MATH 215: NOTES

Contents

1. Jan 8 (Syllabus day)

- Go through syllabus
- Finish with mathematical warmup: what is an even number ($x = 2k$ with $k \in \mathbb{Z}$), what is an odd number ($y = 2k + 1$ with $k \in \mathbb{Z}$). Must every number be even or odd? (Yes, but to prove this will require later material). Idea is to get students thinking about precise, useful definitions and how to prove facts they are used to assuming.

Here $\in$ is read "in" and $\mathbb{Z}$ denotes the set of integers (i.e. the set $\{\dots, -3, -2, -, 1, 0, 1, 2, 3, \dots\}$ of positive whole numbers, zero, negative whole numbers). "$k \in \mathbb{Z}$" therefore means that k is an integer.

2. Jan 10 (Statements)

- Introduction to *statements* in the mathematical sense (declarative statement that can be assigned a truth value: it is either True or False, not both).
- Building statements from new statements. Negation, and, or. Truth tables below.

P	$\neg P$
T	F
F	T

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

- Use examples to motivate logical equivalences. Two things are logically equivalent if they always have the same truth value. This means they can be swapped for one another in statements, expressions, etc. DeMorgan's laws:

$$\neg(A \wedge B) \text{ logically equiv to } \neg A \vee \neg B$$
$$\neg(A \vee B) \text{ logically equiv to } \neg A \wedge \neg B$$

as well as distributive properties:

$$A \wedge (B \vee C) \text{ logically equiv to } (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \text{ logically equiv to } (A \vee B) \wedge (A \vee C)$$

3. Jan 17 (Conditionals)

Another example of building new statements from old ones. Given P, Q statements we can form $P \Rightarrow Q$. It has the following truth assignments, depending on those of P, Q.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

We discuss what it means to "prove" a statement of the form $P \Rightarrow Q$: this means, show it is always true. Looking at the table above, we only need to worry about landing in the case of $T \Rightarrow F$. So proving a conditional means assuming P is true, and trying to use logical arguments to deduce that Q is true. We see that, for x an integer,

$$x \text{ is a multiple of } 4 \Rightarrow x \text{ is a multiple of } 2$$

is true (information on the left always implies information on the right) , but

$$x^2 > 0 \Rightarrow x > 0$$

is not true (there are situations where $x^2 > 0$ and $x < 0$).

From the conditional $P \Rightarrow Q$, we can define the inverse $(\neg P \Rightarrow \neg Q)$ as well as the converse $(Q \Rightarrow P)$ and the contrapositive $(\neg Q \Rightarrow \neg P)$. We then go through writing their truth values:

P	Q	$P \Rightarrow Q$	$\neg P \Rightarrow \neg Q$	$Q \Rightarrow P$	$\neg Q \Rightarrow \neg P$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

From there we see the original $P \Rightarrow Q$ is logically equivalent to the contrapositive. We also see the inverse, converse are logically equivalent to eachother (note that the inverse is the contrapositive of the converse). We discuss how this will be useful: sometimes the contrapositive is way easier to prove than the original statement.

Lastly, if $P \Rightarrow Q$ and $Q \Rightarrow P$ are true, then we say $P \iff Q$ (read "P if and only if Q). This means P is true exactly when Q is true and vice versa: i.e. this means P, Q are logically equivalent. So from now on we write P, Q logically equivalent as $P \iff Q$. If trying to prove $P \iff Q$ on a HW/in class: there should be two parts: showing $P \Rightarrow Q, Q \Rightarrow P$.

Direct students to Taylor 1.4 for $\forall$ (for all/any) and $\exists$ (there exists) quantifiers.

4. Jan 19 (Proof methods 1: direct proofs)

Three major proof methods when trying to show $P \Rightarrow Q$

- Direct proof: assume P true, use logical deductions, algebra, lemmas (small results) and theorems from class to try to show Q is true.
- Contradiction: assume P is true but Q is false. Show that this yields a logical contradiction (say, contradict a part of the assumption, or run into a logical fallacy like $0 = 1$). Then the original assumption must have been wrong, and Q is true.
  - Good to start these proofs with "Assume, for the sake of contradiction" or "Suppose P is true but Q were false." Something to indicate to the reader that you are doing a contradiction proof.
  - Colloquially, this also gets used for: if you're trying to show a statement A is true, you assume $\neg A$ is true instead and run into a contradiction.
- Contrapositive: show $\neg Q \Rightarrow \neg P$.

We focus on direct proof today.

Two exercises:

- **Show that x even, y odd $\Rightarrow x + y$ odd.**
- **Show that x odd $\iff x + 2$ odd.**

Proof of the first result: Since x even, y odd: by definition we have

$$x = 2k$$
$$y = 2\ell + 1$$

with k, ℓ integers. Then $x + y = 2k + 2\ell + 1 = 2(k + \ell) + 1$. $k + \ell$ is an integer since k, ℓ are integers. Thus, by definition, $x + y$ is odd. □

Similar definition unwinding yields the second result.

Things to note: using separate variables for writing $x = 2k$, $y = 2\ell + 1$. At each point we are clear about what results/definitions/information/etc we are using. Note that for the second result: make sure proof has two parts.

5. Jan 22 (Proof methods 2: contradiction, contrapositive)

This lesson we focus more on contradiction, contrapositive: i.e. the methods that involve some sort of negation.

Warmup: you may assume every integer is exactly one of even or odd. Show that x^2 even $\Rightarrow$ x even.

Proof. (Note that this is hard to do directly! Contrapositive helps flip this into turning info about x into info about x^2 in a pretty straightforward manner.) We use proof by contradiction: we will show x not even $\Rightarrow$ x^2 not even. Equivalently, this means showing x odd $\Rightarrow$ x^2 odd. If x is odd, then $x = 2k + 1$ for some k an integer. Then:

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

$2k^2 + 2k$ is an integer because k is an integer. So by definition, x^2 is odd and we are done. □

Next, some definitions. A number x is **rational** provided that it can be written as $x = \frac{p}{q}$ where p, q are integers and $q \neq 0$. A number is **irrational** if it is not rational.

Show: if x is rational, y irrational, then $x + y$ is irrational.

One thing that jumps out: hard to do this directly. Contrapositive seems difficult because negative the left side seems tedious. So let's try contradiction. That will turn $x + y$ irrational into $x + y$ rational, which will be nice to work with.

Proof. Suppose, for the sake of contradiction, that x is rational, y irrational, $x+y$ irrational. Then $x = \frac{p}{q}$ and $x + y = \frac{a}{b}$ with p, q, a, b integers and q, b nonzero. Then:

$$y = (x + y) - x = \tfrac{a}{b} - \tfrac{p}{q} = \frac{aq - pb}{bq}.$$

The numerator and denominator are integers since a, b, p, q are. bq is nonzero because b, q are nonzero. But that means y is rational, which contradicts y being irrational. Hence our assumption is false, and $x + y$ must be irrational. □

We end by trying to prove the following: **Show $\sqrt{2}$ irrational.** Start by supposing, for the sake of contradiction, that $\sqrt{2}$ is rational. Then:

$$\sqrt{2} = \frac{p}{q}.$$

Square both sides, get $2 = p^2/q^2$, equivalently $2q^2 = p^2$. Try messing with even-ness, odd-ness to see if can get a contradiction.

(Another fun result one can do with contradiction: $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$ is never an integer).

6. Jan 24 (Proof methods 3: contradiction, casework)

We finish the proof of $\sqrt{2}$ irrational. Intuitively: look at $2q^2 = p^2$. Look at the prime factorization of each. The number of 2's on the left is odd, the number of 2's in the right is even (because the primes in the factorization of a square all have even power).

Proof that $\sqrt{2}$ irrational. Suppose, for the sake of contradiction, that $\sqrt{2}$ is irrational. Then

$$\sqrt{2} = \frac{p}{q}$$

We shall assume that p, q are in lowest terms. Squaring both sides and rearranging, we get

$$2q^2 = p^2$$

Looking at this equation, p^2 is even. By a result from last class, this means p is even. Write $p = 2k$, k an integer. Then:

$$2q^2 = (2k)^2 = 4k^2.$$

Cancelling a factor of 2, we see

$$q^2 = 2k^2,$$

hence q is even. But if p, q are both even: the fraction couldn't have been in lowest terms! We could cancel a factor of 2 from top and bottom! So we've arrived at a contradiction. Our assumption must be false, and so $\sqrt{2}$ is irrational. □

The heart of what's going on is factorization issues. We'll see more about factorization in the number theory section of the course.

A nice bookend to the proof methods chunk is to cover proof by cases. We show that $n^2 - n$ is always even by looking at even, odd cases. This and proof of $\sqrt{2}$ help motivate induction. Time permitting, show multiple proofs of $n^2 - n$.

7. Jan 26 (Induction 1)

Results like:

- all fractions can be put in least terms
- all integers are even or odd

rely on induction (or one of its equivalent formulations: strong induction, well ordering principle). It is an axiom, and a very useful and major method. Likened to "mathematical dominos."

Idea of induction: if a property holds for $k = 1$, and a property holding for k implies it holds for $k + 1$, then we can start at 1 and "domino effect" down to get a property holds for all natural numbers ($\{1, 2, 3, 4, \dots\}$). Good for proving a fact holds for all natural numbers.

Proofs by induction always have two parts: base case (the $k = 1$ part) and inductive step (showing the property holds for k implies the property holds for $k + 1$).

Examples of proofs by induction:

- Show that every integer is even or odd. (casework + induction)
- Show that
$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$
for all natural numbers n Note: provides a fun proof that $n^2 - n$ is even as a corollary.
- Show that $k^3 + 2k$ is always divisible by 3.
- Show that
$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$
for all natural numbers n
- Show that
$$\sum_{k=1}^{n} k(k+1) = (1 \times 2) + (2 \times 3) + (3 \times 4) + \cdots + (n \times (n+1)) = \frac{n(n+1)(n+2)}{3}$$
for all natural numbers n.

Proof of the second statement. We use proof by induction. Base case: note that $1 = \frac{1(2)}{2}$ so the formula holds for $k = 1$.

Inductive step: suppose the formula is true for k. Then:

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

which means the formula is true for $k+1$. So, by induction, the formula is true for all natural numbers n. □

8. Jan 29 (Induction 2)

Start with note about for all, there exists. $P(x)$ being some property of x, etc. Recall $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.

Go over

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

more slowly.

Induction

- Useful for proving things about the natural numbers (and this sometimes lets you yield statements about $\mathbb{Z}, \mathbb{Q}$)
- Useful in situations with *recursive structure* or properties that can "build up"

Let's get some motivation for why this might be true:

- $n = 1$: Well, $1 = 1(1+1)/2$.
- $n = 2$ Well, $1 + 2 = 3 = 2(2+1)/2$.
- $n = 3$ Well, $1 + 2 + 3 = 6 = 3(3+1)/2$.

Grouping trick: first and last add to $n+1$. Second and penultimate add to $n+1$. And so on, and there will be $n/2$ such pairs (if n even get $n/2$ pairs and if n odd get $(n-1)/2$ pairs and a loner with the value of $(n+1)/2$).

Then: circle back to induction and formal proof Say you want a property P to hold for all natural numbers, so write $P(k)$ to denote the property for the natural number k. (ex: $P(k)$ is the property that $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$).

Induction says that if you have the following:

- $P(1)$ is true
- $P(k)$ is true implies $P(k+1)$ is true

then $P(k)$ is true for all natural numbers k. That is, your desired property is true for every natural number. (With our example choice of P, this would mean the formula for $1 + \cdots + n$ always holds.

Proof. We use proof by induction. Base case: note that $1 = \frac{1(2)}{2}$ so the formula holds for $k = 1$.

Inductive step: suppose the formula is true for k. Then:

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

which means the formula is true for $k+1$. So, by induction, the formula is true for all natural numbers n. □

9. Jan 31 (Induction 3: more examples)

Use induction to show all integers are even or odd. The main thing is that we need to start by doing this for all *natural numbers* n, and then handle 0 and negatives separately. The last part is either done by some slightly tedious algebra or just checking that (-1) is odd and citing that odd $\times$ odd, even is odd, even respectively.

This is a special case of the *division algorithm*, which we will see in the next unit (number theory). This is saying we can divide a number by 2 with remainder, and the remainder has the usual size constraints $0 \leq r < b - 1$ with $b = 2$ here.

10. Feb 2 (Induction 4: strong induction)

Suppose we want some property P to hold for all natural numbers n. Let $P(n)$ to denote the property for the natural number n. Strong induction says: if you have the following

- $P(1)$ is true
- ($P(k)$ true for $1 \leq k < n \Rightarrow P(n)$ true) is true

then $P(n)$ is true for all natural numbers n.

One of the first applications of this is showing every fraction can be put in least terms. Another classical application is showing the fundamental theorem of arithmetic (every integer decomposes as a unique product of primes. We'll see this later).

For our first application, we'll do that every natural number is 1 or splits as a product of primes. (Main part: in inductive step, you'll have n. If it is prime, done. If it splits, write $n = ab$ with $1 \leq a, b < n$. Then can apply the inductive hypothesis to get a, b are products of primes (and so n is a product of primes).

End on an example of finding an error in a proof:

False theorem: if the sum of two integers is even, then both integers are even ($m+n$ even $\Rightarrow m, n$ even).

Proof. Assume, for the sake of contradiction, that the result is false, i.e. either m or n is odd. Then $m = 2k + 1$ and $n = 2j$ with $j, k \in \mathbb{Z}$ (swap the label of m and n as needed). Then:

$$m + n = 2(k + \ell) + 1$$

is odd. Contradicts our assumption that $m+n$ is even. So our assumption is false and the theorem is true. □

Where is the error? (Where: in the contradiction setup, assumed *either* m or n is odd. Why: it's assumed precisely one odd one even, when the failure could come from both odd. In failing to account for this, they miss the phenomena that m odd and n odd will yield $m + n$ even, which is where this theorem fails).

