TEXT: *Book of Proofs*, Hammack, R., Ed. 2

Lecture 1 - Sec 1.1 Sets

DUE TUES: Sec 1.1: 1, 12, 19, 26, 29, 35

set, element, finite vs infinite sets, equality for sets, membership (epsilon), cardinality,

Welcome
Syllabus/Calendar
2-minute intros (?)

THIS COURSE: Big ideas + technical knowledge

Big idea: This is course about how to prove theorems.

- Being precise and unambiguous when we express ourselves. *(Definitions matter. A lot.)*
- Metacognition - thinking about the way we think. *The math is not the most difficult part of this course - we'll be looking at it in new ways, and asking questions about it that we don't normally ask!*

QUICK METACOGNITION EXERCISE: Complete the following problem, either in your head or on paper (no technology). Pay attention to the specific steps you went through while solving it.
Give 2 minutes. Then ask for volunteers to share back. How many different strategies were used?

Technical knowledge: Sets, logic (reasoning), proofs

GROUP WORK - THINK/PAIR/SHARE

SETUP: What is pi equal to? $\pi \approx 3.1415...$

Think/Write: You have 3 minutes to formulate a one-sentence response to the question on your own (write it down).

QUESTION: How do we know that pi = 3.1415…?

(What if I were to tell you that pi is REALLY equal to 2.93? How could you tell if I was right?)
Pair: Ask students to share thoughts with their partners and ask questions if they don't understand what their partner is saying. Circulate around the room, listening to student conversations.
Share: Ask for student volunteers to share as you begin this process. Later, you should call on non-volunteers to increase student accountability in this cooperative learning strategy.

SETS
Definitions
A **set** is a collection of things. The things in the collection are called **elements** (or **members**) of the set.

The notation "$x \in A$" means "x is an element of A"
Two sets are **equal** if they contain the same elements.
The **cardinality**, or **size**, of a set A is the number of elements it has, and is written |A|.
A set is called **finite** if it has a finite number of elements, otherwise it is **infinite**.

Example 1: A = {2,4,6,8} B = {1,2,3,4,...}

a. What does the "..." mean in set B?
b. True or false: i. $2 \in A$ ii. $5 \in A$ iii. $5 \in B$
c. True or False: i. A=B ii. {2,4,6,8}={8,6,4,2} iii. A={2,2,4,6,8}
d. What is |A| (the cardinality of A)? What is |B|?
e. The set B is a very common one in mathematics. What is it called?

a. "the pattern continues forever"
b. i. T, ii. F, iii. T
c. i. F, ii. T, iii. T (the order of the elements in the list doesn't matter, the number of times an element appears in the list doesn't matter)
d. $|A|$=4, the cardinality of B is infinity, $|B|$=infinity (we'll give a more precise answer later)
e. the set B is called the ***natural numbers****, usually written* $\mathbb{N} = \{1, 2, 3, 4, ...\}$

Example 2: Does C=D, where C = {...-4,-3,-2,-1,0,1,2,3,4…}, D = {0, 1, -1, 2, -2, 3, -3, 4, -4, …} ?
NOTE: this set also has a special name - anyone know it?
The ***integers*** *are the set* $\mathbb{Z} = \{... -4, -3, -2, -1, 0, 1, 2, 3, 4...\}$

Example 3: Sets don't have to consist of numbers.
A = {T, F}
B = {a, e, i, o, u}
C = {students in this class right now}
D = { (0,0), (0,1), (1,0), (1,1) }
E = {5, {2,3}, {4,6}}

QUESTIONS:
set A: What is the cardinality of set A?
set B: What is the cardinality of set B?
set C: Is John Fredrickson a member of set C? Is Prof Reitz a member of set C? Give an example of a member of set C. What is the cardinality of set C?
set D: Elements of this set are ordered pairs, or coordinates. What is the cardinality of this set? If we plot the four points, what shape do they make? Is (0,1) an element of D? Is 1 an element of D?
set E: Note that sets can have other sets as elements. What are the elements of set E? Is $5 \in E$? Is $\{2, 3\} \in E$? Is $2 \in E$? Is $\{2, 3, 4, 6\} \in E$?

There is a special set that, though small in size, plays an important role in set theory -- it is the set with no elements, called the **empty set**.

Definition: The **empty set** is the set {} with no elements. The symbol for the empty set is $\emptyset$.
NOTE: The symbol $\emptyset$ is just shorthand for {}.

QUESTIONS:

a. What is the size of the empty set $|\emptyset|$?
1. Is $\{\emptyset\}$the same as the empty set $\emptyset$?
2. True of False: i. $\emptyset \in \emptyset$? ii. Is $\emptyset \in \{\emptyset\}$?
3. What is the size of the set: $\{ \emptyset, \{\emptyset\}, \{\{\emptyset\}\} \}$?

HELPFUL IDEA: "a set is just a box"
$\emptyset$ is an empty box. $\{\emptyset\}$ is a box which is not empty - it has another box inside it (the inside box *is* empty).

For more complicated sets, we often describe their contents using **set-builder notation**.
Ex: Consider the set E={...,-6,-4,-2,0,2,4,6,...}, the set of even integers. In set-builder notation, this is $E = \{2n: n \in \mathbb{Z}\}$. In words, "E is the set of all things of the form 2n, such that n is in Z"

Definition: In general, a set X written with **set-builder notation** has the form

X = {expression : rule}

where X is the set of all values of the expression that are specified by the rule.

