course Curriculum: Discrete Mathematics

Talley Amir

Yale University

Summer 2020

Citation and Disclaimer

I acknowledge here that the theorems and algorithms presented below are not my own work, and the compilation of this material is intended for educational purposes only.

Several problems for the activities were taken directly from *CSCI0220: Introduction to Discrete Structures and Probability*, a college-level mathematics course taught at Brown University, and can be found here. These problems are marked by ‡.

Module 1: Introduction to Proof Writing

The goal of this lesson is to motivate the reason for taking this course, which is to learn how to communicate mathematical concepts clearly and effectively. It is easier to solve a problem than it is to convince another person that the solution you have arrived at is true. Nonetheless, this skill is of the utmost importance because it enables the understanding, sharing, and growth of knowledge.

1. Introduction to the class, overview of topics, and a brief summary of applications of the concepts covered by this course to other fields, including computer science, engineering, and data science.

2. Goal of the class: To develop *mathematical literacy*, the ability to clearly and effectively convince someone else that a mathematical statement is true.

3. Quick example: Direct proof.

   If I tell you that I have a number x, and x^2 is even, I claim that x is also even. Is this obvious? In this course, no, nothing is obvious! We will build up to every claim from the most basic mathematical assumptions. Then how can I prove the parity of x?

   Split into pairs and do the following exercise.

   Exercise 1:

   One person assumes that x is even and tries to convince the other. Next, the other person assumes that x is odd and tries to *disprove* this assumption. Because the correct answer is that x is even, both students should successfully be able to convince the other of their assumptions.

   Reconvene as a class and discuss the exercise. What strategies were successful in convincing the other person that your claim is correct? How many steps did you use to convey your argument? Break down each piece of your argument: What was convincing and what was not? These questions will help students better understand what makes for a successful proof and motivate the importance of *clarity* and *conciseness*.

   Next, discuss the difference in the two parts of the exercise (i.e. proving that x is even directly versus proving that x is even via *contradiction*). Elaborate on both proof structures and discuss their pros and cons. These discussions can happen as a class, or in small groups (depending on class size).

Module 2: All About Sets

The goal of this lesson is to learn about the set element method and apply it to determine the containment or equality of two sets.

A *set* is an unordered collection of distinct objects.

- Examples of sets: $\{2, 4, 6\}$, $\{1, B, \texttt{'eleven'}\}$, or $\{9, 7, \{9\}\}$.
- Not sets: $\{a, a, 3\}$.
- NOTE: $\{1, 2, 3\} = \{3, 1, 2\}$ because order does not matter. Two sets are *equal* if they contain exactly the same elements.
- A special set is the set with no elements in it. This is often denoted $\{\}$, or with its own special symbol $\emptyset$.
- Another special set is the complement of a set A^C. This is the set of all elements in the specified universe U that are not in the set A.

A set A is a *subset* of another set B if all elements of the set A are elements of the set B. This is denoted $A \subseteq B$. If the sets are necessarily not equal, then $A \subset B$ (called a strict subset).

- Examples of subsets: $A = \{1, 2\}$ is a subset of $B = \{1, 2, 3\}$.
- Not subsets: $A = \{1, 2, 4\}$ is not a subset of $B = \{1, 2, 3\}$ because $4 \notin B$.

We write $x \in A$ to mean that x is an element of set A. To signify that an element is not in a set, we write $x \notin A$.

A set A is a *superset* of another set B if all elements of the set B are elements of the set A. This is denoted $A \supseteq B$. If the sets are necessarily not equal, then $A \supset B$ (called a strict superset).

The *power set* of a set is the set of all subsets of that set.

- Examples of power sets: Let $A = \{1, 2\}$. Then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Split into pairs and do the following exercise.

Exercise 1:

Let $A = \{1, 2, 2\}$, $B = \{2, 3, 5\}$, and $C = \{1, 2, 3, 4, 5\}$.

- Is A a set? Is B a set? Is C a set?
- Is B a subset of C?
- Is C a subset of B?
- Is C a superset of B?
- Is B a subset of itself?
- What is $\mathcal{P}(\{6\})$?
- What is $\mathcal{P}(\{\star, \circ\})$?
- What is $\mathcal{P}(\{x, y, z\})$
- What is $\mathcal{P}(\{\{\emptyset\}, \emptyset\})$?