Can also write a proof of $\sqrt{m}\sqrt{n}$ an integer, then $\sqrt{m}/\sqrt{n}$ is rational.

Can also do a strong induction example or take HW 1/ HW 2 questions. Strong induction example: We will define a sequence of numbers. Let $a_1 = 1, a_2 = 2$, and then for $n \geq 3$ we set

$$a_n := a_{n-1} + a_{n-2}.$$

Use strong induction to show that $a_n < 2^n$ for all $n \in \mathbb{N}$. (Need two base cases!)

11. Feb 5 (Induction 5: putting fractions in least terms)

We'll show that every fraction can be put into least terms. Let $P(n)$ be the property that

For every $m \in \mathbb{Z}$, m/n can be put in least terms.

(This is saying that any fraction that can be written with a denominator of n can be written in least terms) We first show that $P(1)$ holds. Certainly $m/1 = 1$ is in least terms; the only factors 1 has is $1, -1$, so we can't do any cancellation from the top and bottom.

Next we show $P(k)$ true for $1 \leq k < n$ implies that $P(n)$ is true (n is an arbitrary natural number). Boils down to: if you can put fractions with denominator $< n$ in least terms, can you put fractions with denominator $= n$ in least terms?

Assume that indeed, $P(k)$ is true for $1 \leq k < n$. Note that our goal is to show every m/n can be put in least terms. Well, either m/n is in least terms (and we are fine), or it is not. In that case,

$$\frac{m}{n} = \frac{m'}{n'}$$

with $1 \leq n' < n$. Note that the fraction on the right has a smaller denominator, so $P(n')$ is true. In particular, m'/n' can be put in least terms. So $m/n = m'/n'$ can be put in least terms. No matter what, we can always put m/n in least terms. So $P(n)$ holds. By strong induction, $P(n)$ holds for all n, and so all fractions can be put in least terms.

(Rephrase to students: we're saying: need to show: if we can put m/k in least terms for every $k < n$, then m/n can always be put in least terms).

12. Feb 7 (Division algorithm 1)

Hamkins 3 material.

Talk about division with remainder: put as many copies of b into a, get a leftover bit. The remainder should be $o \leq r < b$, otherwise I could shrink it.

For $a \in \mathbb{Z}, b \in \mathbb{N}$ with b nonzero, can find *unique* q, r such that $a = bq + r$ with $0 \leq r < b$. This is the division algorithm. It is division with remainder. q is the quotient, and r is the remainder.

So, with $a = 12, b = 5$ performing the division algorithm is $12 = 5 \cdot 2 + 2$, i.e. we put as many copies of 5 as we can into 12, and then we have a remainder that is non-neg and strictly less than the thing we're dividing with.

With $a = 27, b = 8$, performing the division algorithm yields $27 = 8 \cdot 3 + 3$. When $a = 16, b = 8$ we get $16 = 8 \cdot 2 + 0$.

In fact, can let a just be an integer, no necessarily positive. Still get that $a = bq + r$ with $0 \leq r < b$.

Restrict to $b = 2$ case: Note that diving by 2 always gets a remainder of 0 or 1. i.e. division algorithm being true $\Rightarrow$ every natural number even or odd.

So splitting into even and odd cases in proofs was like splitting into cases based on remainder when dividing by 2. Leads us to another example of useful cases: we can split into cases based on remainder when dividing by, say, 3 or 5.

Example: Can split into cases by remainder ($3k$, $3k + 1$, $3k + 2$) to show that $n(n + 1)(n + 2)$ is always divisible by 3. (You could do this with induction too, but it's a little painful and less intuitive).

Start proof of division algorithm.

13. Feb 9 (Division algorithm 2)

Prove the division algorithm. Handle $b = 1$ case separately. Fix b. We'll show that division works for $a \in \mathbb{N}$, but holds for $a \in \mathbb{Z}$ in general. For fixed b, we then induct on a:

$$P(n): \text{ there exists } q, r \in \mathbb{Z} \text{ such that } n = bq + r \text{ with } 0 \leq r < b.$$

(i.e. $P(n)$ is the property that n can be divided by b with remainder). Do scratch work on side with $b = 4$ to see:

$$5 = 4 \cdot 1 + 1$$
$$6 = 4 \cdot 1 + 2$$
$$7 = 4 \cdot 1 + 3$$
$$8 = 4 \cdot 2 + 0$$
$$9 = 4 \cdot 2 + 1$$
$$10 = 4 \cdot 2 + 2$$

In general, seems like we increment remainder by 1 unless $r = b - 1$, in which case we have to be careful. Suggests that we need to split proof into cases. Back to the proof:

Base case: $1 = b \cdot 0 + 1$. $0 \leq 1 < b$ since we can assume $b \geq 2$ (as we handled $b = 1$ separately).

Inductive step: We need to show $P(n) \Rightarrow P(n+1)$. We know we can write $n = bq + r$, $0 \leq r < b$.

Case 1: $r < b - 1$. Then $n + 1 = bq + (r + 1)$ and $0 \leq r + 1 < b$.

Case 2: $r = b - 1$. Then $n + 1 = b(q + 1)$, and $r = 0$.

End on proving $n(n+1)(n+2)$ is always a multiple of 3 for any $n \in \mathbb{Z}$. This comes from casework: div algorithm says you can split into $n = 3k$ or $n = 3k + 1$ or $n = 3k + 2$. Have students observe: in this case, better to not try to expand the product.

14. Feb 12 (Least number principle/Well ordering principle)

Natural numbers: has smallest element + discreteness means **any nonempty subset of $\mathbb{N}$ has smallest element**. This is LNP.

So: If you look at the collection of natural numbers with a certain property P (and that collection isn't empty) then there is a smallest natural number with that property P.

Strong induction, induction, LNP all equivalent. Some slightly nicer in certain proofs, LNP sometimes "picks out" a number we want with a certain property (good for minimizing/inequality conditions). But in the end the three tools are equivalent. We now reprove some old results with the LNP.

- **Example 1:** Show that for all $n \in \mathbb{N}$ we have $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

  Look at collection of natural numbers such that the formula doesn't hold. We want to show this collection is empty. Suppose, for sake of contradiction, that collection isn't empty. Then it has a least element k. Note: $1 = \frac{1(1+1)}{2}$, so 1 not in the set. So $k \geq 2$. Then $k - 1$ a natural number and not in the set so:

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

  Adding k to both sides:

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

  Contradiction, so assumption was false and collection was empty. So formula holds for all $n \in \mathbb{N}$.

  (Note how you get something like a base case and an inductive step here).
- **Example 2:** Show that all fractions can be put in least terms.

  Take an arbitrary fraction $\frac{a}{b}$. We'll show it can be put in least terms. We may assume $b \in \mathbb{N}$. Look at all the different expressions $\frac{a'}{b'}$ that are equal to $\frac{a}{b}$ and look at the collection of (natural number) denominators b' that appear. Take the smallest one using LNP, call

it b''. There is some associated a'' such that $\frac{a''}{b''} = \frac{a}{b}$, by definition of how we formed this collection.

Can show that $\frac{a''}{b''}$ is in least terms.

- **Example 3:** We'll show the division algorithm works. Fix $b \in \mathbb{N}$ and $a \in \mathbb{Z}$. Look at the collection of non-negative numbers r' that can be written as $r' = a - bq$ for some q. This collection is nonempty (take q to be negative with large absolute value to get *an* example of a $a - bq$ non-negative). Use LNP to take the smallest element, call it r. Can show that $0 \leq r < b$.

  (Remind students: using a slight variant of LNP so that we can work with $\mathbb{N} \cup \{0\}$, but it still works).

15. Feb 14 (Set theory 1)

Today is the first day of set theory. All about collections of objects, and some basic operations you can do on them. Very useful in a "building foundations" sense, since lots of things in math/STEM are phrased in terms of sets. Implicitly you've likely worked with some notion of them in the past, today we talk about them more in detail.

Rigorous definition is... difficult to do! We will not worry too much about it– a colloquial idea is enough, and we understand the operations well enough.

A set is a(n unordered) collection of objects. We usually denoted sets with capital letters. An object a in a set S is called an **element** of that set, and is denoted $a \in S$. We've seen this with, e.g., $2 \in \mathbb{Z}$ and $\frac{3}{4} \in \mathbb{Q}$.

There are two ways we usually denote them. First: There is the **roster method**: just list elements.

$$S = \{\text{red}, \text{green}, \text{blue}\},$$
$$P = \{1, 2, 7, 9\}$$

(The first being a set with three elements: red, green blue. The second being a set with four distinct elements: the numbers 1,2,7,9).

Before we do the second: note that we have some "stock" sets already: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. This will help us with the second method: **set builder** notation, where you characterize the elements of your set as having some shared property. For example:

$$\{x \in \mathbb{N} : 4 \leq x \leq 7\}$$

Read "x in $\mathbb{N}$ such that $4 \leq x \leq 7$". In set builder notation, this set is $\{4, 5, 6, 7\}$, because those are all the x in $\mathbb{N}$ that satisfy the condition after the colon: $4 \leq x \leq 7$.

Another example: $\{x \in \mathbb{R} : |x| < 1\}$ is the interval $(-1, 1)$. (Draw this).

Examples for the class: Draw the following sets on the number line.

- $\{x \in \mathbb{Z} : |x| \leq 2\}$
- $\{x \in \mathbb{R} : x^2 = -1\}$
- $\{x \in \mathbb{R} : x^2 = 4\}$
- $\{x \in \mathbb{R} : x = \frac{n}{2}, n \in \mathbb{Z}\}$

The middle one leads us to: $\varnothing$: the empty set. The set that contains no elements. We use $a \mid b$, read "a divides b," to denote that b is a multiple of a, i.e. $a = bk$ for some $k \in \mathbb{Z}$. Describe the following sets in words.

- $\{x \in \mathbb{Z} : x = 2k,\ k \in \mathbb{Z}\}$
- $\{x \in \mathbb{Z} : a \mid x \Rightarrow a \in \{1, -1, x, -x\}\}$
- $\{x \in \mathbb{R} : x \notin \mathbb{Q}\}$

Some more notation: for two sets A, B, **we say that $A \subseteq B$ if every element of A is an element of B.** (That is: $a \in A \Rightarrow a \in B$ is always true). (So, set theory analogue of implication). Draw venn diagram, possibilities, this is same as containment. Examples:

$$\{1,3\} \subseteq \{1,2,3,4\}, \quad \mathbb{Q} \subseteq \mathbb{R}.$$

If you are trying to show $A \subseteq B$ in a proof: it basically follows the same format always: you fix an arbitrary element a of A. Show that it is in B. Since your choice of a was arbitrary, it works for any element of A. So any element of A is an element of B, and $A \subseteq B$

Let's do a practice problem. We'll show: $\mathbb{Z} \subseteq \mathbb{Q}$. Let n be an element of $\mathbb{Z}$. Then $n = \frac{n}{1}$, and we satisfy the usual conditions for a rational number: $n, 1 \in \mathbb{Z}$ and $1 \neq 0$. So $n \in \mathbb{Q}$. So $n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q}$. Therefore, $\mathbb{Z} \subseteq \mathbb{Q}$. (In practice you don't need to prove "obvious" containments between stock sets, but it's good practice).

(Note: this means that LNP is saying: if $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then S has a smallest element).

Two sets are equal if $A \subseteq B$ and $B \subseteq A$ (set theory analog of a biconditional). Therefore, showing an equality of two sets has two parts: showing $A \subseteq B$ (so $a \in A \Rightarrow a \in B$) and showing $B \subseteq A$ (so $b \in B \Rightarrow b \in A$). For example:

$$\{x \in \mathbb{Z} : x \text{ is even}\} = \{x \in \mathbb{Z} : x/2 \in \mathbb{Z}\}$$

(Run through proof). In practice, you can just say x is even $\iff x/2 \in \mathbb{Z}$, so the two sets above are equal. But we needed a nice simple problem to practice the idea on.

16. Feb 16 (Set theory 2)

Set operations! Union (or) and intersection (and). Set complement. Demorgan's law. Do concrete examples with finite amounts of numbers. Remind them at start: sets are just unordered collections of objects. So the elements don't have to be numbers. $\{[0,1],[2,3]\}$ is a valid two element set. $\{\varnothing\}$ is a valid one element set. Refresh on terminology from other day.

Run through containment proofs: We'll show: $\mathbb{Z} \subseteq \mathbb{Q}$. Let n be an element of $\mathbb{Z}$. Then $n = \frac{n}{1}$, and we satisfy the usual conditions for a rational number: $n, 1 \in \mathbb{Z}$ and $1 \neq 0$. So $n \in \mathbb{Q}$. So $n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q}$. Therefore, $\mathbb{Z} \subseteq \mathbb{Q}$. (In practice you don't need to prove "obvious" containments between stock sets, but it's good practice).

(Note: this means that LNP is saying: if $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then S has a smallest element).

Two sets are equal if $A \subseteq B$ and $B \subseteq A$ (set theory analog of a biconditional). Therefore, showing an equality of two sets has two parts: showing $A \subseteq B$ (so $a \in A \Rightarrow a \in B$) and showing $B \subseteq A$ (so $b \in B \Rightarrow b \in A$). For example:

$$\{x \in \mathbb{Z} : x \text{ is even}\} = \{x \in \mathbb{Z} : x/2 \in \mathbb{Z}\}$$

(Run through proof). In practice, you can just say x is even $\iff x/2 \in \mathbb{Z}$, so the two sets above are

Use venn diagram analogy: define $A \cup B$. Analogue of "or" in that:

$$x \in A \cup B \iff (x \in A \text{ or } x \in B)$$

The formulation on the right is quite useful in proofs.