Example 4
List the members of each set. If the set is infinite, list a few members.

a. $\{n^2: n \in \mathbb{N}\}$
b. $\{3n + 1: n \in \mathbb{Z}\}$
c. $\{x \in \mathbb{Z}: 2x + 7 = 3\}$
d. $\{2n: n \in \mathbb{Z}, |n| < 3\}$
e. $\{x: x \in \mathbb{R}, 1 < x \leq 5\}$

Write each set in set-builder notation:

f. {2,4,8,16,32,64,...}
g. {...-15,-10,-5,0,5,10,15,...}
h. the closed interval [-3,8] on the number line

BEWARE: The notation |X| means cardinality if X is a set, but |x| means absolute value is x is a number.
NOTE: discuss interval notation for d.

Some sets are important enough that they are given special names/symbols:

- The **empty set** $\emptyset = \{\}$
- The **natural numbers** are the set $\mathbb{N} = \{1, 2, 3, 4,...\}$
- The **integers** are the set $\mathbb{Z} = \{... -4, -3, -2, -1, 0, 1, 2, 3, 4...\}$
- The **rational numbers** are the set of fractions $\mathbb{Q} = \{x: x = \frac{m}{n},\ where\ m, n \in \mathbb{Z}\ and\ n \neq 0\}$
- The **real numbers** are the set $\mathbb{R}$(all the numbers on the number line)

Lecture 2 - Sec 1.2 Cartesian Products, 1.3 Subsets

ordered pair, Cartesian product, ordered triple, (Cartesian power), subset

DO NOW:
100 ants (zero-length points) walk on a meter stick (a line) at 1 cm/second. When two ants collide, they both reverse direction. If an ant reaches the end of the stick, it falls off. What arrangement of ants maximizes the time before all ants have fallen off? How long can they last?

UNPACK: Simple insight/change of perspective that makes answer much more clear? (reflecting is equivalent to "passing through").
QUES: Why ask this question in this class?

Three kinds of theorem proving:

1. ***Given a proof of a theorem, can you follow it?***
2. ***Given a theorem, can you find a proof of it?***
3. ***Given a problem, can you formulate a theorem ("conjecture"), and then prove it?***

Given two sets A and B, it is possible to "multiply" them to form a new set, AxB, called the **Cartesian product** of A and B. This idea is based on *ordered pairs*.

Definition. An **ordered pair** is a list (x,y) of two things, x and y, enclosed in parentheses and separated by a comma.

THE MAIN DIFFERENCE BETWEEN AN ORDERED PAIR, AND A SET WITH 2 ELEMENTS: The in an ordered pair, the order the elements are written in matters!

Ex: (2,4) is an ordered pair, and so is (4,2). These are NOT equal, even though they contain the same things, because the order is different.

Examples of ordered pairs: i) (a,b) ii) ({3,6},{2,7, 5}) iii) ((5,6), (11,9)) iv) $(\mathbb{R}, \{\emptyset\})$

Definition. The **Cartesian product** of two sets A and B is another set, written $A \times B$, and defined as $A \times B = \{(a, b): a \in A,\ b \in B\}$.

Example 1: If A={p,q,r} and B={w,x},

i) find $A \times B$
ii) What is the cardinality $|A \times B|$? How does this compare to the cardinalities |A| and |B|?

Diagram for AxB -- show it in a plane, first coord along bottom, second on left side (axes).

Fact. If A and B are finite sets, $|A \times B| = |A| \times |B|$.

Example 2:
i) Describe the Cartesian product $\mathbb{R} \times \mathbb{R}$.
ii) If A is the closed interval [0,1] and B is the half-open interval [2,3), draw a sketch of $A \times B$.
Recall interval notation - discuss.

We can multiply more than two sets - for three sets, we use **ordered triples** instead of **ordered pairs**.

Example 3: If $A = \{3, 7\}$, $B = \{2, 4\}$, and $C = \{5, 9\}$, then:
i) is $(3, 2, 9) \in A \times B \times C$?
ii) is $(3, 5, 2) \in A \times B \times C$?

A **Cartesian power,** like $\mathbb{R}^2$, is simply shorthand for the product of a set with itself $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (similar for higher powers: $\mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$)

SECTION 1.2 - SUBSETS

Definition. If A and B are sets, and every element of A is also an element of B, then we say **A is a subset of B** and we write $A \subseteq B$. If this is *NOT* the case then we say **A is not a subset of B**, and we write $A \nsubseteq B$.
NOTE: $A \nsubseteq B$ means there is at least one element of A that is not an element of B.

Example 4: If $A = \{2, 3, 5\}$, $B = \{2, 3, 4, 5, 6, 7, 8\}$ and $C = \{1, 2, 3\}$,
i) is $A \subseteq B$? Why?
ii) is $A \subseteq C$? Why?
iii) is $C \subseteq A$? Why?
iv) is $A \subseteq A$? Why?
v) is $\emptyset \subseteq A$? Why?

Theorem: Every set is a subset of itself, $A \subseteq A$
Theorem: The empty set is a subset of every set: for any set A, $\emptyset \subseteq A$.

?Optional: Creating subsets of a set.
Ex: B={1,2,3}. Discuss creating a subset by starting with { }, and choosing some members of B to insert. -- ex: choose 1, 2 to get {1,2}, or choose 2,3, to get {2,3}. In general, we can get **any** subset of B by simply considering each member in turn, and making a Yes/No decision whether to include it or not. *Create a tree diagram for this!* -- Each branch of the tree gives a subset. How many subsets are there?