The *intersection* of two sets A and B is the set of all elements x such that $x \in A$ and $x \in B$. This is denoted $A \cap B$.

- Example: Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Then $A \cap B = \{2, 3\}$.
- Example: Let $C = \{1, 2\}$ and $D = \{3, 4\}$. Then $C \cap D = \emptyset$.

The *union* of two sets A and B is the set of all elements x such that $x \in A$ or $x \in B$ (or both). This is denoted $A \cup B$.

- Example: Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Then $A \cup B = \{1, 2, 3, 4\}$.
- Example: Let $C = \{1, 2\}$ and $D = \{3, 4\}$. Then $C \cup D = \{1, 2, 3, 4\}$.

The *set difference* of two sets A and B is the set of all elements x such that $x \in A$ but $x \notin B$. This is denoted $A \setminus B$.

- Example: Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Then $A \setminus B = \{1\}$.
- Example: Let $C = \{1, 2\}$ and $D = \{3, 4\}$. Then $C \setminus D = \{1, 2\}$.

The *cross product* of two sets A and B is the set of all pairs of elements (a, b) such that $a \in A$ and $b \in B$. This is denoted $A \times B$.

- Example: Let $A = \{1, 2\}$ and $B = \{3, 4\}$. Then $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

The *set element method* is a proof technique that can be used to compare the containment of sets. The basic intuition is as follows: Say that I tell you I have two sets, and I know that all of the elements of one set are in the other; I also tell you that all of the elements in

the other set are not necessarily in the first. What do we know about these sets? Is one a subset or a superset of the other?

Consider the set of integers between 1 and 100, call this set A. Let set B be the set of all *even* integers between 1 and 100. All of the elements of B are in A, but not vice versa, thus we know that B is a *subset* of A. Here, we know this to be true.

Now consider that I tell you I have two sets X and Y, and all the elements in set X are in Y and vice versa. What do we know about X and Y? (Answer: They must be equal).

Formally, this is written as:

$$X \subseteq Y, Y \subseteq X \Rightarrow X = Y$$

Assignment: Find another way to write $A \setminus (B \cap C)$ and prove that the new expression you wrote equals this one.

Module 3: Functions, Relations, and Bijections

The goal of this lesson is to learn how to use bijective proofs to determine the relative sizes of two sets.

Today we will learn about another proof technique called *bijective proofs*. These let us prove that the size of two sets are the same. This is useful when we know how to count one set but not necessarily how to count another set; however, if we can prove that both sets have the same number of elements, then we can essentially count both.

A *relation* on two sets A and B is a set of pairs (a, b) such that $a \in A$ and $b \in B$. (How big can a relation be relative to the sizes of A and B?) Notice that this is a *subset of the cross product* of A and B.

A *function* is a relation such that all of the elements of the first set appear in the relation exactly once (i.e. an input cannot be mapped to more than one output). (Give examples of sets of pairs and of defined mappings between sets).

An *injective* function $f : A \to B$ has the following property:

$$\forall\, x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

A *surjective* function $f : A \to B$ has the following property:

$$\forall\, y \in B, \exists\, x \in A \text{ s.t. } f(x) = y$$

Draw pictures with dots to illustrate both concepts, explain which pictures define functions and which define relations and why.

A *bijection* is a function that is both *injective* and *surjective*.

Now we can use this concept to prove something about the sizes of sets. (Explain using the two diagrams of injective and surjective functions that this means that if two sets have the same size, there must exist a bijection between them).

Recall the definitions of sets and subsets from yesterday. If one set is a subset of another, the subset must have size less than or equal to the set of which it is a subset.

- Consider again the set of all integers from 1 to 100, call this set A. Let B be the set of even integers from 1 to 100. Let $f : A \to B$ be a function that maps elements of A to elements of B, $f(a) = 2a$. (Talk about domain and codomain, explain why this is not a function on the defined sets, talk about what would need to be changed, i.e. make B be all evens from 1 to 200).

Split into pairs and do the following exercise.