Use venn diagram analogy: define $A \cap B$. Analogue of "and" in that:

$$x \in A \cap B \iff (x \in A \text{ and } x \in B)$$

Define set difference: $A \setminus B$. (Read: A cut B, A minus B, A setminus B). It consists of all elements of A that aren't in B. i.e.

$$x \in A \setminus B \iff x \in A \text{ and } x \notin B$$

Example time! Say we have $A = \{1, 2, 3, 6\}$ and $B = \{3, 6, 9, 10\}$ and $C = [1, 2]$.

- What is $A \cup B$?
- What is $A \cap B$?
- What is $A \setminus B$?
- What is $B \setminus A$?
- What is $B \cap C$?
- What is $A \cap C$?
- What is $C \setminus A$?

Quick proof: for any two sets A, B, we have that $A \subseteq A \cup B$:

$$x \in A \Rightarrow x \in A \text{ or } x \in B \Rightarrow x \in A \cup B$$

You'll be asked to prove some more complicated facts on your homework. For now, we note a few more:

- $A, B \subseteq A \cup B$
- $A \cap B \subseteq A, B$
- $A \setminus B \subseteq A$.

17. Feb 19 (Set theory 3)

Products and power sets. Indexed unions

Products. Given sets X, Y, we define the set product (or product set, or cross product):

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

i.e. it's the set of **ordered pairs** (x, y) with the first entry being X and the second being in Y.

$$(x, y) \in X \times Y \iff x \in X, y \in Y$$

Examples: If $X = \{a, b, c\}$ and $Y = \{1, 2\}$ then

$$\{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)$$

Notice the number of elements. If $|X|, |Y|$ finite then $|X \times Y| = |X||Y|$.

Example: $\mathbb{R} \times \mathbb{R}$, also denoted $\mathbb{R}^2$, is visualized as the usual x, y plane. Draw that and $[1, 2] \times [3, 4]$ to motivate cross/set product.

Consider the intervals $[0, 1], [3, 5]$ and $[2, 3], [-1, 0]$

- Draw $[0, 1]$ and $[0, 1] \cup [3, 5]$
- Draw $[0, 1] \times [2, 3]$
- Draw $([0, 1] \cup [3, 5]) \times [2, 3]$
- Draw $[0, 1] \times ([2, 3] \cup [-1, 0])$

What pattern do we notice? What do you think $([0, 1] \cup [3, 5]) \times ([2, 3] \cup [-1, 0])$ would look like?

Proposition: (A distributivity-type law) Show that $(A \cup B) \times C = A \times C \cup B \times C$.

Proof.

$$\begin{aligned}
(x, y) \in (A \cup B) \times C &\iff x \in (A \cup B) \wedge y \in C \\
&\iff (x \in A \vee x \in B) \wedge y \in C \\
&\iff (x \in A \wedge y \in C) \vee (x \in B \wedge y \in C) \\
&\iff (x, y) \in A \times C \vee (x, y) \in B \times C
\end{aligned}$$

The second-to-last bit comes from the distributive property in logic: $(Q \vee R) \wedge P = (Q \wedge P) \vee (R \wedge P)$. Our chain of biconditionals implies that $(A \cup B) \times C = (A \times C) \cup (B \times C)$. □

Being able to reason out some of these set theory equations and their logic equivalents is useful for things like probability.

Power sets. Given a set A, it has a *power set*, denoted $\mathscr{P}(A)$. (Different from $P(k)$ in induction!!) $\mathscr{P}(A)$ **is the set of all subsets of** A**.**

Example: (count by number of elements)

$$\mathscr{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

Yes, the empty set counts! Every element of the empty set is an element of $\{1,2,3\}$. This is *vacuously* true. We can never pick any elements; all zero of the elements in $\varnothing$ are in $\{1,2,3\}$. As in, $x \in \varnothing \Rightarrow x \in \{1,2,3\}$ is true, because the first part is always F. So $\varnothing \subseteq \{1,2,3\}$.

And then ask: what should this be?

$$\mathscr{P}(\varnothing) = \{\varnothing\}$$

Can also ask:

- Is $\{\varnothing\} \subseteq \mathscr{P}(\varnothing)$? (yes)
- Is $\{\varnothing\} \in \mathscr{P}(\varnothing)$? (no)
- Is $\varnothing \in \mathscr{P}(\varnothing)$? (yes)
- Is $\varnothing \subseteq \mathscr{P}(\varnothing)$? (yes)

— If time, cover indexing sets. Likely not. So give sufficient characterization to do the HW and expound next class. $A_i = \{1, 2, \ldots, n\}$.

$$x \in \bigcup_{i \in \mathbb{N}} A_i \iff x \in A_n \text{ for some } n \in \mathbb{N} (\iff \exists n \text{ s.t. } x \in A_n)$$

$$x \in \bigcap_{i \in \mathbb{N}} A_i \iff x \in A_n \text{ for every } n \in \mathbb{N} (\iff \forall n \in \mathbb{N}, x \in A_n)$$

18. Feb 21 (Set theory 4)

First, let's talk about unions indexed over $\mathbb{N}$. (Might want to motivate with sigma notation. $1^2 + 2^2 + \cdots + n^2$ clunky so could write as $\sum_{i=1}^{n} i^2$ instead).

Could take union of two sets A_1, A_2. Drag venn diagram. Maybe union with a third set A_3.

$$x \in A_1 \cup A_2 \cup A_3 \iff x \in A_1 \text{ or } A_2 \text{ o r} A_3$$

Similarly with A_4. Can do with A_n.

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i \left(= \bigcup_{i \in \{1,2,\ldots,n\}} A_i \right)$$

Analogous to sigma notation. The i is the indexing variable, start at 1, iterate to get n. The right most is thoguht of as: take every choice of i in the set $\{1, 2, \ldots, n\}$ and add the corresponding A_i to the union.

But sometimes we want to take unions of infinity many sets!

$$\bigcup_{i=1}^{\infty} A_i = (A_1 \cup A_2 \cup \ldots) \left(= \bigcup_{i \in \mathbb{N}} A_i \right)$$

Again: rightmost says you union all the sets A_i with i in the prescribed indexing set.

$$x \in \bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{N}} A_i \iff x \in \text{at least one of the } A_i$$

Above: It's an existence statement

Example: let $A_i = \{2i, 4i\}$ for $i \in \mathbb{N}$. What is $\cup_{i\in\mathbb{N}} A_i$?

Next, sometimes we want unions over index sets that aren't like $\mathbb{N}$. Maybe want them indexed by the real numbers instead. Suppose you have an indexing set I, and for each choice of $i \in I$, you have a set B_i. So you have a family of sets $\{B_i : i \in I\}$. Then you can form a new set $\cup_{i\in I} B_i$. It is characterized by:

$$x \in \bigcup_{i\in I} B_i \iff \text{there exists an } i \in I \text{ such that } x \in B_I$$

i.e. the elements of the union are elements that appear in at least one B_i.
Example: for $r \in \mathbb{R}$, let $B_r = \{r\}$. Then:

$$\bigcup_{r\in R} B_r = \mathbb{R}$$

A similar idea extends to intersections.

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

where x is in this set if and only if it's in all of them. Likewise:

$$x \in \bigcap_{i=1}^{\infty} A_i = \bigcap_{i\in\mathbb{N}} \iff x \in A_i \text{ for all } i \in \mathbb{N}$$

and then we can do intersections with any sort of indexing set. I an indexing set, have a B_i for each $i \in I$. Then:

$$x \in \bigcap_{i\in I} B_i \iff x \in B_i \text{ for } \underline{\text{every}}\ i \in I$$

Example: let's use $\mathbb{R}$ as an indexing set again. For $r \in \mathbb{R}$, set $B_r = \{0, r\}$. Then

$$\bigcap_{r\in\mathbb{R}} B_r = \{0\}.$$

If $B_r = \{r\}$, then $\cap_{r\in\mathbb{R}} = \varnothing$.
If time, do power set counting stuff. Or ask: is $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$?
If time, could also do $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

19. Feb 23 (Set theory 5)

We'll do examples of indexed unions, intersections. Key formulas: if $I \subseteq J$ then:

$$\bigcap_{i\in I} B_i \supseteq \bigcap_{j\in J} B_j$$

(makes sense: intersecting more sets should make the intersection smaller). If $I \subseteq J$ then:

$$\bigcup_{i\in I} C_i \subseteq \bigcup_{j\in J} C_j$$

(makes sense: unioning more sets should make the union bigger).

- **Example 1**:

$$\bigcap_{r\in\mathbb{R}} [r^2 - 1, r^2 + 1] = \varnothing$$

Note: each individual $[r^2-1, r^2+1]$ is an interval with length 2, and as r ranges they can be very far apart! In particular, if we pick, say, $r = 0$ and $r = 10$ we get

$$\bigcap_{r\in\mathbb{R}} [r^2-1, r^2+1] \subseteq [-1,1] \cap [99,100] = \varnothing$$

which means this intersection must be $\varnothing$.

- **Example 2**:

$$\bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1] = [-1,1]$$

Intuitively: as we increase the size of $|r|$, get a window "growing" around $[-1,1]$. Minimum at $r = 0$, which is $[-1,1]$. So intersection is $[-1,1]$.

More formally: every $[-r^2-1, r^2+1]$ contains $[-1,1]$ so, since the intersection consists of elements common to each "piece," we get

$$[-1,1] \subseteq \bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1]$$

On the other hand, the intersection is a subset of any $[-r^2-1, r^2+1]$ piece. Pick $r = 0$ to get:

$$\bigcap_{r\in\mathbb{R}} [-r^2-1, r^2+1] \subseteq [-1,1]$$

Hence we have both containments and the two sets are equal.

- **Example 3**:

$$\bigcup_{n\in\mathbb{Z}} ([-2,|n|] \cap \mathbb{Z}) = [-2,\infty) \cap \mathbb{Z}$$

Note: our final answer definitely needs to be a subset of $\mathbb{Z}$ since every $[-2,|n|] \cap \mathbb{Z}$ is a subset of $\mathbb{Z}$. As we increase $|n|$ we can get arbitrarily large integers in this union, and all the integers below until -2.

- **Example 4**:

$$\begin{aligned}\bigcup_{n\in\mathbb{N}} (n-1, n) &= (0,\infty) \setminus \mathbb{N} \\ &= (0,\infty) \setminus \mathbb{Z} \\ &= \{x \in \mathbb{R} : x > 0 \wedge x \notin \mathbb{Z}\}\end{aligned}$$

Best way to see this is to draw the first few terms in this union: $(0,1), (1,2)$, etc. Get all positive numbers, except the positive integers.

20. Feb 26 (Exam review)

Do practice problems from sheet, discuss proof strategies.

21. Feb 28 (N/A due to exam)

Administer exam.

22. March 1 (Relations 1)

(Reference: Hamkins chapter 11, Taylor chapter 5)

Math and real life full of relations: a way to associate certain pairs of objects, numbers, people, etc usually based on some property. Examples of relations:

aSb we write this if person a is a sibling of b. $x = y$: we write this if the two numbers are the same $x < y$: write if y is bigger than x (i.e. $y - x$ is positive)

In general, a relation on a set S is a subset of $S \times S$. If $R \subseteq S \times S$ is our relation subset, we say s is related to t if and only if $(s, t) \in R$. For shorthand, we'd usually write $s \sim t$. If we have multiple relations running around in a problem, we might do $\sim_1, \sim_2$ to differentiate them.

(Can also define a relation between X and Y: it is again a subset of $X \times Y$ and is meant to relate objects of X to objects of Y, often under some nice rule. For now we focus on binary relations, i.e. between a set and itself.).

- If the relation is equals, the associated subset of, say, $\mathbb{R} \times \mathbb{R}$ is $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y\}$
- If the relation is $x < y$, the associated subset of $\mathbb{R} \times \mathbb{R}$ if $R = \{(x, y) : y - x \text{ is positive}\}$.

Example: If $S = \{1, 2, 3\}$ and we have the relation $R = \{(1, 1), (1, 2), (2, 1), (1, 3), (3, 1)\}$. Which of the following is true?

- $1 \sim 1$? (Yes)
- $3 \sim 1$? (Yes)
- $3 \sim 2$? (No)

We often like relations with some nice properties. Suppose R is a relation on a set S.

- A relation R is **reflexive** if $s \sim s$ for all $s \in S$,
- R is **symmetric** if, whenever $s \sim t$, then also $t \sim s$. (So, for all $s, t \in S$: $s \sim t \Rightarrow t \sim s$).
- R is **transitive** if, whenever $s \sim t$ and $t \sim u$, then also $s \sim u$). (So, for all $s, t, u \in S$: $s \sim t$ and $t \sim u \Rightarrow s \sim u$).

Is our example relation reflexive? Symmetric? Transitive? Asking for a relation on some fixed set that is some number of reflexive, symmetric, transitive is a common question, so want to become comfortable with such problems as you go through this unit.

Let's do more examples: recall the divides symbol $|$. $|$ is a relation on $\mathbb{Z}$: we say $a \mid b$ if and only if $b = ak$ for some $k \in \mathbb{Z}$.

Question: is $|$ reflexive? Symmetric? Transitive?

23. March 4 (Relations 2)

Review equivalence relations, reflexive/symmetric/transitive. One use of equivalence relations is they split a set into *equivalence classes*. Sometimes it is useful to consider equality up to equivalence classes.

If R is an equivalence relation on a set S, then for any element $s \in S$, we can define its equivalence class.

$$[s] = \{t \in s : s \sim t\}$$

Because $R, \sim$ is an equivalence relation, the set of equivalence classes form a *partition* of S. That is, it is a collection of sets that are pairwise *disjoint* (i.e. if $[s_1] \neq [s_2]$, then $[s_1] \cap [s_2] = \varnothing$) and the union of all the equivalence classes is the whole set S. Note that this means if $[s_1] \cap [s_2] \neq \varnothing$, then $[s_1] = [s_2]$. See Hamkins 11.3 for more details.