?Optional: Theorem. If A is a finite set with *n* elements, then A has exactly 2^n many different subsets

GROUP WORK:

Example 5

a) If $A = \{\pi, 5\}$and $B = \{4, 7\}$, then

i) Find $A \times B$ and B^2

ii) is $(\pi, 7) \in A \times B$?

iii) is $(4, 5) \in B \times A$?

iv) is $(\pi, \pi) \in A^2$?

b) If $A = \{\{4, 5, 6\}, \emptyset\}$ and $B = \{ \mathbb{N}, \mathbb{Z}, (\emptyset, \{2, 7\}) \}$, then

i) is $(\{4, 5, 6\}, \mathbb{Z}) \in A \times B$?

ii) is $(\emptyset, \emptyset) \in A \times B$?

iii) Find $A \times B$. What is $|A \times B|$?

iv) is $((\emptyset, \{2, 7\}), \mathbb{N}, \{4, 5, 6\}) \in B^3$? What product of A's and B's **is** it an element of?

c) Sketch the set $[0, 1] \times \{1, 3, 5\}$ in the plane.

*** More examples like this??*

d) Consider the set with two elements$\{5, \{5\}\}$. True or False:

i) $5 \in \{5, \{5\}\}$

ii) $5 \subseteq \{5, \{5\}\}$

iii) $\{5\} \in \{5, \{5\}\}$

iv) $\{5\} \subseteq \{5, \{5\}\}$

v)$\{\{5\}\} \in \{5, \{5\}\}$

vi) $\{\{5\}\} \subseteq \{5, \{5\}\}$

e) True or False:

i) $\{ (1, 1), (2, 6), (5, -1), (3, 2) \} \subseteq \mathbb{Z} \times \mathbb{Z}$

ii) $\mathbb{N} \times \mathbb{N} \subseteq \mathbb{R} \times \mathbb{R}$

Lecture 3 - 1.4 Power Sets, 1.5 Union Intersection Difference, 1.6 Complement, 1.7 Venn Diagrams

bring colored chalk today?
power set, union, intersection, difference, complement, universal set, Venn diagram

DO NOW: Somewhere on Earth….
You go on a hike, as follows: First you hike 1 mile due South, then 1 mile due West, then 1 mile due North. To your amazement, at the end of your hike you find yourself *back in the same place you started(!)* Where did you start your hike?

UNPACK: Is there anywhere ELSE you could start your hike?
QUES: Why would we look at this question, in this class?

Definition. If A is a set, then the **power set** of A is another set, denoted $\mathcal{P}\mathcal{P}P(A)$, and defined to be the set of all subsets of A: $P(A) = \{X: X \subseteq A\}$.

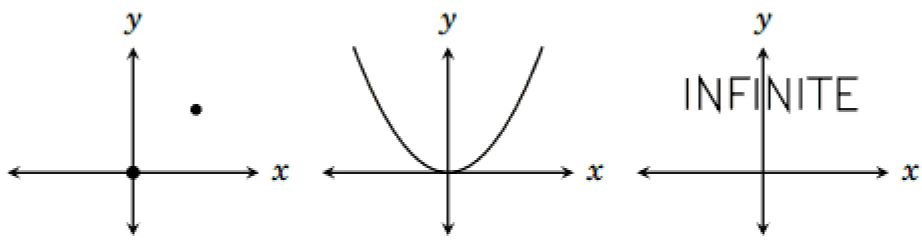
Example 1: If A={1,2,3}, find P(A).
?Use tree diagram to list members of A?
QUES: What is |A|? What is |P(A)|
Note: If a set A has n elements, then the power set P(A) has 2^n *elements.*

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

Ex: Is it a member of $P(\mathbb{N})$?
a) {7}
b) 7
c) {7,11,25,99}
d) {-2,-1,0,1,2}
e) *the even numbers*
f) {2,3,5,7,11,13,...}
NOTE: Must be a subset of N!

Ex: Is it a member of $P(\mathbb{R}^2)$?
a) {(0,0), (0,1)}
b) {0,1}
d) The graph of the equation $y = x^2$, that is, $\{(x, y): y = x^2\}$
e) The graph of ANY function.
f) *Sketch a silly picture*
g) ANY black-and-white image in the plane

Ex: some of the many, many sets in $P(\mathbb{R}^2)$



(a) (b) (c)

Sec 1.5 Union Intersection Difference
Just as we can combine numbers with operations like addition, subtraction, multiplication, we can also combine sets together with various operations (we learned about one, Cartesian product, already).

Definition. Suppose A and B are sets, then
the **union** of A and B is the set $A \cup B = \{x: x \in A \text{ or } x \in B\}$.
the **intersection** of A and B is the set $A \cap B = \{x: x \in A \text{ and } x \in B\}$.
the **difference** of A and B is the set $A - B = \{x: x \in A \text{ and } x \notin B\}$ (sometimes written $A \backslash B$)
NOTE: in union, the word "or" means "either in A or in B or in both" (inclusive or)

Example 3: Suppose $A = \{a, b, c, d, e\}$ and $B = \{d, e, f\}$
a) $A \cup B$
b) $A \cap B$
c) $A - B$
d) $(A - B) \cup (B - A)$
e) $(A \cap B) \cup (A \backslash B)$
f) $(A \cap B) \times B$

*?** Example: Let* $A = \{(x, x^2): x \in \mathbb{R}\}$ *be the graph of the equation* $y = x^2$*, and* $B = \{(x, x + 2): x \in \mathbb{R}\}$*be the graph of the equation* $y = x + 2$*. Find* $A \cap B$, $A \cup B$, $A - B$.

1.6 Complement
There is basically one more set operation, called **complement**, but to define it we need the idea of a **universal set**. Almost always, when we are given a set, we regard it as a subset of some larger set that is our "universe" or "context for the problem at hand".

Ex: the set of prime numbers P={2,3,5,7,11,13,...} is a subset of what? ($\mathbb{N}$).

We don't mention the set $\mathbb{N}$, but it's assumed that $P \subseteq \mathbb{N}$, because that is the most natural context for discussing prime numbers. If we are asked to name things that are NOT prime numbers, we might give examples like 4 or 12, but we probably wouldn't give examples like 17.45, or $\sqrt{2}$, or "frogs" or "Barack Obama".