Exercise 1:

Let $A = \{1, 2, 5\}$ and let $B = \{3, 4, 8, 9\}$. Let $R \subseteq A \times B$.

1. Is R a relation? (Yes)
2. Define $R = \{(1, 3), (1, 4), (2, 8), (5, 3)\}$. Is R a function? (No, 1 maps to two elements)
3. Define $R = \{(1, 3), (2, 4)\}$. Is R a function? (No, 5 is not mapped to anything)
4. Define $R = \{(1, 3), (2, 4), (5, 4)\}$. Is R a function? (Yes!)

Now let $R = \{(1, 8), (2, 3), (5, 9)\}$.

5. Is R injective?
6. Is R surjective?
7. Is R bijective?
8. What do the answers to these questions tell us about the sizes of A and B?

Reconvene as a class and discuss the answers the groups came up with.

A 0/1 *string of length* n is an ordered sequence of 0's and 1's where the total number of bits is equal to n, for $n \geq 0$. This is often denoted $\{0, 1\}^n$. (Write up examples where $n = 4$ - how many of these are there? How do you know?)

Claim: The number of subsets of a set of size n equals the number of 0/1 strings of length n.

Swap pairs and do the following exercise.

Exercise 2:

With your partner, discuss the answers to the following questions:

1. How many 0/1 strings of length n are there?
2. How many subsets of a set S of size n are there?
3. How did you answer parts (a) and (b)?
4. Start to construct a mapping. Which 0/1 string would you map to the empty set? Which string would you map to the set S itself? What are potential strategies for coming up with a more general function?

Reconvene as a class and discuss the answers the groups came up with. Walk through a solution and proof together.

Exercise 3:

Switch partners and solve the following problem:
‡Let T be the set of all 0/1/2/3 strings of length n, and let S be a set of n objects. (X, Y) are pairs of subsets of the set S. Does there exist a bijection from S to T? If so, prove it. If not, why not?

Assignment: ‡I want to buy 10 pints of ice cream. There are four flavors: Vanilla, Chocolate, Strawberry, and Pistachio. I can buy any number of each flavor as long as I buy 10 pints altogether. Prove that the number of 0/1 strings of length 10 with exactly 3 1's is equal to the number of unique ways to choose the flavors for my 10 pints of ice cream.
Hint: Give (and prove) a bijection!

Module 4: Number Theory

Today everyone will learn the number theory background needed to understand and prove the security of RSA.

An integer a is *divisible* by a positive integer b if there exists an integer c such that $a = bc$. b and c are both *divisors* of a.

A *prime* is an integer that is only divisible by 1 and itself. Likewise, a *composite* is an integer that has more divisors than only 1 and itself (example: $6 = 3 \cdot 2$).

The *greatest common divisor* of two numbers a and b is the maximum integer that is a divisor of both a and b. This is written as $\gcd(a, b)$.

If $\gcd(a, b) = 1$, then a and b are said to be *coprime*, or *relatively prime*.

Exercise 1:

- What is the gcd of 9 and 17?
- What is the gcd of 30 and 75?

You may have figured out the answer by writing out all of the prime factors of each number and taking the maximum overlapping set of primes and multiplying them together. However, in practice this is hard to do because factoring is considered to be a "hard problem." Say I give you the number 1789 and ask you to find its prime factors? How would you do this? You might have to go through all the numbers between 1 and 1789 to find each of its divisors (though in fact this number is prime)! For very large numbers, this becomes unfeasible.

There is a fast algorithm that computes the gcd of two numbers. This is called the *Euclidean algorithm*, and it is defined as follows:

To compute $\gcd(a, b)$:

$$\begin{aligned} \mathbf{a} &= q_0\mathbf{b} + r_0 \\ \mathbf{b} &= q_1\mathbf{r_0} + r_1 \\ \mathbf{r_0} &= q_2\mathbf{r_1} + r_2 \\ \mathbf{r_1} &= q_3\mathbf{r_2} + r_3 \\ &\dots \end{aligned}$$

If a is smaller than b, the first step of the algorithm swaps the numbers.

Walk through example: $\gcd(8, 30)$.

Proof of Correctness. Loop invariant: At each iteration, the gcd of the two bold values is the same as in the previous iteration. Thus at the end, we get the gcd of the first two bolded values (a and b).