Do an example: a relation on the integers $\mathbb{Z}$, where $x \sim y \iff x, y$ have the same parity. (Parity is the even-ness or odd-ness of a number. For example the parity of 2 is 'even' and the parity of 7 is 'odd.' $f(n) = (-1)^n$ is a function that depends only on the *parity* of the number n).

Show reflexive, symmetric, transitive. Demonstrate that this splits the integers into two equivalence classes (not infinitely many! Because lots of equiv classes the same!)

End by talking about how a partition yields an equiv relation.

24. March 6 (Functions 1)

Taylor 5 a little more comprehensive in terminology.

A *function* f from a set A to a set B ($f : A \to B$) does the following: for each $x \in A$, it assigns some $u \in B$ (and assigns only *one* value!). That element y is denoted by $f(x)$.

Example: functions from real numbers to real numbers, $f(x) = x^2$, $g(x) = \sin x$, $h(x) = -x$.

Example: $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7, 8\}$, sending

$$1 \mapsto 5$$
$$2 \mapsto 8 \quad 3 \mapsto 6$$

A way that mathematicians are fond of packaging all this info is:

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

for example, the squaring function:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

Now, there are a lot of new definitions/terminology when we talk about functions! We'll get used to them as we use them, feel free to stop and ask me about any of these new words.

Another word for a function is a **map**, and we say f is a **map** from A to B. A is the **domain**, B is the **codomain**. The **range** or **image (of A)** is

$$f(A) = \{y \in B : y = f(a) \text{ for some } a \in A\} = \{f(a) \in B : a \in A\}$$

i.e. all the things actually "hit" by the map/function. Note that $f(A) \subseteq B$, but is not necessarily equal to B.

Graph the following functions. What are the domains, codomains, and images of the following:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \\ g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin x \\ h : \mathbb{Z} &\to \mathbb{N} \\ x &\mapsto |-x| \\ \alpha : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto 2x \end{aligned}$$

If we have a function $f : A \to B$, and $A' \subseteq A$, then we can also look at the image of A', i.e.

$$f(A') = \{y \in B : y = f(a) \text{ for some } a \in A'\} = \{f(a) \in B : a \in A'\}$$

that is, you just look at the elements getting mapped to from stuff *specifically in* A'.

Relatedly, we can define the **restriction** to A:

$$\begin{aligned} f|_{A'} : A' &\to B \\ a &\mapsto f(a) \end{aligned}$$

i.e., the function rule is the same, you just consider the function on fewer elements. Ex: graph $f|_{[0,\infty)}$ with f as above (the squaring map). Or $g|_{[0,2\pi]}$. Or $h|_{2\mathbb{Z}}$ (the even integers). They will look like a smaller portion of the full graph.

25. March 8 (Functions 2)

Finish up restriction from last time. Talk about image in general. And then define the preimage. $f : A \to B$, then for $B' \subseteq B$ we define

$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

that is, it's a subset of A consisting of all elements that land in B' after you apply the function f.

Demonstrate with $g(x) = \sin x$. Take $g^{-1}(\{0\})$ and $g^{-1}([-1, 0])$.

- $g^{-1}(\{0\}) = \{\dots, -2\pi, -\pi, 0, \pi, 2\pi, 3\pi, \dots\}$
- $g^{-1}([-1, 0]) = \bigcup_{n\in\mathbb{Z}}[2(n-1)\pi, 2n\pi]$
- $f^{-1}([0, 1/4]) = [-1/2, 1/2]$.

Time for even more definitions!

- A function $f : A \to B$ is **injective** if $f(x) = f(y) \Rightarrow x = y$. That is, no two elements of A map to the same element of B.
- A function $f : A \to B$ is **surjective** if, for any $y \in B$, you can find some $x \in A$ such that $f(x) = y$, That is, you can hit everything in B. i.e., $f(A) = B$.
- A function $f : A \to B$ is **bijective** if it is both injective and surjective.

[Draw arrow diagrams of the usual injective/surjective/bijective]

If A, B are finite sets, then an injection $A \to B$ means $|A| \leq |B|$. A surjection means $|A| \geq |B|$. And a bijection means $|A| = |B|$ (so sometimes a clever way to show two numbers are equal is to relate the two quantities to sizes of sets, and write down a bijection). We'll prove some of these in class and some in HW.

The idea is that bijections pair up elements: nice and *invertible*.

For f, g, h, α as they are above:

- f is not injective and not surjective. $f(-1) = f(1)$. $f|_{[0,\infty)}$ is injective, though. And $f : [0, \infty) \to [0, \infty)$ is injective and surjective.
- g is not injective and not surjective. $g(0) = g(2\pi)$.
- h is surjective, but not injective. $h(-1) = h(1)$.
- α is injective, but not surjective.

26. March 11 (Functions 3)

We should do an example of proving something is a bijection.

Proposition 26.1. The function

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ n &\mapsto n + 1 \end{aligned}$$

is a bijection.

Proof. First, we show the function is injective. Suppose $f(x) = f(y)$. That means that $x+1 = y+1$. Subtracting 1 from both sides, we get $x = y$ as desired.

Next, we show the function is surjective. Let $y \in \mathbb{Z}$. We want to show there is some $x \in Z$ such that $f(x) = y$. Well, pick $x = y - 1$. Then $f(x) = (y - 1) + 1 = y$, and we are done.

Since f is injective and surjective, it is bijective. □

(Note: some of this extra exposition written for the benefit of students, but could be trimmed down in an exam situation).

Next, let's talk about some nice properties of injections. Nice prop of surjection done on HW.

Function composition: $f : A \to B$ and $g : B \to C$, can define:

$$g \circ f : A \to C$$
$$x \mapsto g(f(x))$$

i.e. $g \circ f(x) = g(f(x))$.

Proposition 26.2. If $f : A \to B$ is injective and $g : B \to C$ is injective, then $g \circ f : A \to C$ is injective.

Proof. We'll show $g \circ f : A \to C$ injective. (This means: whenever $g(f(x)) = g(f(y))$, we need $x = y$).

Well, take $g(f(x)) = g(f(y))$. Since g is injective, we get $f(x) = f(y)$. Since f is injective, we get $x = y$. □

Proposition 26.3. If A is a finite set, then there does not exist an injection $f : A \to B$ with $|B| < |A|$.

Proof. We induct on the size of the set. First, note that the above is true for a set with 0 elements, i.e. $A = \varnothing$, then this easily holds because there is no set with number of elements < 0.

We now handle the case of $1 \leq |A| < \infty$. Define $P(k)$ to be the property that:

> Any set with k elements cannot inject into a smaller set.
>
> That is, for any A with $|A| = k$, and any B with $|B| < k$, there is no injection $A \to B$.

It is enough to show that $P(k)$ is true for all k (as we range over k, get all finite sets).

Base case: $P(1)$ is true, can't have an injection to the empty set (can't have a function, in fact).

Inductive step: Suppose $P(k)$ true. We'll show $P(k+1)$ true.

To show $P(k+1)$ true, let A be an arbitrary set with $k+1$ elements. Let B be an arbitrary set with fewer than $k+1$ elements. We need to show there is no injection $f : A \to B$.

Suppose such an injection f exists. Pick $a \in A$. We know it maps to some $f(a) \in B$, and we know it's the only element of A that maps to it. So we get a well-defined function (draw picture):

$$f' : A \setminus \{a\} \to B \setminus \{f(a)\}$$
$$x \mapsto f(x)$$

this is essentially a restriction of f with the codomain adjusted. Then f' is well-defined, and still injective. And:

$$k + 1 = |A| > |B| \Rightarrow k = |A \setminus \{a\}| = |A| - 1 > |B| - 1 = |B \setminus \{f(a)\}|.$$

But then we have an injection from a set with k elements to a set with fewer than k elements. This contradicts $P(k)$. So our assumption must be false, and no such f exists. This means $P(k+1)$ is true.

Then by induction, we get that a finite set cannot inject into a smaller set. □

27. March 13 (Functions 4)

Suppose $f : X \to Y$. Then f is invertible if there exists $g : Y \to X$ such that $(f \circ g)(y) = y$ for all $y \in Y$ and $(g \circ f)(x) = x$ for all $x \in X$.

For example: $f : \mathbb{R} \to \mathbb{R}$ given by $x \mapsto x + 1$ has inverse $x \mapsto x - 1$.

Key idea: invertible $\iff$ bijective. It is part of why we like bijections so much. (Draw picture: pair up elements, track back up the arrow).

Invertible $\Rightarrow$ bijective: Suppose $f(x_1) = f(x_2)$. Then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, so injective. And for any $y \in Y$, note that $f(g(y)) = y$, so f surjective.

Bijective $\Rightarrow$ invertible: Define the inverse as follows: for $y \in Y$, define $g(y)$ to be the unique x mapping to it (which has to exist for a bijection). One can check that $f(g(y)) = y$ and $g(f(x)) = x$.

(Can also view through relation perspective. A relation on $A \times B$ with the property that for every $a \in A$, unique b such that $(a, b) \in R$. Can flip $R' \subseteq B \times A$ – see Hamkins. If this has function property above, get that this functions as inverse. This perspective less stressed in this course.)

Give examples of computing inverses $y = f(x)$ and solve for x in terms of y.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto x + 1 \end{aligned}$$

Set $y = f(x) = x + 1$. Like one might do in Calc I/II, we solve for x in terms of y to see what the unique x mapping to a given y in the codomain is. This should be the inverse, if we look above at the bijective $\Rightarrow$ invertible paragraph.

$$y = x + 1 \Rightarrow x = y - 1$$

so the inverse is $g : \mathbb{Z} \to \mathbb{Z}, y \mapsto y - 1$.

Now consider

$$\begin{aligned} F : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3 \end{aligned}$$

Set $y = x^3$. Then $x = y^{1/3}$. And one can indeed check that $G : \mathbb{R} \to \mathbb{R}, y \mapsto y^{1/3}$ is the inverse of F.

28. March 15 (Combinatorics 1)

We now shift to combinatorics. The reference for this is Hamkins 5.6. If any additional texts are needed, I will either provide notes or link a free source.

Combinatorics is an area of math that concerns *counting*. Nice applications such as: if I have to compute...

$$\begin{aligned} (x + y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\ (x + y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \end{aligned}$$

I can perform this computation quite quickly, without doing the extremely tedious work of expanding out the 4-term multiplication. How is this possible? Through a result of combinatorics.

As we'll see after the break, many results in combinatorics have two proofs with two distinct flavors: a proof involving careful algebra to manipulate an algebraic formula (like the factorial formula for $\binom{n}{k}$ seen below) *or* a clever counting argument that shortens the proof to a couple lines.

We first concern ourselves with choosing objects when caring about order, i.e. permutations.

- How many ways to choose an object from 3 objects? 3
- How many ways to choose two objects from three objects (while caring about the order in which we choose them)? There are 6. If you label the objects A, B, C, the possibilities are:

  $$AB, AC, BA, BC, CA, CB$$

  Another way to see it is 6: note that $6 = 3 \cdot 2$. When picking the objects: think about your three objects being in a bucket, and pulling out one object and then another. There are three options for the first choice. Then two options for the second choice. So there are $3 \cdot 2$ options.

What about picking 3 objects from a collection of 4 objects (caring about order)? Again we can imaging picking them out of a bucket. There are 4 choices when we pick the first object. Then 3 choices for the second. And then 2 choices for the next. So there are $\mathbf{24} = 4 \cdot 3 \cdot 2$ ways to choose three objects from four when caring about order.

This motivates a definition. We define the symbol $n!$ to be the quantity...

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

In order for some formulas to work out, we define

$$0! = 1$$

And do note that:

$$(n+1)! = (n+1) \cdot (n!)$$

Let's return to our discussion of choose objects. As we see from out previous examples, the number of ways to choose k objects from a collection of n objects (when caring about the order we choose them in) is:

$$n(n-1)(n-2)\dots(n-(k-1)) = n(n-1)(n-2)\dots(n-k+1)$$

We can express this as:

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

Note that this means the number of permutations of n objects (i.e. the number of ways to rearrange n objects) is $n!$.

Now: what if we don't care about the order of the objects? So now things like AB are considered the same as BA. (Think about picking groceries and tossing them in a cart: don't really care what order you put them in. Mathematically, there are lots of scenarios where you're picking objects but don't care about the order).

Consider two objects, A and B. If we picked two objects from these two objects and cared about order: there would be two options: AB and BA. If we don't care about order, then there is only one option.

Consider three objects: A, B, C. If we picked two objects from these three and cared about order: there would be six options. But remember those options are AB, AC, BA, BC, CA, CB. If we don't care about order, then stuff like AC and CA should be considered the same. i.e. this list double counts if we're not caring about order. **So:** if we pick two objects from three objects and don't care about order, there are **three options**. The best way to think about this is $\frac{3\cdot 2}{2}$. There are $3 \cdot 2$ ways to pick when caring about order, and then we divide by 2 to account for the double-counting.

Consider four objects: A, B, C, D. If we pick three objects from this and care about order, there are $24 = \frac{4!}{(4-1)!}$ options. But like we discussed before: this number over-counts if we don't care about order. We need to divide by something to account for that. Specifically, we want to divide by the number of ways to re-arrange 3 objects. Because if we have a choice like ABC then the permutations

$$ABC, CAB, BCA, BAC, CBA, ACB$$

all correspond to the same thing. There are $6 = 3 \cdot 2 \cdot 1$ ways to permute three objects. So there are:

$$\frac{24}{6} = \frac{(4!/(4-1)!)}{3!} = 4$$

ways to pick three objects from four when not caring about order.