In this context, the set $\mathbb{N}$ is called the **universal set** or **universe** for P.

Ex: the unit circle is the set $C = \{(x, y): x^2 + y^2 = 1\}$. What is the universal set for C?

Definition. Let A be a set with universal set U. The **complement** of A, denoted $\overline{A}$ (or A^C), is the set $\overline{A} = U - A$.

Example 4:
a) If P is the set of prime numbers, then what is $\overline{P}$?
b) If A={a, c, d, e, g} has universal set U={a, b, c, d, e, f, g}, then what is $\overline{A}$?

1.7 Venn diagrams
It can be useful when thinking about combinations of sets to be able to draw a simple picture that lets you see how they are combined. These pictures are called Venn diagrams (British logician John Venn, 1834-1923).
- in a Venn diagram, each set is represented by a circle.
Sketch Venn diagram for two sets. Include UNIVERSAL SET!

Example 5.
I. For two sets A and B, sketch Venn diagrams for:
a) $A \cup B$
b) $A \cap B$
c) $A - B$

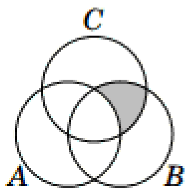
CLASS
II. For three sets A, B, and C, sketch Venn diagrams for:
a) $A \cap B \cap C$
b) $(A \cup B) \cap C$
c) $A \cup (B \cap C)$

WHEN DO WE NEED PARENTHESES?
When an expression contains only unions ∪, then parentheses are optional.
When an expression contains only intersections ∩, then parentheses are optional.
When an expression contains a combination of ∪ and ∩, parentheses are **essential**!

Example 6.
a) Sketch a Venn diagram for $(A - B) \cup (B \cap C)$
b) If $|D| = 10$, $|E| = 12$, and $|D \cap E| = 6$, what is $|D \cup E|$? *HINT: It might help to draw a Venn*

diagram for D and E, and figure out how many elements are in each region.

c) Write an expression for this Venn diagram:



d) Consider the following intervals of the real line: $A = [1,4]$, $B = (2,3]$ and $C = (3,\infty)$. Sketch the set $(A - B) \times (A \cap \overline{C})$ in the plane.

e) If $A = \{a, b\}$ and $B = \{a\}$, with universal set $U = \{a, b, c, d\}$, find:

i) $\overline{A} \times \overline{B}$ ii) $P(A) \cap P(B)$ iii) $P(B \times A)$ iv) $P(\overline{A})$

Lecture 4 - (1.7 Venn Diagrams), 1.8 Indexed Sets, 2.1 Logic

indices, indexed sets, index set, logic, statements

FOLLOWUP TO LAST TIME
GROUPS: Do example 6 from last time
(- example 3)

When we need to talk about a lot of different sets, instead of giving each of them different names A, B, C, D, E, F it's convenient to keep track of them by using subscript numbers, like A_1, A_2, A_3, A_4, A_5 -- the subscript numbers are called indexes ("indices"), and the sets are called **indexed sets**.

Definition. **Indexed sets** are sets that are distinguished by attaching subscript numbers instead of using different letters, such as A_1, A_2, A_3, A_4, A_5. We call the number 1,2,3,4 and 5 the **indices**.

We've talked about taking the union or intersection of two sets. What does it mean to take the union or intersection of many sets?
Write a union on the board - what does it mean for an element to be in the union? (it's in at least one of them).
Intersection?

Definition. Unions and intersections of many sets. Suppose $A_1, A_2, A_3, ..., A_n$ are sets. Then
$A_1 \cup A_2 \cup A_3 \cup ... \cup A_n = \{x: x \in A_i \textit{ for at least one set } A_i, \textit{ for } 1 \le i \le n\}$
$A_1 \cap A_2 \cap A_3 \cap ... \cap A_n = \{x: x \in A_i \textit{ for every set } A_i, \textit{ for } 1 \le i \le n\}$

We'd like a compact way of writing intersections and unions for a collection of indexed sets -- this may look familiar, as it is similar to the sigma (summation) notation you learned in Calc II.

Notation. Given sets $A_1, A_2, A_3, ..., A_n$, we define
$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup ... \cup A_n$ and $\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap A_3 \cap ... \cap A_n$

Example 1. Suppose $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$ and $A_3 = \{2, 5, 7\}$. Find $\bigcup_{i=1}^{3} A_i$ and $\bigcap_{i=1}^{3} A_i$.
This notation is also useful when the list of sets is infinite $A_1, A_2, A_3, ...$

Example 2. Consider the following infinite list of sets:

$A_1 = \{-1, 0, 1\},\ A_2 = \{-2, 0, 2\},\ A_3 = \{-3, 0, 3\}, \ldots, A_i = \{-i, 0, i\}, \ldots$

Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.

?How many elements in each Ai? What is A_{50}? A_{127}? *etc.*

Finally, here's a new twist on this notation: Instead of $\bigcup_{i=1}^{3} A_i$ we can write $\bigcup_{i\in\{1,2,3\}} A_i$.

We call the set {1,2,3} the **index set**, denoted *I.*

Definition. The **index set *I*** is the set of all indices (of a collection of sets).

Instead of $\bigcup_{i=1}^{\infty} A_i$ we can write WHAT? *?What is the index set?* $(\bigcup_{i\in\mathbb{N}} A_i)$

Notation. If *I* is an index set, and for each $\alpha \in I$ we have a corresponding set A_α, then

$$\bigcup_{\alpha\in I} A_\alpha = \{x: x \in A_\alpha \textit{ for at least one set } A_\alpha \textit{ with } \alpha \in I\}$$

$$\bigcap_{\alpha\in I} A_\alpha = \{x: x \in A_\alpha \textit{ for every set } A_\alpha \textit{ with } \alpha \in I\}$$

Why do we care? It allows us to take unions/intersections of sets even when they are not arranged in the order 1,2,3,4,5,...