Thus it suffices to show that $\gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2})$.

□

Exercise 2:

- Compute $\gcd(9, 17)$ and $\gcd(30, 75)$ by hand and verify your answers with what you computed before.

We can use the *extended Euclidean algorithm* to write $\gcd(a, b)$ as a *linear combination* of a and b. Specifically, we can find integers u, v such that:

$$au + bv = \gcd(a, b)$$

Let's bring back the relations we learned about on Day 1. Define the relation R_m to be a relation over integers such that $(a, b) \in R_m$ if and only if m divides $a - b$. We write that a and b are *congruent* under the modulus m as follows:

$$a \equiv b \pmod{m}$$

Each number will be equivalent to its *remainder* when divided by m. Another way to think about this relation: If $(a, b) \in R_m$, then there exists an integer k such that $a = b + km$.

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Given this definition, some properties of the "mod" relation:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ ac &\equiv bd \pmod{m} \\ a^n &\equiv b^n \pmod{m} \text{ for } n \in \mathbb{Z} \\ a + k &\equiv b + k \pmod{m} \\ ak &\equiv bk \pmod{m} \end{aligned}$$

Notice that *division* does not always work here. (Example: $18 \equiv 6 \pmod{12}$ but $9 \not\equiv 3 \pmod{12}$).

The *multiplicative inverse* of an integer a modulo m is an integer $b = a^{-1}$ such that $ab \equiv 1 \pmod{m}$. For example, the inverse of 3 modulo 17 is 6 because $3 \cdot 6 \equiv 18 \equiv 1 \pmod{17}$. *Not all numbers have an inverse for a given modulus.* The rule is that an integer a has an inverse modulo m iff $\gcd(a, m) = 1$.

Now, we can use the extended Euclidean algorithm to find the inverse! Why? Because if we can find u, v such that $au + mv = 1$, then u is the multiplicative inverse of a modulo m.

Exercise 3:

- Use the extended Euclidean algorithm by hand to express 4 as a linear combination of 12 and 32 (Answer: $4 = 12 \cdot 3 + 32 \cdot (-1)$).
- Use the extended Euclidean algorithm by hand to find the inverse of 21 modulo 92 (Answer: 57).

Euler's totient function computes the number of integers between 1 and N that are relatively prime to N. This is often denoted $\varphi(N)$. Notice that for a prime number p, $\varphi(p) = p - 1$.

We also have a general form for $\varphi(N)$ when N is the product of *exactly two primes* p and q:

$$\varphi(N) = (p-1)(q-1)$$

However, this does not extend to three or more primes.

Fermat's little theorem (FℓP): For prime p and any integer a not divisible by p,

$$a^{p-1} \equiv 1 \pmod{p}$$

Euler's theorem generalizes Fermat's little theorem for composite numbers: For any integer N and any integer a such that $\gcd(a, N) = 1$:

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

Module 5: RSA Encryption

Today we will learn how to encrypt and decrypt messages using RSA.

Last time we learned about the mod relation R_m. Essentially this relation groups together all integers with the same remainder when divided by m. Just like how we know that factoring is hard for integers, we know certain problems are hard within the mod relation.

The *RSA problem* is the problem of finding g such that $g^a \equiv h \pmod{m}$ for some $h \in \{0, 1, ..., m-1\}$. This problem is "hard," that is, we have no efficient algorithm for computing g. Finding the value of g is as hard as guessing the value at random. We can use this fact to build an encryption scheme!

RSA is a public key encryption scheme that was developed by Ron Rivest, Adi Shamir, and Leonard Adleman (where the name RSA comes from) in 1977. It is "secure" because we assume that factoring is hard and the *RSA problem* is hard.

Public key encryption schemes consist of three kinds of algorithms:

- KeyGen: This is a key generation algorithm. It produces pairs of keys (a public key and a private key) that are used to encrypt messages to one another. An individual runs the algorithm and then publishes their public key, but keeps their private key a secret.
- Enc: This is the encryption algorithm. If Alice wants to send a message to Bob (who has published his public key PK_{Bob}, Alice can encrypt a message to Bob using his public key.
- Dec: This is the decryption algorithm. If Alice sends a ciphertext C to Bob that was encrypted under Bob's public key PK_{Bob}, Bob can use his secret key SK_{Bob} to decrypt the message. Recall that the pair of keys $(PK_{\text{Bob}}, SK_{\text{Bob}})$ was obtained from the KeyGen algorithm.