In general, we can obtain a formula for the number of ways to choose k objects from n objects. This quantity is denoted by $\binom{n}{k}$ and read aloud as "n choose k." We start by looking at the $\frac{n}{(n-k)!}$ ways to choose k objects with order, and then divide out by the number of ways to rearrange the k objects. In the end we get:

$$\begin{aligned}\binom{n}{k} &= \text{number of ways to choose } k \text{ objects from } n \text{ objects without order} \\ &= \frac{n!}{(n-k)!k!}\end{aligned}$$

These are also known as **binomial coefficients**.

One really fun thing to note: this means the fraction $\frac{n!}{(n-k)!k!}$, which at first just looks like some element of $\mathbb{Q}$, in fact has to be an integer! That's because it's counting an integer quantity.

29. March 25 (Combinatorics 2)

We begin with review of last time: the major formulas and how to derive them. **Also, note that when $k < 0$ or $k > n$, we have that $\binom{n}{k} = 0$.**

Then, main goal is to work out some rows of Pascal's triangle and observe some patterns. Pascal's triangle is a way of organizing the various binomial coefficients, i.e. the various $\binom{n}{k}$.

$$\begin{array}{ccccccccccccc}
 & & & & & \binom{0}{0} & & & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}$$

With each row, the n value is fixed, and the k value ranges across the row. We then compute:

$$\begin{array}{ccccccccccccc}
 & & & & & 1 & & & & & & & \\
 & & & & 1 & & 1 & & & & & & \\
 & & & 1 & & 2 & & 1 & & & & & \\
 & & 1 & & 3 & & 3 & & 1 & & & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

From here, we have a few observations.

- We can compute a few quick vlaues: $\binom{n}{0} = 1\binom{n}{n}$ is always true. This makes sense: to pick 0 objects from n objects, there's only one option (pick nothing) and to pick n objects there's only one option (pick everything).
- Likewise we see $\binom{n}{1} = n$ always. This also makes sense: this is picking one object from a collection of n objects. There are n possibilities corresponding to the n objects.
- The triangle is symmetric: that is, $\binom{n}{k} = \binom{n}{n-k}$. One way to see this: every choice of k objects yields a choice of $n-k$ objects to *exclude*.
- You can generate an entry by taking the entries to the top-left and top-right of it, and adding them up. Like in the last two rows, observe how $5 + 10 = 15$, $10 + 10 = 20$, etc. This corresponds to Pascal's formula:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

we'll talk more about this formula next time.

30. March 27 (Combinatorics 3)

Today: the fun of combinatorics: can prove things algebraically, or with a clever counting argument! By counting argument, we mean proving an equation holds by proving that both sides of the equation count the same thing/quantity (and therefore they must be equal).

We will prove our observations from last time. First things first, let's observe something:

$$\begin{aligned}\binom{n}{k} &= \#\text{ of } k\text{-element subsets of } \{1,\dots,n\}\\ &= \#\text{ of } k \text{ element subsets of [n]}\\ &= |\{A \in \mathscr{P}([n]) : |A| = k\}|\end{aligned}$$

where $[n] = \{1, 2, \dots, n\}$. If we think of the numbers $1, 2, \dots, n$ as the n objects we can choose from, picking k objects is the same as picking a k element subset (note that subsets do not care about order!). You could replace $[n]$ with any set with n elements in these formulas.

Theorem 30.1. *(Symmetry of Pascal's triangle) For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$, we have that:*

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

Proof 1 (Algebraic)

One way: firstly, note that if $k < 0$, then $n - k > n$ and if $k > n$, then $n - k < 0$. So for $k < 0$ or $k > n$ we get:

$$\binom{n}{k} = 0 = \binom{n}{n-k}$$

For the other cases, we can use the factorial-based formula for $\binom{n}{k}$. Note that:

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{(n-k)!k!}\\ \binom{n}{n-k} &= \frac{n!}{(n-(n-k))!(n-k)!} = \frac{n!}{k!(n-k)!}\end{aligned}$$

so the two quantities are the same.

Proof 2 (Counting)

Recall that $\binom{n}{k}$ counts the number of ways to choose a k-element subset from $[n] = \{1, 2, \dots, n\}$. For every choice of k elements, it gives rise to a choice of $n-k$ elements to *exclude* (i.e., the elements you didn't pick). Observe the following two things:

(1) Every choice of $n - k$ elements arises as one of these sets of excluded elements.
(2) Different choices of k elements give rise to different sets of excluded elements.

Hence, the number of ways to pick a k element subset of $[n]$ is the same as a number of ways to pick an $n - k$ element subset of $[n]$, and we get:

$$\binom{n}{k} = \#\text{ of } k \text{ element subsets of [n]} = \#\text{ of } (n-k) \text{ element subsets of [n]} = \binom{n}{n-k}$$

Proof 3 (A more formalized version of Proof 2)

Consider the following function:

$$f : \{A \in \mathscr{P}([n]) : |A| = k\} \to \{B \in \mathscr{P}([n]) : |B| = n - k\}$$
$$A \mapsto [n] \setminus A$$

f is surjective (this is the same as Observation 1 from Proof 2): for every B in the codomain, note that $f([n] \setminus B) = B$.

f is furthermore injective: if $A_1 \neq A_2$, are distinct elements of the codomain then, after potentially relabeling, there is an element $a \in [n]$ such that $a \in A_1$ and $a \notin A_2$. Then $a \notin f(A_1)$ and $a \in f(A_2)$, so $f(A_1) \neq f(A_2)$. So distinct elements of $\{A \in \mathscr{P}([n]) : |A| = k\}$ map to distinct outputs.

So, f is a bijection. That means the domain and codomain have the same size. So:

$$\binom{n}{k} = |\{A \in \mathscr{P}([n]) : |A| = k\}| = |\{B \in \mathscr{P}([n]) : |B| = n - k\}| = \binom{n}{n-k}$$

and we are done.

Next, we prove the addition formula for Pascal's triangle.

Theorem 30.2. *(Pascal's rule/formula) For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ we have*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Proof 1 (Algebra)
Remember that:

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

Then:

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

Proof 2 (Counting)
But perhaps an easier way to see it is: $\binom{n+1}{k}$ counts the number of ways to choose k objects from $n+1$. Label these objects $1, 2, \ldots, n+1$.

When you pick k objects, you fall into one of two disjoint and exhaustive cases:

(1) Either you do not include $n+1$, and so you are picking k objects from the first n objects $(1, 2, \ldots, n)$
(2) You do include $n+1$ in your choice, and so you pick $k-1$ objects from the remaining n objects $1, 2, \ldots, n$.

So the number of ways to pick k objects from $n+1$ should be the number of options/ways to do Scenario 1, and the number of options/ways to do Scenario 2. But note that the number of ways to do Scenario 1 is $\binom{n}{k}$ and the number of ways to do Scenario 2 is $\binom{n}{k-1}$. Summarized:

$$\begin{aligned}\binom{n+1}{k} &= \#\text{ of ways to pick } k \text{ objects from } n+1\\ &= \#\text{ options in scenario (1)} + \#\text{ options in scenario (2)}\\ &= \binom{n}{k} + \binom{n}{k-1}\end{aligned}$$

So we are done.

One thing to observe: for both these theorems, the counting argument tends to give more "insight" into why these formulas need to be true.

31. March 29 (Combinatorics 4)

First off, since we're taking counting, it would be nice to count the size of the power set. We conjectured a formula last thing based on the fact that:

$$\begin{aligned}|\varnothing| = 0, \quad |\mathscr{P}(\varnothing)| = 1\\ |\{1\}| = 1, \quad |\mathscr{P}(\{1\})| = 2\\ |\{1,2\}| = 2, \quad |\mathscr{P}(\{1,2\})| = 4\\ |\{1,2\}| = 3, \quad |\mathscr{P}(\{1,2,3\})| = 8\end{aligned}$$

Theorem 31.1. *If A is a finite set, then $|\mathscr{P}(A)| = 2^{|A|}$.*

Proof 1.

One way to see this: A is finite, so we can list the elements as $A = \{a_1, a_2, \ldots, a_n\}$. Note that $n = |A|$. Now let $B \subseteq A$ be an element of the power set. For each $a_1, a_2, \ldots, a_n$, we can assign it a ✓ or a $\times$ based on whether B includes that element or not.

For example, for $A = \{1,2,3,4\}$ we would assign the subset $\{1,4\}$ the following sequence of ✓'s and $\times$'s

✓	$\times$	$\times$	✓
1	2	3	4

and we would assign $\{2,4\}$ the following sequence of ✓'s and $\times$'s:

$\times$	✓	$\times$	✓
1	2	3	4

Each $B \in \mathscr{P}(A)$ gives rise to a sequence of ✓'s and $\times$. We claim:

Picking a subset B of A is the same data as picking a sequence of n checkmarks and $\times$'s

(The idea is that counting the power set is hard, but counting these sequences of ✓'s and $\times$'s is not so bad.)

Now to support our claim:

(1) Distinct B give distinct sequences: if you have $B_1, B_2 \in \mathscr{P}(A)$ with $B_1 \neq B_2$ then, after potentially relabeling, there is an element $a_i \in A$ such that $a_i \in B_1$ and $a \notin B_2$. Then in their corresponding sequences, one will have a ✓ and one will have a $\times$ in the spot above a_i, so they can't be the same.

(2) Every sequence of ✓'s and ×'s arises in this way: take any sequence $s_1, s_2, \ldots, s_n$ with each $s_i = ✓$ or $\times$. Then construct the set:

$$B = \{a \in A : a = a_i, \text{ with } s_i = ✓\}$$

then the sequence associated to B is the original $s_1, s_2, \ldots, s_n$. For example, if $A = \{1, 2, 3, 4\}$ and the sequence is $✓, \times, ✓, \times$, the above construction would yield $B = \{1, 3\}$.

Hence, counting the number of subsets of A is precisely the same thing as counting sequences $s_1, s_2, \ldots, s_n$, where each s_i is allowed to be a ✓ or a $\times$. Thus:

$$\begin{aligned} |\mathscr{P}(A)| &= \#\text{ of subsets of } A \\ &= \#\text{ of sequences } s_1, \ldots, s_n \text{ where each } s_i = ✓ \text{ or } \times \\ &= 2^n && \text{(2 options for each of the } s_i\text{)} \\ &= 2^{|A|} && \text{(since } |A| = n\text{)} \end{aligned}$$

And we are done.

Proof 2 (Proof 1 but with more formal notation)

Note that if you have a set S, then:

$$S^2 = S \times S = \{(s_1, s_2) : \text{ each } s_i \in S\}$$

That is, the elements of $S^2 = S \times S$ look like pairs (s_1, s_2) with each entry s_i in S. Likewise:

$$S^n = \underbrace{S \times \cdots \times S}_{n \text{ times}} = \{(s_1, \ldots, s_n) : \text{ each } s_i \in S\}$$

That is, elements of S^n look like sequences $(s_1, \ldots, s_n)$ with each entry s_i in S. Lastly, note that from our observation that $|S \times T| = |S| \times |T|$, we have:

$$|S^n| = |S|^n$$

Now, we begin the proof. Again we have $A = \{a_1, \ldots, a_n\}$ so that $|A| = n$. Observe that we have a map:

$$\begin{aligned} f : \mathscr{P}(A) &\to \{✓, \times\}^n \\ B &\mapsto (\delta_1(B), \ldots, \delta_{|A|}(B)) \end{aligned}$$

where $\delta_i(B)$ is ✓ if B includes a_i, and $\times$ if it doesn't.

f is a bijection. Property (1) from Proof 1 is the same as f being injective. Property (2) from Proof 1 is the same as f being surjective. Since f is a bijection, the size of the domain and codomain have the be the same. Therefore:

$$\begin{aligned} |\mathscr{P}(A)| = |\{✓, \times\}^n| &= |\{✓, \times\}|^n \\ &= 2^n \\ &= 2^{|A|} && \text{(since } n = |A|\text{)} \end{aligned}$$

32. April 1 (Combinatorics 5/ Number theory 1)

One last formula to know: the number of ways to pick k objects from n when repeats are allowed. This is the same as placing k balls into n buckets.

For example. if you are picking 3 objects from 3 objects A, B, C with repeats allowed (i.e. placing 3 balls into buckets labeled A, B, C, you have 10 options.

$$AAA, BBB, CCC, AAB, AAC, BBA, BBC, CCA, CCB, ABC$$

We would like to find a general formula.

We can envision putting the balls into buckets as using two dividers to create the three buckets:

$$(A \text{ bucket})\big|(B \text{ bucket})\big|(C \text{ bucket})$$

And then draw three circles. Their placement determines what bucket they're in. For example, AAB corresponds to two balls in the A bucket and one ball in the B bucket:

$$\circ\circ\,\big|\,\circ\,\big|$$

And ACC corresponds to the picture:

$$\circ\big|\;\;\big|\,\circ\circ$$

Note that there are $3-1$ dividers being drawn and 3 balls being drawn, so $(3-1)+3$ symbols have to be drawn in total.

We can think about the general idea similarly. **Suppose you're trying to put k balls into n buckets. Similar to our previous discussion, the number of ways to do this is the number of ways to draw k balls and $n-1$ dividers.**

This requires us to draw $n-1$ dividers and then k balls, so $n-1+k$ symbols in total. If we think about having $n-1+k$ slots to draw a symbol:

$$\underbrace{\_\quad\_\quad\cdots\quad\_\quad\_}_{n-1+k \text{ slots}}$$

After you fill in the $n-1$ dividers, the rest of the slots have to be taken up by balls. So drawing one of these diagrams corresponds to a choice of $n-1$ of the slots from $n-1+k$ slots. This is $\binom{n-1+k}{n-1}$. So we get:

$$\begin{aligned}
&\#\text{ ways to pick } k \text{ objects from } n \text{ objects with repeats allowed}\\
&\quad= \#\text{ of ways to put } k \text{ balls in } n \text{ buckets}\\
&\quad= \#\text{ ways to draw } k \text{ balls and } n-1 \text{ dividers}\\
&\quad= \binom{n-1+k}{n-1}\\
&\quad= \binom{n-1+k}{k} && \text{(by symmetry of Pascal's triangle)}
\end{aligned}$$

Now, to return to number theory (roughly, an area of math that concerns itself with equations and fundamental facts about $\mathbb{Z}, \mathbb{Q}$). We want to talk about gcds, divisibility, primes, and how it connects to this $\mod m$ equivalence relation. First things first: Euclid's algorithm. Which is the following...