Warmup: Sketch the subset of $\mathbb{R}^2$ - $\{(x, 0.5): 1 \le x \le 2\}$

Example. Here the sets will be subsets of $\mathbb{R}^2$. *Each of my sets will be a horizontal line stretching between x=1 and x=2. My sets are all those lines that appear between the x-axis and y=2. Sketch a few examples - with alpha=1, 2, 1.5, 1.687, etc.*

Example 3. Let the index *I* be the closed interval [0, 2], that is $I = [0, 2] = \{x: 0 \le x \le 2\}$. For each number $\alpha \in I$, let the set $A_\alpha = \{(x, \alpha): x \in \mathbb{R}\ ,\ 1 \le x \le 2\}$. Find $\bigcup_{\alpha\in[0,2]} A_\alpha$ and $\bigcap_{\alpha\in[0,2]} A_\alpha$.

Chapter 2 - LOGIC

The word **logic** refers to the way that humans *reason* **-** how we combine old information to deduce new information. It is nothing exotic - you use logic all the time in your everyday life, and certainly when you do mathematics. For example, suppose you are studying a certain circle, circle X, and you have available the following two pieces of information:

1. Circle X has radius 3.
2. If any circle has radius *r*, then it's area is πr^2.

What do we get when we combine these two facts?

3. Circle X has area 9π

We used logic to combine two given facts, to produce a new fact. We are used to doing this naturally and intuitively, but in this class we are going to try study and understand this process in detail - what are the rules that govern logic?

logic vs. information

NOTE: It's important to realize the difference between ***correct logic*** *and* ***correct information*** *(we are interested in BOTH). For example, what if it turned out that we had made a mistake, and that*
Circle X actually has radius 4. Then our first fact is wrong, and our conclusion 3 is also wrong - BUT our logic is correct - we we used the correct logical steps, just based on incorrect information

Sec 2.1 - Statements
The study of logic begins with basic building blocks called statements.

Definition (informal). A ***statement*** *is a sentence or a mathematical expression that is either definitely true or definitely false.*

Example 1
Examples of statements:
The three items 1,2,3 above are examples of statements:

1. *Circle X has radius 3.*
2. *If any circle has radius r, then it's area is* πr^2.
3. *Circle X has area* 9π

Also,

4. $2 \in \mathbb{Z}$
5. *The set {0,1,2} has three elements.*

Statements don't have to be true - here are some false ones:

6. $\mathbb{Z} \subseteq \mathbb{N}$
7. *Every right triangle has two right angles.*

Example 2 -
What is NOT a statement?

1. *Is it raining? - Questions can have different answers, like YES or NO, but the question itself is not definitely true or definitely false.*
2. $x^2 + 1$ *- This is a function - if you plug in an x, it will give you back a number - but it is not true or false.*
3. *Take the square root. - Commands, or instructions, simply give you something to do - they are not true or false*

Example 3. Is it a statement? If so, is it true or false?

a) *Add 5 to both sides of* $x - 5 = 7$.

b) Adding 5 to both sides of $x - 5 = 7$ *gives* $x = 17$.
c) $\mathbb{N}$
d) $56 \in \mathbb{N}$
e) What is the solution of $3x = 9$*?*
f) The solution of $3x = 9$ *is* 3.

Lecture 5 - 2.1 Statements, 2.2 And, Or, Not, 2.3 Conditional Statements

statement, open sentence, and, or, not, if..then, truth table

NOTE: Laureen Park guest lectured today - see link to her slides on OpenLab Handouts page

Recall **statements**. (what makes something a statement?).
Notation: We often use the letter P, Q, R and S to stand for statements. Sometimes we also use subscripts.
When a statement involves a variable *x*, we sometimes use notation like a function, P(x).
Definition. A sentence whose truth depends on the value of one or more variables is called an **open sentence**. An **open sentence** is not a statement.

Example 1. Is it a statement? Is it true or false?
Q: Every polynomial of degree *n* has at most *n* roots
S_1: The function $f(x) = x^2$ is continuous.
S_2: $\mathbb{Z} \subseteq \emptyset$
$S_3(x)$: If *x* is an even integer and $x > 2$ then *x* is not prime.
$P(x)$: *x* is an even integer.
$R(f, g)$: The function *f* is the derivative of the function *g*.

True or False:
a) $P(11)$
b) $P(14)$
c) $R(x^3, 3x^2)$
d) $R(3x^2, x^3)$

NOTE: Discuss $S_3(x)$ -- built up of simpler statements, using connecting words “and” “if...then”. In this chapter we are going to focus on these connecting words - how do we combine statements to make more complicated statements?
and, or, not, if...then

Statements are the heart of mathematics - *every* mathematical discovery, theorem, “fact”, hypothesis, axiom and conjecture is, in essence, a statement.
Some famous mathematical statements
P: If a right triangle has legs of length *a* and *b* and hypotenuse of length *c*, then $a^2 + b^2 = c^2$.
Q: There are natural numbers $a, b, c, n \in \mathbb{N}$ with $n > 2$, satisfying $a^n + b^n = c^n$.
R: Every even integer greater than 2 is the sum of two primes.

P - TRUE. pythagorean theorem (around 500 BC). Q - FALSE. The opposite was proven in 1993 by Wiles (Fermat’s Last Theorem - asked in 1637). R - Goldbach conjecture (first asked in 1742, *still open)*

COMBINING STATEMENTS TO MAKE NEW STATEMENTS
Example: R_1: The number 2 is even and the number 3 is odd.
Ques: True or False?