The RSA encryption scheme is defined as follows:

- $\mathsf{KeyGen}(1^\lambda)$:
  1. Pick two large primes p and q and compute $N = pq$.
  2. Pick e such that $\gcd(e, \varphi(N)) = 1$, and compute $d = e^{-1} \pmod{\varphi(N)}$.
  3. Publish public key $PK = (N, e)$. Keep private secret key $SK = (p, q, d)$.
- $\mathsf{Enc}(m, PK)$:
  1. m must be an integer in $\{1, ..., N-1\}$. If not, define a reversible mapping from the message space to this set of integers.
  2. Compute and output $c = m^e \pmod{N}$.
- $\mathsf{Dec}(c, SK)$:
  1. Compute and output $m' = c^d \pmod{N}$.

Claim: The decryption m' is the originally encrypted message.

Proof.

$$\begin{aligned} m' &\equiv c^d \pmod{N} \\ &\equiv (m^e)^d \pmod{N} \\ &\equiv m^{ed} \pmod{N} \\ &\equiv m^{1+k\cdot\varphi(N)} \pmod{N} \\ &\equiv m \cdot (m^k)^{\varphi(N)} \pmod{N} \\ &\equiv m \cdot 1 \pmod{N} \\ &\equiv m \pmod{N} \end{aligned}$$

□

Let's try it! Split up into pairs and do the following activity:

Exercise 1:

- Let $A = 1$, $B = 2$, ..., $Z = 26$.
- Pick your own two primes (they should be *large*) and compute your public and private keys. Write your name and your public key on the board.
- Write a message to a friend! Pick someone on the board and encrypt a message to them using their public key. You should write the person's name on the message (unencrypted) for the next step.
- Give the message to your friend. Now they should decrypt their message, but still keep it private.

Why is RSA *secure*? Given a ciphertext c, it is hard to find the decryption m as long as p and q are unknown. What happens if p and q are known?

If p and q are known, then we can easily compute $\varphi(N)$ and use the extended Euclidean algorithm to find the inverse of e (a public parameter) modulo $\varphi(N)$. This inverse is exactly equal to the decryption exponent, which we can then use to decrypt any message we see!

Exercise 2:

- Steal someone else's message (a message that you did not write and that was not written to you).
- Everyone writes their prime numbers on the board.
- Use the now public private values to compute the private key and decrypt the message you stole!

Module 6: Induction

The goal of today's lesson is to learn about the inductive proof technique and to apply it to prove a predicate for an infinitely large set.

Induction is a proof technique that is used to prove that a statement holds true for every element of an infinite, enumerable set. For example, say I have an infinitely tall ladder, and I want to prove that I can climb the whole thing. I must prove two things:

1. I can climb onto the first rung of the ladder.
2. If I can get to the k-th step of the ladder, then I can get to the $k+1$-th step of the ladder. I do this by taking a step from the k-th to the $k+1$-th rung.

Induction has a special kind of proof structure:

- Base case: Prove that a statement holds true for the "first" thing, the base of the set (if this is the set of all positive integers, the base case is $k = 1$; if it is the set of all integers greater than 10, the base case is $k = 11$).
- Inductive hypothesis: Assume that the statement holds for k.
- Inductive step: Prove that *if* the statement holds for k, *then* it must also hold for $k + 1$.
- Conclusion.

Given this structure, we can prove that the statement holds for the base case, and then also for every case that comes next by one step. Let's see it in action!

Claim: The sum of the first n positive integers is $\frac{n(n+1)}{2}$.

Proof.
- Base case: For 1, we have $\frac{1(2)}{2} = 1$, as needed.
- Inductive hypothesis: Assume that

$$1 + 2 + ... + k = \frac{k(k+1)}{2}$$

- Inductive step: We know that $1 + 2 + ... + k = \frac{k(k+1)}{2}$, so let's add $k + 1$ to both sides. Now we get

$$\begin{aligned} 1 + 2 + ... + k + (k+1) &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

- Conclusion: This proves the statement for $k+1$, as needed!

