

MATH 215: CONTINUOUSLY UPDATED NOTES

CONTENTS

1. Jan 8: Syllabus day	2
2. Jan 10: Statements	2
3. Jan 17: Conditionals	2
4. Jan 19: Proof methods part 1 (direct proofs)	3
5. Jan 22: Contradiction, contrapos	4
6. Jan 24: Finish contradiction. Casework	4
7. Jan 26: Induction	5
8. Jan 29: Induction part 2	6
9. Jan 31: Induction, some more examples, strong induction (if time)	7
10. Feb 2: Strong induction	7
11. Feb 5: Division alg, reducing fractions	8
12. Feb 7: (Number theory 1) Division algorithm	8
13. Feb 9 (Number theory 2): Euclid's algorithm	8
14. Feb 12 (Number theory 3):	8
15. Feb 14 (Set theory 1):	9
16. Feb 16 (Set theory 2):	10
17. Feb 19 (Set theory 3):	11
18. Feb 21 (Set theory 4) :	12
19. Feb 23: (Relations)	13
20. Feb 26: Exam review	14
21. Feb 28: N/A due to exam	14
22. March 1 (Relations)	14
23. March 4 (Equivalence classes)	14
24. March 6	14
25. March 8	14
26. March 11	14
27. March 13	15
28. March 15	15
29. March 25	15
30. March 27	15
31. March 29	15
32. April 1	15
33. April 3	15
34. April 5	15
35. April 8	15
36. April 10	16
37. April 12	16
38. April 15	16
39. April 17	16
40. April 19	16
41. April 22	16
42. April 24	16

43. April 26: Review for final exam

16

Below are continuously updated notes for Math 215.

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	$\neg P$	P	Q	$P \vee Q$	P	Q	$P \wedge Q$
T	F	T	T	T	T	T	T
T	F	T	F	T	T	F	F
F	T	F	T	T	F	T	F
		F	F	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 each other (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 $P \Rightarrow Q, Q \Rightarrow P$.

4. JAN 19: PROOF METHODS PART 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. \square

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: CONTRADICTION, CONTRAPOS

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. \square

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:

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

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. \square

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: $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k}$ is never an integer).

6. JAN 24: FINISH 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. \square

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

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

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

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

$$1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$$

for all natural numbers n

- Show that

$$\sum_{k=1}^n k(k+1) = (1 \times 2) + (2 \times 3) + (3 \times 4) + \dots + (n \times (n+1)) = \frac{n(n+1)(n+2)}{3}$$

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 . \square

8. JAN 29: INDUCTION PART 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 . \square

9. JAN 31: INDUCTION, SOME MORE EXAMPLES, STRONG INDUCTION (IF TIME)

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 is 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: 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
- $(P(k) \text{ true for } 1 \leq k < n \Rightarrow P(n) \text{ true})$ 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).

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?

Note that our goal is to show every m/n can be put in least terms. Assume that indeed, $P(k)$ is true for $1 \leq k < n$. 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).

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:

$$m + n = 2(k + j) + 1$$

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

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: DIVISION ALG, REDUCING FRACTIONS

Do reducing fractions proof. Then also do division algorithm.

For $a \in \mathbb{N}, b \in \mathbb{N}$ 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).

12. FEB 7: (NUMBER THEORY 1) DIVISION ALGORITHM

Hamkins 3

Talk about division with remainder: put as many copies of b into a , get a leftover bit. The remainder should be $< b$, otherwise I could shrink it. Well-ordering might be useful here.

If time, talk about Euclid's algorithm. Have students do examples, look for patterns. Suggest GCD stuff.

13. FEB 9 (NUMBER THEORY 2): EUCLID'S ALGORITHM

[To be filled in]

14. FEB 12 (NUMBER THEORY 3):

[To be filled in]

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.

$$S = \{\text{red, green, blue}\},$$

$$P = \{1, 2, 7, 9\}$$

(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: \emptyset : 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 $S \neq \emptyset$, 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. $\{\emptyset\}$ 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 $S \neq \emptyset$, 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.

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 $(A \cup B) \times C = (A \times C) \cup (B \times C)$. \square

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 $\mathcal{P}(A)$. (Different from $P(k)$ in induction!!) $\mathcal{P}(A)$ is the set of all subsets of A .