This statement was created by combining two simpler statements:
P: The number 2 is even.
Q: The number 3 is odd.
R_1: P *and* Q

They were joined by the word "**and**" to build the statement R_1. R_1 asserts that both P and Q are true -- since P is true, and Q is true, then R_1 is true. If either P or Q had been false, then R_1 would have been false.

Example: Is each of the statements R_1, R_2, R_3, R_4 true or false?
R_1: The number 2 is even and the number 3 is odd.
R_2: The number 1 is even and the number 3 is odd.
R_3: The number 2 is even and the number 4 is odd.
R_4: The number 1 is even and the number 4 is odd.

Rule. Any two statements P and Q can be combined to form a new statement "P **and** Q", which is true if both P is true and Q is true, and is false otherwise. The word **'and'** is represented by the symbol ∧, so "P **and** Q" is written $P \wedge Q$.
Truth Table for $P \wedge Q$

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

NOTE: The truth table is our ultimate authority when trying to understand a statement - this is what we rely on when we have disagreements about what a complex combination of statements means.

We can also combine statements using the word **or**. Consider
Example: Is each of the statements true or false?

S_1: The number 2 is even or the number 3 is odd.
S_2: The number 1 is even or the number 3 is odd.
S_3: The number 2 is even or the number 4 is odd.
S_4: The number 1 is even or the number 4 is odd.

Rule. Any two statements P and Q can be combined to form a new statement "P **or** Q", which is true if either P is true or Q is true or both. The word **'or'** is represented by the symbol ∨, so "P **or** Q" is written $P \vee Q$.

Example: Complete the truth table for $P \vee Q$.
Truth Table for $P \vee Q$.

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

> NOTE: as previously discussed, in mathematics the word 'or' ALWAYS means "one, or the other, or both". If we ever want to express the idea "one, or the other, but not both", we will use one of the following phrases:
> 1. P or Q, but not both. *"You can have either an ice cream cone or a cupcake, but not both."*
> 2. Either P or Q. *"Either pay your tuition, or you will be withdrawn from school."*

A final way of creating a new statement is to **negate it**, that is, to say "it is not true that".
Example: The number 2 is even.
True or False?)
To negate this statement, we add the phrase "It is not true that" at the front --
It is not true that the number 2 is even.
Is the new statement True or False?

Rule. For any statement P, we can create the new statement "It is not true that P", or simply "not P", called the **negation of P**. The negation of P is true only when P itself is false, and the negation of P is false only when P is true. The notation for the negation of P is $\sim P$.

Truth Table for $\sim P$

P	$\sim P$

T	
F	

We express the negation in various ways -- if P: The number 2 is even, then we might say:
$\sim P$: It's not true that the number 2 is even.
$\sim P$: It's false that the number 2 is even.
$\sim P$: The number 2 is not even.

??? Example: Translating statements into this notation.

Sec 2.3 Conditional Statements
One more way of combining statements.
R: If you pass the final exam, then you pass the class.

R is formed from two statements:
P: You pass the final exam.
Q: You pass the class.
Combined using "If...then"
R: If P, then Q.

Rule. Any two statements P and Q can be combined to form the new statement "if P, then Q", called a **conditional statement**. The notation for "if P, then Q" is "$P \Rightarrow Q$". $P \Rightarrow Q$ will be true if P and Q are both true, or if P is false and Q is anything.

Truth Table for $P \Rightarrow Q$

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

The conditional $P \Rightarrow Q$ is like a promise - a promise that if P is true, then Q is also true. The only way for that promise to be broken (for $P \Rightarrow Q$ to be false), is if P is true, but Q is false. In all other cases , the promise is correct.

In mathematics, especially when reading proofs, you will see this idea expressed in many different ways. List of alternative phrases, all of which mean "$P \Rightarrow Q$"

- If P, then Q.
- Q if P.

- Q whenever P.
- Q, provided that P.
- Whenever P, then also Q.
- P is a sufficient condition for Q.
- For Q, it is sufficient that P.
- Q is a necessary condition for P.
- For P, it is necessary that Q.
- P only if Q.

Example 4

Express each statement as $P \wedge Q$, $P \vee Q$, $\sim P$, or $P \Rightarrow Q$. Be sure to state P and Q exactly.

a) You must present either a passport or a driver's license.

b) The number 8 is both even and a power of 2.

c) If a man is a superhero then he has superpowers.

d) Six times nine is not equal to 42.

e) Having frog legs is a necessary condition for being a frog.

Lecture 6 - 2.4 Biconditional Statements, 2.5 Truth Tables for Statements, 2.6 Logical Equivalence

statement, open sentence, and, or, not, if..then, truth table

Question: Is $P \Rightarrow Q$ the same as $Q \Rightarrow P$?
Example:
(a is a multiple of 6) ⇒ (a is even)
(a is even) ⇒ (a is a multiple of 6)

Definition. The statement $Q \Rightarrow P$ is called the **converse** of $P \Rightarrow Q$.
NOTE: A conditional statement and its converse express entirely different things!
(ex: If I am Mr. Reitz then I have long hair. *What's the converse?*)

However, it is sometimes the case that both a statement $P \Rightarrow Q$ and its converse $Q \Rightarrow P$ are both true -- for example:
(a is even) ⇒ (a is divisible by 2)
(a is divisible by 2) ⇒ (a is even)
Since these are both true, we have $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is true. We have a shorthand for this:

Definition. $P \Leftrightarrow Q$ means $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. It is read "P if and only if Q".