□

Exercise 1:
Split into pairs and answer the following questions:

- ‡Prove by induction that for all positive integers n, there exists a positive integer m such that:
$$m^2 \leq n < (m+1)^2$$
- ‡Prove that this m is unique (i.e. there is only one such m).

Module 7: Counting

The goal of today's lesson is to learn new techniques for counting.

So far in this class, we have seen counting in various contexts. We counted the number of 0/1 strings of length n, as well as the size of the power set of a set of size n. Today we will learn how to count more complicated sets of objects.

Consider the following scenario: There are 3 students – Alice, Bob, and Carol – standing in a line. How many possible ways can we order them? We can answer this question by considering a sub-problem:

Let's say we decide that Alice will be first in line. How many ways are there to order the rest of the kids in line? Now, let's say that instead of Alice being first, Bob is first. How many ways are there to order the rest of the kids? How many ways are there to pick the first kid?

Now, let's say we have 100 kids in a line. How many ways are there to order the kids? The answer is 100! (pronounced "100 factorial") and is equal to

$$100! = 100 \cdot 99 \cdot 98 \cdot ... \cdot 2 \cdot 1$$

Generally speaking, the number of ways to order n objects is

$$n! = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 2 \cdot 1$$

By convention, $0! = 1$.

This number grows *fast*. We can see this even in the first few integers:

$$\begin{aligned} 0! &= 1 \\ 1! &= 1 \\ 2! &= 2 \\ 3! &= 6 \\ 4! &= 24 \\ 5! &= 120 \\ 6! &= 720 \\ 7! &= 5040 \\ &... \\ 25! &\approx 1.5 \cdot 10^{25} \end{aligned}$$

Let's see how we can use factorials to count:

Exercise 1:
Split into pairs and answer the following questions:

- A word is a unique sequence of letters (it does not have to be a real word with meaning). For example, given the letters `'A'`, `'C'`, and `'R'`, we can make the words CAR, ARC, RAC, RCA, ACR, and CRA. How many words can we make with the letters `'O'`, `'C'`, `'R'`, `'K'`, and `'S'`? List 3 of them.
- How many words can we make with the letters `'A'` and `'A'`? List all of them.
- How many words can we make with the letters in `'SALAD'`? Why isn't the answer 5!?

In the last example, we saw that repeated letters cause us to count more carefully than before. Why?

Now, let us consider a new problem. We have 25 students in the class, and we want to select 3 to be in a special committee. How many unique sets of three students can we pick from the set of 25? Let's say I pick Alice, Bob, and Carol. Is this the same as choosing Alice, Carol, and Bob? Does order matter?

The way that we count this quantity is using an expression called the *binomial coefficient*:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Exercise 2:
Split into pairs and answer the following questions:

- There are 7 books I am interested in reading, but I only want to read 3 books this summer. How many ways can I choose 3 books to read from the set of 7 books?
- I decide I actually want to read 4 books this summer. How many ways can I choose 4 books to read from the set of 7 books?
- What do you notice about the answers to the first two questions? Why does this happen?
- Recall the ice cream problem from the day we covered bijections. How many ways can I choose the 10 pints of ice cream from the 4 flavors?
- There are 8 identical red balls and 2 identical blue balls. How many ways can I uniquely choose 5 balls from the total set of 10?

Reconvene as a class and walk through the answers together.

Module 8: More Counting

The goal of today's lesson is to learn and apply counting arguments to show that two expressions count the same thing.

A *counting argument* is a type of proof where we show that two expressions are equal by explaining how they count the same thing.

Let's take a look at the following example that we discussed in class yesterday:

$$\binom{n}{k} = \binom{n}{n-k}$$

We can show that these two expressions are equal by writing them out in terms of factorials:

$$\binom{n}{k} = \binom{n}{n-k}$$
$$\frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{k!(n-k)!}$$

However, we can also use a counting argument:

- The left-hand side of the equation counts the number of ways to choose k objects from a set of n objects.
- The right-hand side of the equation counts the number of ways to choose $n-k$ objects from a set of n objects. We can instead think of this as choosing the $n-k$ objects that *are not* being chosen, which would make this count exactly the same number of choices as the left-hand side.