Say we talk $a = 97$ and $b = 20$. We successively perform the division algorithm, and after each row we shift so that the number playing the role of b plays the role of a, and the remainder becomes the number playing the role of b.

$$\begin{aligned}
97 &= 20 \cdot 4 + 17\\
20 &= 17 \cdot 1 + 3\\
17 &= 3 \cdot 5 + 2\\
3 &= 2 \cdot 1 + 1\\
2 &= 1 \cdot 1 + 0
\end{aligned}$$

When we hit zero, we are done and can't go further. One thing to notice: what is $\gcd(a, b)$? What is the last nonzero remainder? It's 1. It's also true that $\gcd(97, 20) = 1$.

Let's try it again with $a = 765$ (which is $3^2 \cdot 5 \cdot 17$) and $b = 231$ (which is $3 \cdot 7 \cdot 11$).

$$\begin{aligned} 765 &= 231 \cdot 3 + 72 \\ 231 &= 72 \cdot 3 + 15 \\ 72 &= 15 \cdot 4 + 12 \\ 15 &= 12 \cdot 1 + 3 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

Again, last nonzero remainder is 3, and $\gcd(765, 231) = 3$.

Let's try it again with $a = 651 = 3 \times 7 \times 31$ and $b = 399 = 3 \times 7 \times 19$.

$$\begin{aligned} 651 &= 399 \cdot 1 + 252 \\ 399 &= 252 \cdot 1 + 147 \\ 252 &= 147 \cdot 1 + 105 \\ 147 &= 105 \cdot 1 + 42 \\ 105 &= 42 \cdot 2 + 21 \\ 42 &= 21 \cdot 2 + 0 \end{aligned}$$

Again, the last nonzero remainder is 21 and $\gcd(651, 399) = 21$. So it seems that we can use Euclid's algorithm to find the gcd. This is great, because when you find the gcd of two small numbers like 30 and 12, you factor them and see what prime factors they share.

$$\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 \\ 12 &= 2^2 \cdot 3 \end{aligned}$$

So we get $\gcd(12, 30) = 6$. This is fine for small numbers, but if you're working with big ones: factoring is *extremely hard*, and computationally taxing. But Euclid's algorithm can produce the gcd without factoring! (It also gives us some useful other info, as we see later). We'll see why it works next class.

Written out generally, Euclid's algorithm starts with a, b, and then you successively divide.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

Here we have the $\vdots$ becaue it's not immediately clear that the algorithm always has to terminate! We will also prove this later on.

33. April 3 (Number theory 2)

We resume our discussion of Euclid's algorithm. Let's talk about some of our upcoming goals a little more concretely.

- We want to study primes and divisibility and GCD's: all important notions when it comes to integers.
- To that end, we want to prove that Euclid's algorithm works: the algorithm terminates, and it computes the GCD (particularly, the last nonzero remainder is the GCD of the two inputs)

- We will show a nice consequence of Euclid's algorithm: $\gcd(a, b)$ can be written as a *linear combination* of the inputs a, b.
- We'll use this to prove Euclid's lemma, which is an incredibly important fact about primes.
- Ultimately, we'll use this to show the **fundamental theorem of arithmetic**, which says that any natural number can be factored into a *unique* product of primes.

We begin with a warmup: performing Euclid's algorithm for $a = 122$ and $b = 23$. Note that $\gcd(122, 23) = 1$ since 23 is prime and does not divide 122.

$$\begin{aligned} 122 &= 23 \cdot 5 + 7 \\ 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Once we get zero as a remainder, we stop the process.

Why does Euclid's algorithm work? That is, why does the last nonzero remainder in the algorithm equal the GCD of the two inputs? Well, before we think about that we need to check something: that the algorithm ends!

Let's look at Euclid's algorithm in general, using variables so that we can study the general process.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

We use $\vdots$ because, just from the definition we gave last time, it's not clear that the process ends! We need to check that we eventually get some $r_n = 0$. Let's look at our example above with $a = 122$ and $b = 23$. Note that the remainders are strictly decreasing. That is, it seems like $r_1 > r_2 > \dots$. This observation will prove useful.

Theorem 33.1. *Euclid's algorithm always terminates.*

Proof. Say we perform Euclid's algorithm on some inputs:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

We'll use (a slight variant of) the least number principle: if $S \subseteq \mathbb{N} \cup \{0\}$ and $S \neq \varnothing$, then S has a smallest element.

So let's take the set

$$R = \{r_1, r_2, \dots\} = \text{ set of all remainders that appear above}$$

We would be done if we can show $0 \in R$. Note that certainly $r_1 \in R$, so $R \neq \varnothing$. And, by construction, $R \subseteq \mathbb{N} \cup \{0\}$. Hence R has a least element. Call it r_k.

If $r_k = 0$, we're done. If $r_k > 0$, then we can perform the next step of the algorithm:

$$\begin{aligned} r_{k-2} &= r_{k-1} q_k + r_k \\ r_{k-1} &= r_k q_{k+1} + r_{k+1} \end{aligned}$$

The inequality property of the division algorithm tells us $0 \leq r_{k+1} < r_k$. But this contradicts r_k being the smallest element of R. So it must be that $r_k = 0$. So we have guaranteed that the algorithm ends. □

Corollary 33.2. *The remainders of Euclid's algorithm decrease to zero. That is, you get*

$$r_1 > r_2 > \cdots > r_k = 0$$

for some $k \in \mathbb{N}$. (The k will vary depending on the inputs a, b).

We can now show that Euclid's algorithm "works." We will need a result from the homework, namely Homework 3 Extra Credit 2:

Lemma 33.3. *If $a = bq + r$ with $a, b, q, r \in \mathbb{Z}$ with $a, b \neq 0$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let $C = \gcd(a, b)$ and $D = \gcd(b, r)$. Now, rearranging the equation $a = bq + r$, we get that:

$$r = a - bq$$

We claim that any integer x that divides a and b also divides r. If x divides a and b, then $a = x \cdot k_1$ and $b = x \cdot k_2$ for $k_1, k_2 \in \mathbb{Z}$. Then

$$r = a - bq = xk_1 - bxk_2 = x(k_1 - bk_2).$$

So x divides r, which is what we wanted. Now, by definition, C divides a and b. So it must divide r. Since C is therefore a common divisor of b and r, we have $C \leq D$.

Now, since $a = bq + r$, a similar argument shows that any integer that divides b and r also divides a (we could factor a copy out of it from b, r and then use the distributive property to pull it out to the front). Since D divides both b and r, we therefore get that D divides a. Since D divides both a and b, it must be that $D \leq C$.

Then we have $C \leq D$ and $D \leq C$. Given these inequalities, it must be that $C = D$. So $\gcd(a, b) = \gcd(b, r)$ and we are done. □

Theorem 33.4. *When performing Euclid's algorithm with inputs a and b, the last nonzero remainder is $\gcd(a, b)$.*

Proof. Now that we know the algorithm ends, we can write the general form for the algorithm as:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{k-1} &= r_k q_{k+1} + r_{k+1} \\ r_k &= r_{k+1} q_{k+2} + 0 \end{aligned}$$

We want to show that $r_{k+1} = \gcd(a, b)$. Applying the lemma to each row, we get a nice chain of equalities:

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_k, r_{k+1}) = \gcd(r_{k+1}, 0)$$

Note that $\gcd(n, 0) = n$ for any natural number n. So:

$$\gcd(a, b) = \gcd(r_{k+1}, 0) = r_{k+1}$$

and we are done. □

So: Euclid's algorithm computes the gcd! This is already quite useful. It has another great usage, which we'll see next time.

34. April 5 (Number theory 3)

Last time, we saw that Euclid's algorithm computes the gcd of the inputs. It also helps with the following theorem.

Theorem 34.1. *Let $a, b \in \mathbb{Z}$, and let $d = \gcd(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that:*

$$d = ax + by$$

That is, d can be expressed as a linear combination (with integer coefficients) of a and b.

On your homework, you'll see that the gcd is the only common divisor of a, b with this property.

Let's do an example of how Euclid's algorithm can help us with this. Let's remember our computation from last time:

$$\begin{aligned} 122 &= 23 \cdot 5 + 7 \\ 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Our goal is to write $\gcd(122, 23) = 1$, the last nonzero remainder, as a linear combination of $122, 23$. Let's aim for something a little easier: let's just try to write the first remainder as a linear combo of $122, 23$. Rearranging the first equation:

$$7 = 122 - 23 \cdot 5$$

Let's try to get the second remainder, 2, as a linear combination of 122 and 23. Well, let's try getting it to just be a linear combo of 23 and 7.

$$2 = 23 + 7(-3)$$

We have a 23 there, which is fine. The 7 is not so great, but 7 can be written as a linear combo of 122 and 23, so let's try substituting that in.

$$\begin{aligned} 2 &= 23 + 7(-3) = 23 + (122 - 23 \cdot 5)(-3) \\ &= 23 + 122(-3) + 23(15) \\ &= 23(16) + 122(-3) \end{aligned}$$

So we've gotten the second remainder as a linear combo of $23, 122$! This is good progress, if we can repeat this process we can get the least nonzero remainder. Again we have...

$$\begin{aligned} 1 &= 7 + 2(-3) \\ &= (122 + 23(-5)) + (23(16) + 122(-3))(-3) \\ &= 122(1) + 23(-5) + 23(-48) + 122(9) \\ &= 122(10) + 23(-53) \end{aligned}$$

So we get a *recursive* process where we're using that you can write previous remainders as linear combos of a, b to get the next remainder is a linear combo of a, b. This is the sort of argument that should scream: induction! Specifically, strong induction.

We will omit the proof of the theorem, since it is basically the same process but with variables and is not that insightful. **You may use the result of Theorem 34.1 on homeworks and the final exam.**

Note: you can find an alternate proof in Hamkins. It's shorter than the induction proof and has a nice consequence (the GCD is the smallest natural number that can be written as $ax + by$), but it doesn't tell you how you should go about finding the x, y

An immediate corollary of the theorem we proved last time is...

Corollary 34.2. *If* $\gcd(a, b) = 1$*, then there exists* $x, y \in \mathbb{Z}$ *such that*

$$1 = ax + by$$

This allows us to prove an incredibly useful lemma:

Theorem 34.3 (Euclid's lemma)**.** *Let* p *be a prime number, and* $a, b \in \mathbb{Z}$*. If* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

(Note that this is not true for a general integer! $4 \nmid 2 \cdot 6$, but $4 \nmid, 4 \nmid 6$. In fact, this property characterizes primes: we will prove the converse on HW.)

Proof. Let p be a prime, and a, b, integers such that $p \mid ab$. If $p \mid a$, then we are done! If not, then $\gcd(p, a) = 1$, because p only has two (positive) factors: p and 1.

Then, by the corollary:

$$1 = px + ay$$

Multiplying by b:

$$b = px + aby$$

Recall that $p \mid ab$, so $ab = pk$ for some $k \in \mathbb{Z}$. (To motivate this step: we haven't used $p \mid ab$ yet, and we have an ab in our equation, and there's not much else we can do).

$$b = px + pky = p(x + ky)$$

So, $p \mid b$ and we are done. □

Corollary 34.4. *If* $p \mid a_1 a_2 \dots a_n$*, then* $p \mid a_i$ *for some* a_i*.*

Do note: Euclid's lemma is the crux of the proof of unique factorization! We already proved that any natural number can be factored into primes. But it's not clear that it's unique.

35. April 8 (Number theory 4)

We can write $12 = 2 \cdot 2 \cdot 3$, but what if there were some other combination of primes that could yield it? We would like to be able to guarantee this **can't** happen (for *any* integer). That is, we want to know that prime factorizations are unique.

Theorem 35.1 (Fundamental theorem of arithmetic)**.** *Let* n *be a natural number. Then* n *factors uniquely into primes. That is, if you have two prime factorizations of* n*:*

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

then the q_i *must be a rearrangement of the* p_i *(and consequently,* $k = \ell$*).*

Proof. We proceed via strong induction. Let $P(n)$ be the property that n has unique factorization: if you write

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

then the q_i must be a rearrangement of the p_i. Showing that $P(n)$ is true for all n will prove the theorem.

Base case: We'll show $P(1)$ is true. The only way to factor 1 is to write it as the product of no primes, so it has a unique factorization. [1]

[1] It might be odd to think of a product of no terms. But, much like how an "empty" sigma notation like

$$\sum_{i=0}^{-1} a_i$$

should be zero, an "empty" product ends up being 1. Handling the base case is largely boils down to technicalities.

Inductive step: Suppose we know $P(k)$ is true for $1 \leq k < n$. We want to show $P(n)$ is true. Suppose we have two factorizations of n:

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

In order to show $P(n)$ is true, we need to show that the two factorizations are just rearrangements of eachother. Consider p_1. By Corollary 34.4, p_1 must divide some q_i. But q_i is prime, so its only positive factors are 1 and q_i. Certainly $p_1 \neq 1$, so it must be that $p_1 = q_i$. Then I can cancel $p_1 = q_i$ from each side:

$$\frac{n}{p_1} = p_2 \dots p_k = q_1 \dots q_{i-1} q_{i+1} \dots q_\ell$$

Note that n/p_1 is an integer, and that $n/p_1 < n$, so $P(n/p_1)$ is true. Therefore, it must be that:

$$p_2, \dots, p_k \text{ is a rearrangement of } q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_\ell$$

so when we add back in $p_1 = q_i$, we still get that the p_j are just rearrangements of the q_j.

$$p_1, p_2, \dots, p_k \text{ is a rearrangement of } q_1, \dots, q_\ell$$

And therefore, $P(n)$ is true.