Example 1: Truth table for $P \Leftrightarrow Q$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$ $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	T			
T	F			
F	T			
F	F			

Use the statement (a is even) ⇔ (a is divisible by 2) *as a reference - if a is even, what happens? If a is odd, what happens? Can we have a even, but not divisible by two? etc.*

List of alternative phrases, all of which mean "$P \Leftrightarrow Q$"

- P if and only if Q
- P is a necessary and sufficient condition for Q.
- For P is it necessary and sufficient that Q.
- If P, then Q, and conversely.

LOGICAL EQUIVALENCE

Recall: $P \Leftrightarrow Q$. *QUES: When is it true? When is it false?*

It seems that $P \Leftrightarrow Q$ means the same thing as “$(P \wedge Q) \vee (\sim P \wedge \sim Q)$”. Is this true? We can answer this question “for sure” by comparing truth tables.

Example 2: Is $P \Leftrightarrow Q$ logically equivalent to $(P \wedge Q) \vee (\sim P \wedge \sim Q)$**?**

P	Q	$(P \wedge Q)$	$\sim P$	$\sim Q$	$(\sim P \wedge \sim Q)$	$(P \wedge Q) \vee (\sim P \wedge \sim Q)$	$P \Leftrightarrow Q$
T	T						
T	F						
F	T						
F	F						

Definition. Two statements are **logically equivalent** if their truth values match up line-for-line in a truth table. In symbols, we express this using the equals sign.

Fact: $P \Leftrightarrow Q \ = \ (P \wedge Q) \vee (\sim P \wedge \sim Q)$

(informal): We think of two logically equivalent statements as “saying the same thing”.

RULE: We are allowed to replace a statement with a logically equivalent statement.

There are certain logical equivalences that show up again and again in proofs -- here we will discuss three in particular, the **contrapositive** and **De Morgan’s Laws**.

CONTRAPOSITIVE

QUES: Is $P \Rightarrow Q$ logically equivalent to $Q \Rightarrow P$? *ANS: NO - the converse means something different.*

QUES: Is there anything that’s **like** the converse, but **is** logically equivalent to $P \Rightarrow Q$?

Example: Show that $(\sim Q) \Rightarrow (\sim P)$ is logically equivalent to $P \Rightarrow Q$

Definition. $(\sim Q) \Rightarrow (\sim P)$ is called the **contrapositive** of $P \Rightarrow Q$. The **contrapositive** means the same thing as (is **logically equivalent to**) the original.

NOTE: You can check this by comparing truth tables for $P \Rightarrow Q$ *and* $(\sim Q) \Rightarrow (\sim P)$.

Example: What is the contrapositive of “If I am Prof. Reitz, then I have long hair.”?

DE MORGAN’S LAWS

There are two pairs of logically equivalent statements that show up again and again, and have a special name:

Definition. De Morgan’s Laws.

$\sim (P \wedge Q) \;=\; (\sim P) \vee (\sim Q)$
$\sim (P \vee Q) \;=\; (\sim P) \wedge (\sim Q)$
Discuss briefly - if it's not true that both P and Q are true, then either P is false or Q is false.

CLASS
Example 3. a) Write an expression that means "Either P or Q is true, but not both".
b) Complete the truth table for the expression below.

P	Q	$P \vee Q$	$P \wedge Q$	$\sim (P \wedge Q)$	$(P \vee Q) \wedge\sim (P \wedge Q)$
T	T				
T	F				
F	T				
F	F				

GROUPS
Example 4. Consider the statement

S: The product xy equals zero if and only if $x = 0$ or $y = 0$.

a) Write S as a combination of the three simple statements:

P: $xy = 0$ Q: $x = 0$ R: $y = 0$

b) Write a truth table for the expression you created in a).

HINT: start with columns for P, Q, and R, and consider all combinations of T and F for these three statements.

GROUPS
Example 5. Determine whether the statements: $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$ are logically equivalent.

Lecture 7 - 2.7 Quantifiers, 2.8 More on Conditional Statements, 2.9 Translating English to Symbolic Logic, 2.10 Negating Statements, 2.11 Logical Inference

quantifiers, universal quantifier, existential quantifier

> *?? Necessary vs. Sufficient conditions -- http://en.wikipedia.org/wiki/Fire_triangle*
> ***FACT: To ignite a fire, three elements are required to be present: heat, fuel, and oxygen.***
> *Suppose we are trying to establish the following:*
> *R: Presence of fire*
> *S: Presence of oxygen*
> *Which one is **required** in order for the other to be present? S is a **necessary** condition for R (*
> *If you were to detect S, is that enough ("sufficient") for you to conclude R? If you were to detect R, is that sufficient for you to conclude S? R is a **sufficient** condition for S.*
> *BOTH of these relationships are expressed by the conditional statement $R \Rightarrow S$ (the first is sufficient, the second is necessary)*

The collection of logical symbols we have so far is *not quite* powerful enough -- we really need two additional (related) notions.

Definition. Quantifiers. The symbol ∀ is called the **universal quantifier**, and stands for the phrase *"For all"* or *"For every"*. The symbol ∃ is the **existential quantifier**, and stands for *"There exists"* or *"There is a"*.

Example 1. Translate to symbols. You may use the statements E(n) and O(n) in your answers.

    E(n): n is even
    O(n): n is odd

a. For every $n \in \mathbb{Z}$, $2n$is even.
b. There is a subset X of $\mathbb{N}$ which has cardinality 5.
c. Every integer that is not odd is even.
d. For every real number x, there is a real number y for which $y^3 = x$.
e. Not all integers are even.
f. All integers are not even.

NOTE: Do the first one, have people pair up to complete the rest.
Compare the last two - one is true and one is false - which is which? Be careful - we are often sloppy in casual speech, but we must be very careful in the mathematical context

Order of quantifiers is very important!