Let's take a look at a more complex example:

$$\binom{n}{k} k! = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

Again, we can see that *algebraically* the two sides of the equation work out to be that same:

$$\begin{aligned}
\binom{n}{k} k! &= \frac{n!}{k!(n-k)!} k! \\
&= \frac{n!}{(n-k)!} \\
&= \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \cdot (n-k) \cdot (n-k-1) \cdot \ldots \cdot 2 \cdot 1}{(n-k) \cdot (n-k-1) \cdot \ldots \cdot 2 \cdot 1} \\
&= n \cdot (n-1) \cdot \ldots \cdot (n-k+1)
\end{aligned}$$

But what do both sides *count*?

- First consider the right-hand side. This side looks almost like the simple factorial we looked at yesterday, but it is missing the last $n-k$ terms. We can think of this as choosing k objects from a set of n objects where order *does* matter (i.e. we have n choices for the "first" position, $n-1$ for the "second," and so on until k positions are filled).
- We can see that the left-hand side counts exactly the same thing if we think of first *choosing* the k objects and *then* multiplying each choice of objects by the number of ways to permute them.

Let's try some more examples!

Exercise 1:
Split into pairs and use a counting argument to prove the following equalities:

- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
- $\sum_{k=0}^{n} \binom{2n}{n}$
- $^{\ddagger}\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
- $^{\ddagger}\binom{n}{k} = \binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2}$

Module 9: Introduction to Probability

Today we will cover the basic elements of probability theory and use some of the counting tools we learned in the last two modules to solve some very cool problems!

When you flip a coin, what are the chances it comes up Heads?

When you roll a pair of dice, what are the chances you get two 6's? What about the chances that the sum of the dots on the two dice equals 10?

Today, we are going to formalize the way to answer these questions using the theory of *probability*.

The *probability* of an outcome is the number of ways an outcome can happen divided by the total number of outcomes.

Examples:

- When you flip a fair coin, there are two possible outcomes that happen equally likely, so the probability that the coin lands on Heads is:

$$\mathbb{P}[\text{Heads}] = \frac{1}{2}$$

- When you roll a fair die, there are six possible outcomes that happen equally likely, so the probability that the die lands on any particular face is $\frac{1}{6}$.

Probabilities are just real numbers between 0 and 1. The *more likely* an outcome is, the closer its probability is to 1, and the less likely it is, the closer its probability is to 0.

A *probability density function* is a function that maps outcomes to their probabilities. More formally, we can think about the set of all possible outcomes as $\{w_1, ..., w_k\}$, and the probability density function p as a function that outputs w_i's probability:

$$p(w_i) = p_i$$

The *sample space* is the set of possible outcomes. An *event* is a subset of outcomes. For example, when you roll a die, the set of all possible outcomes is the set of ways the die can land: $S = \{1, 2, 3, 4, 5, 6\}$. However, the event that the die lands on an even number is $\{2, 4, 6\} \subseteq S$.

Law of Total Probability: The sum of the probabilities in a sample space must be 1:

$$p_1 + p_2 + ... + p_k = 1$$

Let's consider the following example: We throw two dice on the floor. What is the probability of the event that one lands on 3 dots and the other lands on 5 dots? We need to consider all possible ways the dice can land, and all possible ways they can land 3 and 5.

We have to consider the two dice as distinct, so there are two ways to land 3 and 5: Die 1 lands 3 and Die 2 lands 5, or the other way around. The total number of possible outcomes is the number of ways one die can fall (6) multiplied by the number of ways the other die can fall (6). Thus the probability of the even that one die lands 3 and the other lands 5 is $\frac{2}{36}$. Let's try some more examples:

Exercise 1:
Split into pairs and work through the following problems. You toss two dice on the floor. What is the probability that...

- ...the sum of the dots adds to 9?
- ...they are both greater than 3?
- ...they are not two 6's (but one of them can be a 6)?
- ...neither of them is a 6?

The last two examples demonstrate that sometimes it is easier to count the number of events that we are *not* trying to count and subtract this from 1 to get the probability we are trying to get.