Since we've shown the base case and the inductive step, strong induction tells us that $P(n)$ is true for all n. Thus we are done. □

Next, let's look at some consequences of this theorem. All prime factorizations of a number are just rearrangements of eachother, and we can "standardize" the arrangement:

Corollary 35.2. *Suppose you factor a natural number n as*

$$n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_k}$$

with $p_1 < p_2 < \dots < p_k$ and $e_i \geq 1$ for $1 \leq i \leq k$. Then this expression is unique, in the sense that if you have

$$n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_k} = q_1^{f_1} q_2^{f_2} \dots q_\ell^{f_\ell}$$

with $p_1 < \dots < p_k$ and $q_1 < \dots < q_\ell$ and the $e_i, f_i \geq 1$, then:

$$k = \ell \qquad \text{(the lengths are the same)}$$
$$p_i = q_i \text{ for } 1 \leq i \leq k = \ell \qquad \text{(the primes are the same)}$$
$$e_i = f_i \text{ for } 1 \leq i \leq k = \ell \qquad \text{(the exponents are the same)}$$

Proposition 35.3. *Let p be a prime. Then $\sqrt{p}$ is irrational.*

Proof. Suppose, for the sake of contradiction, that $\sqrt{p}$ is rational. Then write $\sqrt{p} = \frac{a}{b}$. Then $p = \frac{a^2}{b^2}$ and so:

$$pb^2 = a^2$$

If $a = p_1^{e_1} \dots p_n^{e_n}$ with $p_1 < \dots < p_n$, and the $e_i \geq 1$, then we see that $a^2 = p_1^{2e_1} \dots p_n^{2e_n}$. That is, in the (standardized) prime factorization of a square number, the exponents are all even. So the exponent of p on the right-hand side is even. But, similarly, the exponent of p on the left-hand side is odd. Unique factorization says:

$$\text{exponent of } p \text{ on the LHS} = \text{exponent of } p \text{ on the RHS}$$

But then we would have an odd number equaling an even number, which is impossible. So our assumption is false, and $\sqrt{p}$ is irrational. [2] □

[2]Note that you didn't need $\frac{a}{b}$ to be in least terms in this proof.

36. April 10 (Number theory 5: Modular Arithmetic 1)

Today we shift focus to equivalence mod m. We've been exploring this on HW, and it goes hand-in-hand with some previous material. Some motivation:

- Good for studying divisibility. (Recall that $5 \mid n \iff n \equiv 0 \mod 5$. Recall that it was much easier to show $n^5 - n$ is always a multiple of 5 by plugging in $n \equiv 0, 1, 2, 3, 4 \mod 5$ and studying $n^5 - n \mod 5$, rather than trying to look at $(5k + r)$ for $r = 0, 1, 2, 3, 4$ and trying to raise that expression to the fifth power).
- Useful for other facts about integers too (gives an easy way to show that 75739568163 is not a square, for example).
- Data encryption, namely RSA cryptography
- Naturally shortens some algorithms/code

Let's go back to our example of equivalence mod 5 from homework:

- Recall that:

$$\begin{aligned} x \equiv y \pmod 5 &\iff x = y + 5k, \text{ for some } k \in \mathbb{Z} \\ &\iff x, y \text{ have the same remainder when divided by 5} \end{aligned}$$

- If $a \equiv b$, $c \equiv d \pmod 5$ then we get

$$a + c \equiv b + d \pmod 5, \quad ac \equiv bd \pmod 5$$

  e.g., since $1 \equiv 6, 2 \equiv 7 \pmod 5$ we have

$$1 + 2 \equiv 6 + 7 \pmod 5, \quad 1 \cdot 2 \equiv 6 \cdot 7 \pmod 5$$

  and if you have $n \equiv 2 \mod 5$, then:

$$n^5 - n \equiv 2^5 - 2 \equiv 32 - 2 \equiv 30 \equiv 0 \pmod 5$$

  So you can swap a number for anything it's equivalent to in any reasonable equation.
- There are five equivalence classes: $[0], [1], [2], [3], [4]$. So we have the integers $0, 1, 2, 3, 4$, and then when we increment to 5, we loop back around to get $5 \equiv 0, 6 \equiv 1, 7 \equiv 2$ and so on.

Analogously, we can define *equivalence mod m* and similar properties hold.

- We define

$$\begin{aligned} x \equiv y \pmod{\text{m}} &\iff x = y + mk, \text{ for some } k \in \mathbb{Z} \\ &\iff x, y \text{ have the same remainder when divided by } m \end{aligned}$$

- If $a \equiv b$, $c \equiv d \pmod m$ then we get

$$a + c \equiv b + d \pmod m, \quad ac \equiv bd \pmod m$$

  So you can swap a number for anything it's equivalent to in any reasonable equation.
- There are m equivalence classes: $[0], [1], \ldots, [m-1]$. So we have the integers $0, 1, \ldots, m-1$, and then when we increment to m, we loop back around: $m \equiv 0,\ m+1 \equiv 1,\ m+2 \equiv 2, \ldots$. $(\mod m)$.

When dealing with equivalence mod m, you should think of this as "treating m like it's zero" For example: suppose we're working with equivalence mod 5. Then note that $13 = 2 \cdot 5 + 3$. Since we are treating 5 like it's zero, $13 \equiv 2 \cdot 5 + 3 \equiv 2 \cdot 0 + 3 \equiv 3 \ (\mod 5)$.

Let's get some examples of computing in mod m when m isn't 5. It's common to work with m a prime, though mathematicians also consider cases where m is composite.

Let's consider equivalence mod 7. First, here's an example

$$11 \equiv 4 \pmod 7$$

because $11 = 7 + 4$, and we are "treating 7 like it's zero." (This equivalence can also be seen from the definition). Likewise:

$$29 \equiv 4 \cdot 7 + 1 \equiv 2 \pmod 7$$

Here's another example. Suppose we have $17 \cdot 33$. We know that it should be equivalent to one of $0, 1, 2, 3, 4, 5, 6 \pmod 7$. We would like to determine which one. Well, since $17 \equiv 3$ and $33 \equiv 5$ mod 7, we have:

$$17 \cdot 33 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$$

Now let's consider:

- $5 + 9$
- $44 \cdot 75$
- $11 \cdot 2 - 10$
- $(24)^3 - 9^4$

Each of these should be equivalent to one of $0, 1, 2, 3, 4, 5$, or 6 mod 7. We would like to determine which one. We compute:

- $$5 + 9 = 14 = 7 \cdot 2 \equiv 0 \pmod 5$$
- Note that $44 \equiv 2 \pmod 5$ and $75 \equiv 5 \pmod 7$ so:
$$44 \cdot 75 \equiv 2 \cdot 5 \equiv 10 \equiv 3 \pmod 7$$
- $$11 \cdot 2 - 10 \equiv 22 - 10 \equiv 12 \equiv 5 \pmod 7$$
- Note that $24 \equiv 3$ and $9 \equiv 2 \pmod 5$ so:
$$(24)^3 - 9^4 \equiv 3^3 - 2^4 \equiv 27 - 16 \equiv 11 \equiv 4 \pmod 7$$
That is, we swapped 24 with something it's equivalent to, and swapped 9 for something it's equivalent to. These swaps made it easier to compute.

We end with one more observation:

- Note that $2! \equiv 2 \pmod 3$
- Note that $4! \equiv 24 \equiv 4 \pmod 5$
- Now we consider $6! \pmod 7$. Then:
$$\begin{aligned} 6! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \\ &\equiv 4 \cdot 5 \cdot 6^2 \\ &\equiv 4 \cdot 5 \cdot (-1)^2 \\ &\equiv 20 \\ &\equiv 6 \pmod 7 \end{aligned}$$
- Now we consider $10! \bmod 11$. Then one can compute:
$$\begin{aligned} 10! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &\equiv 10 \pmod{11} \end{aligned}$$

We observe the following pattern: for primes p, we have

$$(p-1)! \equiv p-1 \pmod{p}$$

or equivalently:

$$(p-1)! \equiv -1 \pmod{p}$$

This is called *Wilson's theorem*, and we will prove it in the next class (or two).

37. April 12 (Number theory 6: Modular Arithmetic 2)

Today, we're investigating *invertability* mod m.

Definition 37.1. Let $m \in \mathbb{N}$ and $b \in \mathbb{Z}$. We say that b *is invertible mod* m if there exists some $c \in \mathbb{Z}$ such that

$$bc \equiv 1 \pmod{\text{m}}$$

This equation is meant to parallel something like $2 \cdot \frac{1}{2} = 1$ in $\mathbb{Q}$. Normally one cannot invert the number 2 while staying in the integers, but in modular arithmetic, we have things like $2 \cdot 3 \equiv 1 \pmod{5}$.

The first reason why we care about invertability: it tells us a lot about what equations we can and can't solve mod m. For example if we are trying to solve:

$$\text{Does there exist } x \text{ such that } 2x^2 \equiv 1 \pmod{5}?$$

We would want to multiply 2 by its inverse, 3 on both sides to get the equation $6x^2 \equiv x^2 \equiv 3 \pmod{5}$ and then try to see if there is some square number x^2 equivalent to 3. [3] **Such equations come up a lot in math and coding.**

The second motivation for why we care about invertability: Invertible and non-invertible elements behave very differently. To motivate, consider -1 and 0 in $\mathbb{Z}$. -1 has a multiplicative inverse in $\mathbb{Z}$, and 0 does not. Multiplication by -1 gives a bijection:

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto (-1) \cdot x \end{aligned}$$

but multiplication by 0 does not give a bijection:

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z} \\ x &\mapsto 0 \cdot x = 0 \end{aligned}$$

Now let's give an example of these different behaviors in modular arithmetic. Let's work with equivalence mod 4. Note that 3 is invertible mod 4 as $3 \cdot 3 \equiv 9 \equiv 1 \pmod{4}$. Note that 2 is *not* invertible mod 4, because $2n \equiv 0$ or $2 \pmod{4}$ for any integer n.

If we multiply $0, 1, 2, 3$ by 3 we get:

$$\begin{aligned} \mathbf{0} \cdot 3 &\equiv \mathbf{0} \pmod{4} \\ \mathbf{1} \cdot 3 &\equiv \mathbf{3} \pmod{4} \\ \mathbf{2} \cdot 3 \equiv 6 &\equiv \mathbf{2} \pmod{4} \\ \mathbf{3} \cdot 3 \equiv 9 &\equiv \mathbf{1} \pmod{4} \end{aligned}$$

[3] Think of this as an analogue of solving $2x^2 = 1$ by multiplying both sides by $\frac{1}{2}$ to get $x^2 = \frac{1}{2}$ and then square-rooting.

That is, after multiplying by 3 (and taking the remainder to get a number in $\{0,1,2,3\}$), we see that we've shuffled the numbers $\{0,1,2,3\}$ around. That is, we got a bijection $\{0,1,2,3\} \to \{0,1,2,3\}$, which sends $0 \mapsto 0, 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1$. Contrast this with multiplying by 2:

$$0 \cdot 2 \equiv 0 \pmod 4$$
$$1 \cdot 2 \equiv 2 \pmod 4$$
$$2 \cdot 2 \equiv 4 \equiv 0 \pmod 4$$
$$3 \cdot 2 \equiv 6 \equiv 2 \pmod 4$$

This process doesn't shuffle the numbers $\{0,1,2,3\}$ around. That is, we didn't get a bijection.

So one way we see the difference between invertible and non-invertible elements is getting a bijective map $\{0,1,2,3,\} \to \{0,1,2,3\}$ and getting a non-bijective map $\{0,1,2,3\} \to \{0,1,2,3\}$. We really like bijections, so this is a pretty important split in behavior!.

Equivalently, we can take the equivalence classes $[0],[1],[2],[3]$ and say:

$$\{[0],[1],[2],[3]\} \to \{[0],[1],[2],[3]\}$$
$$[x] \mapsto [3x]$$

is a bijection while

$$\{[0],[1],[2],[3]\} \to \{[0],[1],[2],[3]\}$$
$$[x] \mapsto [2x]$$

is not a bijection.

One place where we would really care about this: data encryption! Hence:

The third reason we care: shortens some algorithms/functions in CS, beginnings of data encryption. Let's work with equivalence mod 26. We've got 26 equivalence classes, corresponding to $0,1,2,\ldots,25$. Assign each number sequentially to a letter of the alphabet:

$$0 \leftrightarrow A$$
$$1 \leftrightarrow B$$
$$2 \leftrightarrow C$$
$$\ldots$$
$$25 \leftrightarrow Z$$

Then we can turn a message HELLO into $7,4,11,11,14$. Let's say we are trying to encrypt this message and send it. One way we could do that is to shift every letter up by 3 places to get

$$10,7,14,14,17(= \text{KHOOR})$$

Now a would-be spy wouldn't be able to immediately tell what your message is. And your buddy receiving the message, who knows the "key" is 3, would shift the letters back down by 3. But this is still perhaps a bit easy to guess. Maybe we could try something a little more complicated?