Example: (count by number of elements)

$$\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$$

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 \emptyset are in $\{1, 2, 3\}$. As in, $x \in \emptyset \Rightarrow x \in \{1, 2, 3\}$ is true, because the first part is always F. So $\emptyset \subseteq \{1, 2, 3\}$.

And then ask: what should this be?

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

Do a few more examples: $\mathcal{P}(\{a\})$ and $\mathcal{P}(\{a, b\})$. $[1, 2] \in \mathcal{P}(\mathbb{R})$ or $[1, 2] \subseteq \mathcal{P}(\mathbb{R})$? Motivate counting the size of the power set.

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

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

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

18. FEB 21 (SET THEORY 4) :

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

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

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

Similarly with A_4 . Can do with A_n .

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

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

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

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

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

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

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:

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

A similar idea extends to intersections.

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

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

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

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:

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

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

If time, do power set counting stuff. Or ask: is $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$?

If time, could also do $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

19. FEB 23: (RELATIONS)

(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 $\mathbb{R} \times \mathbb{R}$ is $R = \{(x, y) : y - x \text{ is positive}\}$.

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 $a | b$ if and only if $b = ak$ for some $k \in \mathbb{Z}$.

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

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)

23. MARCH 4 (EQUIVALENCE CLASSES)

24. MARCH 6

Set theory. Taylor 4.

25. MARCH 8

Combinatorics. Hamkins 5.6. **Note: as going through this: always be doing concrete examples. Start with way to order 3 objects. Then ways to order 2 things chosen from 3. Then what about choosing 2 from 3 without order? Then what about choosing 3 from 4 without order?** Start with working out counting *permutations*. Ways to order n objects? n options for first, $n - 1$ options for second... results in $n(n - 1)(n - 2) \dots 2 \cdot 1 = n!$. Now suppose you have n objects and want to pick k with order. Then, get

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

(have to stop because only choosing k objects). Can express this as:

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

What about just picking k objects without caring about the order? Maybe you're just picking groceries and tossing them in a cart. Don't really care what order they came in. Well, think about a collection of k objects. The above quantity counts it multiple times, because it cares about all the orders they came in. $k!$ ways to reorder it, so the above counts the same grocery cart $k!$ times. Need to divide out by this redundancy.

$$\binom{n}{k} = \text{number of ways to choose } k \text{ objects from } n = \frac{n!}{(n - k)!k!}$$

These are binomial coefficients One really fun consequence: this number above, which *a priori* looks like a fraction, in fact has to be a integer! It's counting an integer quantity! Super fun!

26. MARCH 11

Combinatorics. Hamkins 5.6

Today: the fun of combinatorics: can bash things out with algebra, or do clever proofs with words!!

Do Pascal's triangle $\binom{n}{k}$ with $n \geq k \geq 0$. Row number is index of n on top. Observe an additive pattern. Then: two proofs!

One way: note that

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

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

But perhaps an easier way to see it is: $\binom{n+1}{k}$ counts the number of ways to choose k objects from $n+1$. Consider this new added $n+1$ -th object. When you pick the k objects, you can include this new object or not. If you do, you are picking the remaining $k-1$ objects from the remaining n objects. If you do not pick it, you are choosing k objects from the n original objects. These two scenarios are disjoint and cover everything. Hence you get Pascal's formula.

(Draw this with circles and dot-dot-dots)

27. MARCH 13

Combinatorics

28. MARCH 15

Combinatorics

29. MARCH 25

Functions and equivalence relations

30. MARCH 27

Functions and equivalence relations

31. MARCH 29

Functions and equivalence relations

32. APRIL 1

Functions and equivalence relations

33. APRIL 3

Functions and equivalence relations: now in combination with modular arithmetic!

34. APRIL 5

Graph theory

35. APRIL 8

Graph theory

36. APRIL 10

Graph theory

37. APRIL 12

Graph theory

38. APRIL 15

Graph theory

39. APRIL 17

Finite games

40. APRIL 19

Finite games

41. APRIL 22

Finite games

42. APRIL 24

Finite games

43. APRIL 26: REVIEW FOR FINAL EXAM

Go over practice problems and strategies