Try multiplying by 5. Then:

$$5 \cdot 10 \equiv 50 \equiv 24 \quad (Y)$$
$$5 \cdot 7 \equiv 35 \equiv 9 \quad (J)$$
$$5 \cdot 14 \equiv 70 \equiv 18 \quad (S)$$
$$5 \cdot 14 \equiv 70 \equiv 18 \quad (S)$$
$$5 \cdot 17 \equiv 85 \equiv 7 \quad (H)$$

and now your encrypted message is $24, 9, 18, 18, 7$ or YJSSH, and is a little harder to decode. But how does your buddy figure out the original message? Well, note that: $5 \cdot (-5) \equiv -25 \equiv 1 \pmod{26}$. So:

$$\begin{aligned} -5(5 \cdot 10) &\equiv (-25)10 \equiv 10 \quad (H) \\ -5(5 \cdot 7) &\equiv (-25)7 \equiv 7 \quad (E) \\ -5(5 \cdot 14) &\equiv (-25)14 \equiv 14 \quad (L) \\ -5(5 \cdot 14) &\equiv (-25)14 \equiv 14 \quad (L) \\ -5(5 \cdot 17) &\equiv (-25)17 \equiv 17 \quad (O) \end{aligned}$$

That is, we can undo the encryption by multiplying by the inverse of 5. That is, we know the output is of the form $5x$ for some x, and we can recover x by doing $-5(5x) \equiv (-25)x \equiv x$. This all comes down to computing the inverse of

$$\begin{aligned} \{0, 1, 2, \ldots, 25\} &\to \{0, 1, 2, \ldots, 25\} \\ x &\mapsto \text{remainder of 5x when divided by 26} \end{aligned}$$

or equivalently

$$\begin{aligned} \{[0], [1], [2] \ldots, [25]\} &\to \{[0], [1], [2], \ldots, [25]\} \\ [x] &\mapsto [5x] \end{aligned}$$

Note that if we tried to multiply by 13 (which is *not* invertible mod 26), this encryption would go poorly! Because:

$$\begin{aligned} 13 \cdot 0 &\equiv 0 \pmod{26} \\ 13 \cdot 1 &\equiv 13 \\ 13 \cdot 2 &\equiv 0 \\ 13 \cdot 3 &\equiv 13 \\ 13 \cdot 4 &\equiv 0 \\ &\vdots \end{aligned}$$

So if you had a 0 (which is A) in your would-be encrypted message, you would have no clue if that corresponded to an A or a C or a E (or G, or I, etc) in the original non-encrypted message! So multiplying by the non-invertible element 13 is not a good way to encrypt.

So, this sufficiently motivates wanting to study invertible elements. How do we determine if an element is invertible at all? Well...

Proposition 37.2. *Let $m \in \mathbb{N}, b \in \mathbb{Z}$. Then b is invertible mod m if and only if* $\gcd(b, m) = 1$.

Proof.

- Part 1 ($\Rightarrow$): If b is invertible, then there exists $c \in \mathbb{Z}$ such that $bc \equiv 1 \bmod m$. Then by definition of equivalence mod m, this means there exists $k \in \mathbb{Z}$ such that:

  $$1 = bc + mk$$

  Then $\gcd(b, m)$ divides b and m, so it divides bc and mk, and thus divides $bc + mk = 1$. But then $\gcd(b, m) \mid 1$, which can only happen if $\gcd(b, m) = 1$.

- Part 2 ($\Leftarrow$): if $\gcd(b, m) = 1$, then previous results (namely Theorem 34.1) tell us that there exists $x, y \in \mathbb{Z}$ such that $1 = bx + my$. Then $bx \equiv 1 \bmod m$ by definition. So b is invertible.

□

This proposition also gives another motivation: invertability is tied to division properties. The proposition above says that b is invertible mod m if and only if b, m don't share any prime factors.

Another fun fact: you can take powers of b to eventually get 1.

Proposition 37.3. *Suppose b is invertible mod m. Then there exists $n \in \mathbb{N}$ such that $b^n \equiv 1$ mod m.*

Proof. To be proven next class. □

38. April 15 (Number theory 7: Modular Arithmetic 3)

Today: we're talking about invertibility. From last time: recall the definition of invertible (there exists c such that $bc \equiv 1 \pmod{m}$), and that b is invertible mod m if and only if $\gcd(b, m) = 1$.

One tip worth noting: In the proof of $\gcd(b, m) = 1$ implies b invertible: you use that there exists $x, y \in \mathbb{Z}$ such that

$$bx + my = 1$$

then by definition, $bx \equiv 1 \pmod{m}$. Note that we found these x, y from the substituting process for Euclid's algorithm covered on April 5th. So this substituting technique is one way to find the inverse.

We will begin by doing the proof of Proposition 37.3. That is, we will show that if you fix $b \in \mathbb{Z}, m \in \mathbb{N}$ with b invertible mod m, then there exists $n \in \mathbb{N}$ such that $b^n \equiv 1 \pmod{m}$. Note that $b \cdot b^{n-1} \equiv 1$ in this case, and so we see that the inverse of b can (eventually) be found by taking powers of b.

Proof. We are working mod m, so there are m equivalence classes: $[0], [1], \ldots, [m-1]$. Consider the map:

$$\begin{aligned} f : \mathbb{N} &\to \{[0], [1], \ldots, [m-1]\} \\ n &\mapsto [b^n] \end{aligned}$$

You can think of this as taking powers of b (so taking the b^n) and then seeing which of $0, 1, 2, \ldots, m-1$ they are equivalent to.[4] Now, we've proven that you can't have an injection to a smaller set.[5] We proved this for finite sets, but since $\mathbb{N}$ contains finite sets with more elements than $\{[0], \ldots, [m-1]\}$, certainly f cannot be injective!

So, there exists $n_1, n_2 \in \mathbb{N}$ with $n_1 \neq n_2$ such that $f(n_1) = f(n_2)$. This means:

$$[b^{n_1}] = [b^{n_2}]$$

Which, by definition of equivalence class, means

$$b^{n_1} \equiv b^{n_2} \pmod{m}$$

Now, n_1, n_2 aren't equal, so we can assume one of them is bigger. Let's say $n_2 > n_1$ (swap the labeling of n_1, n_2 otherwise). Then by exponent rules:

$$b^{n_1} \equiv b^{n_2 - n_1} b^{n_1} \pmod{m}$$

[4] If you don't like the notation of this map, you could write it as $g : \mathbb{N} \to \{0, 1, \ldots, m-1\}$ defined by $n \mapsto b^n$ (and take the remainder of b^n mod m as needed to get something in $0, 1, 2, \ldots, m-1$.)

[5] This is basically a variant of the Pigeonhole Principle, which says that if you try to put $n+1$ pigeons (or any k pigeons with $k > n$) into n holes, then two of the pigeons must go to the same hole. If you think of putting pigeons into holes of a coop as akin to a function assigning elements of the domain to elements of the codomain, this is the same as saying you can't have an injective function from one finite set to a smaller finite set.

Since b is invertible, there is a $c \in \mathbb{Z}$ such that $bc \equiv 1 \bmod m$. That is, multiplying by c "cancels" a factor of b. Now, here's a bit of motivation: if you were given the equation (in $\mathbb{R}$) that $x^5 = x^3$ and knew $x \neq 0$ you could multiply by x^{-1} on each side three times to get $x^2 = 1$. Similarly, we will work to cancel some copies of b from this equation. We'll multiply by c^{n_1} on both sides to cancel n_1 copies of b.

$$\begin{aligned} c^{n_1}b^{n_1} &\equiv b^{n_2-n_1}b^{n_1}c^{n_1} \pmod m \\ (bc)^{n_1} &\equiv b^{n_2-n_1}(bc)^{n_1} \\ 1 &\equiv b^{n_2-n_1} \end{aligned}$$

This is getting close to what we want! We just need to guarantee that the exponent is a natural number. Certainly $n_2 - n_1 \in \mathbb{Z}$, and since $n_2 > n_1$, we know $n_2 - n_1 > 0$. Therefore, $n_2 - n_1 \in \mathbb{N}$. So, we've achieved the goal of the Proposition. □

Next, let's shift our focus to primes. Recall that a big goal of ours was to prove Wilson's theorem:

$$(p-1)! \equiv -1 \pmod p$$

Expand the left term out: we want to investigate:

$$(p_1)! \equiv 1(p-1)(p-2)\dots 2 \cdot 1$$

So we get the product of all $1 \leq i \leq p-1$. Note that each i in this range is invertible.

Lemma 38.1. *For $1 \leq i \leq p-1$, i is invertible. (Thus: if $b \not\equiv 0 \pmod p$ then b is invertible mod p).*

Proof. Let i be in the range $1 \leq i \leq p-1$. Note that $\gcd(i,p)$ has to be 1 or p, and it can't be p because $p \nmid i$ (because $1 \leq i \leq p-1$). So $\gcd(i,p) = 1$, and thus i is invertible mod p. □

Any b falls into one of the equivalence classes $0, 1, 2, \dots, p-1$ and we know all but the first one contain invertible elements. So we then get $(p_1)! \equiv 1(p-1)(p-2)\dots 2 \cdot 1$ is the "product of the invertible elements". This suggests that we need to understand invertible elements really well. Looking at $(p-1)!$, we don't have any ideas for showing it's equivalent to -1, so that suggests we need to work on understanding invertible elements better.

Note: if b is invertible mod m, then its inverse is unique "up to mod m." Let's elaborate on that: let's work with mod 5, and look at 2. There are multiple numbers that fulfill the role of inverse. For example, observe:

$$2 \cdot -2 \equiv 2 \cdot 3 \equiv 2 \cdot 8 \equiv 2 \cdot 13 \equiv 1 \bmod 5$$

$-2, 3, 8, 13$, etc aren't the same integer, but they do satisfy:

$$-2 \equiv 3 \equiv 8 \equiv 13 \bmod 5$$

Proposition 38.2. *Let $m \in \mathbb{N}$ and $b \in \mathbb{Z}$ so that b is invertible mod m. Then the inverse of b is "unique mod m" in the sense that if $bc_1 \equiv bc_2 \equiv 1 \pmod m$, then $c_1 \equiv c_2 \pmod m$.*

Proof. If $bc_1 \equiv bc_2 \equiv 1 \pmod m$ then multiplying by c_1 yields:

$$\begin{aligned} c_1(bc_1) &\equiv c_1(bc_2) \pmod m \\ (c_1b)c_1 &\equiv (c_1b)c_2 \\ c_1 &\equiv c_2 \qquad (\text{ since } bc_1 \equiv 1) \end{aligned}$$

Thus we are done. [6] □

[6] A tip to note: lots of basic/foundational proofs about invertibility tend to involve just multiplying some equation by the inverse to cancel some factors and get what you want. There aren't a ton of moves you can do in these proofs.

In general, we'll use things like b^{-1} to refer to any number such that $b \cdot b^{-1} \equiv 1 \pmod{m}$

The above proposition means that the map

$$g : \{[1], [2], \ldots, [p-1]\} \to \{[1], [2], \ldots, [p-1]$$
$$[x] \mapsto [x^{-1}]$$

is well-defined, i.e. it's not trying to send $[x]$ to multiple equivalence classes.

Let's compute an example of this map. Let's work mod 7, and find the inverses of $1, 2, 3, 4, 5, 6$. Note:

$$1 \cdot 1 \equiv 1 \pmod{7}$$
$$2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$$
$$3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$
$$6 \cdot 6 \equiv (-1)(-1) \equiv 1 \pmod{7}$$

So 1 is its own inverse, 6 is its own inverse, 2 and 4 are inverses, and 3 and 5 are inverses. So the function looks like:

$$g : \{[1], [2], [3], [4], [5], [6]\} \to \{[1], [2], [3], [4], [5], [6]\}$$
$$[1] \mapsto [1]$$
$$[2] \mapsto [4]$$
$$[3] \mapsto [5]$$
$$[4] \mapsto [2]$$
$$[5] \mapsto [3]$$
$$[6] \mapsto [6]$$

Proposition 38.3. *Let p be a prime, and consider the equivalence classes of the invertible elements, $[1], [2], \ldots, [p-1]$. We have that the function:*

$$g : \{[1], [2], \ldots, [p-1]\} \to \{[1], [2], \ldots, [p-1]\}$$
$$[x] \mapsto [x^{-1}]$$

is a bijection

Proof. As discussed, the function is well-defined (that is, there is no input that goes to multiple outputs). We'll show that this function is an injection to start.

$$\begin{aligned} g([x]) = g([y]) &\iff x^{-1} \equiv y^{-1} (\bmod p) \\ &\iff (xy)x^{-1} \equiv (xy)y^{-1} \\ &\iff (x \cdot x^{-1})y \equiv x(y \cdot y^{-1}) \\ &\iff y \equiv x \\ &\iff [x] = [y] \end{aligned}$$

So the function is injective. We could finish here: an injective function $f : S \to S$ from a finite set to itself must be a bijection. (Otherwise $|f(S)| < |S|$ and then $f : S \to f(S)$ is an injective function from a finite set to a smaller set, which is impossible). However, we'll also do the proof of surjectivity for completeness's sake.

Let $[y] \in \{[1], [2], \ldots, [p-1]\}$. We want to show there is some $[x]$ such that $g([x]) = [y]$. $[y]$ is invertible, so there is some c such that $y \cdot c \equiv 1$. Then $g([c]) = [y]$. □

Next up: We are close to proving Wilson's theorem. We just need to investigate when g sends $[x]$ to itself or to a different equivalence class.

39. April 17

Potentially do surjectivity proof.

- zero product property and how $[x] \mapsto [x^{-1}]$ only has two fixed points.
- Wilson's theorem: pair up inverses in $(p-1)!$. Get two leftover elements.
- $[x] \mapsto [ax]$ examples and examples of a^{p-1}.
- If time, do proof of $a^{p-1} \equiv 1$.
- Spend some time on: if $a \mid c, b \mid c$ then $ab \mid c$. This can be done with UFT, or with $ax + by = 1$, so $axc + byc = 1$. Write $c = ak_1, bk_2$ to get ab in each summand. Hence divisibility mod 12 can be checked mod 4, mod 3.