Example 2: Translate to English. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$

> *What does it say? Must the same y work for every x?*

What happens if we reverse the quantifiers: $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y^3 = x$.

What does it say? Must the same y work for every x?

CONDITIONAL STATEMENTS

Example 3a. Translate R(x) to symbols, using the statements `P(x): x is prime, and S(x): x is a perfect square.`

R(x): If *x* is prime then *x* is not a perfect square.

Ques: Is R(x) true or false? In fact, very often when we encounter an implication, there is an implied universal quantifier in front.

Definition. If *P(x)* and *Q(x)* are open sentences, then $P(x) \Rightarrow Q(x)$ is interpreted to mean $\forall x,\ P(x) \Rightarrow Q(x)$.

Example 3 (cont'd): b. Translate to symbols, using the set of even numbers E = {2,4,6,8,10,...}, and the set of prime numbers F = {2,3,5,7,11, …}.

Every even integer greater than 2 is the sum of two primes.

NOTE: Two alternatives: $\forall x \in E, \exists p,\ q \ \in F,\ x = p + q$

$(x \in S) \Rightarrow (\exists p,\ q \ \in F,\ x = p + q)$

Fact. If S is a set and Q(x) is an open sentence, then the following statements mean the same thing:

1. $\forall x \in S,\ Q(x)$
2. $(x \in S) \ \Rightarrow Q(x)$

?? Importance of looking at MEANING rather than WORDS

?? Ex: Translate to symbols:

a. At least one of the integers x and y is even.

b. The integer x is even, but the integer y is odd.

Beware - in a, we should use "or" to connect even though the word "and" appears

In b, we use "and" to connect although the word that appears is "but".

NEGATING STATEMENTS

Example. Find the negation of the following statement R.

R: You can solve it by factoring or with the quadratic formula.

R is two statements connected by "or": (you can solve it by factoring) v (you can solve by the quad fmla).

If this is NOT true, then what?

NOTE: let P: you can solve by factoring, Q: you can solve by quadratic formula. Consider negation - this is exactly DeMorgan's law!

Example 4. Find the negation of the sentence, both in symbols and in words.

a. R: x and y are both odd.
b. S: All prime numbers are odd.
c. The square of every real number is non-negative.
d. For every real number x, there is a real number y for which $y^3 = x$.
e. If x is odd, then x^2 is even.

Rules for **negating quantifiers**.
1. $\sim (\forall x \in S,\ P(x)) \ = \ \exists x \in S,\ \sim P(x)$
2. $\sim (\exists x \in S,\ P(x)) \ = \ \forall x \in S,\ \sim P(x)$

Rule for **negating conditional statements**.
3. $\sim (P \Rightarrow Q) \ = \ P \wedge \sim Q$

Finally, consider the negation of $P \Rightarrow Q$. $\sim (P \Rightarrow Q)$ says "$P \Rightarrow Q$ is *false*". The only way $P \Rightarrow Q$ can be false is if P is true and Q is false.

LOGICAL INFERENCE, THE ROLE OF LOGIC
So far almost all of our study of logic has involved understanding the meaning of certain words, and how they are used to form complex statements. We have not really addressed the issue of "proof" -- which is the process of making a sequence of statements, one after the other, according to logical rules (rules of inference). The reason is that, once the meaning of the individual statements is clear, the process of moving from one statement to another is very natural - not usually the source of confusion. We will NOT be testing you on the rules of inference, but I will give a few examples.

Suppose we know that a statement of the form $P \Rightarrow Q$ is true. Does this tell us whether or not P is true, or Q is true? *Consider "If you are Prof. Reitz, then you have long hair."* NO! They might both be false, for example. BUT if we know that P is true, *and* we know that $P \Rightarrow Q$ is true, THEN we can conclude that Q must be true. We write this rule in this fashion:

$$\begin{array}{l} P \Rightarrow Q \\ P \qquad . \\ \hline Q \end{array}$$

Some of the valid rules of inference:

$$\begin{array}{l} P \Rightarrow Q \\ P \\ \hline Q \end{array} \qquad \begin{array}{l} P \Rightarrow Q \\ \sim Q \\ \hline \sim P \end{array} \qquad \begin{array}{l} P \vee Q \\ \sim P \\ \hline Q \end{array}$$

$$\begin{array}{l} P \\ Q \\ \hline P \wedge Q \end{array} \qquad \begin{array}{l} P \wedge Q \\ \hline P \end{array} \qquad \begin{array}{l} P \\ \hline P \vee Q \end{array}$$

Lecture 8 - 3.1 Counting Lists, 3.2 Factorials

list, entry, length, empty list, multiplication principle, repetitive and non-repetitive lists, factorial

FINAL LOGIC TOPIC: NEGATING STATEMENTS
Example. Find the negation of the following statement R.
R: You can solve it by factoring or with the quadratic formula.
R is two statements connected by "or": (you can solve it by factoring) v (you can solve by the quad fmla). If this is NOT true, then what?
NOTE: let P: you can solve by factoring, Q: you can solve by quadratic formula. Consider negation - this is exactly DeMorgan's law!

Example 4. Find the negation of the sentence, both in symbols and in words.
a. R: x and y are both odd.
b. S: All prime numbers are odd.
c. The square of every real number is non-negative.
d. For every real number x, there is a real number y for which $y^3 = x$.
e. If x is odd, then x^2 is even.

Rules for **negating quantifiers**.
1. $\sim (\forall x \in S,\ P(x)) = \exists x \in S,\ \sim P(x)$
2. $\sim (\exists x \in S,\ P(x)) = \forall x \in S,\ \sim P(x)$
Rule for **negating conditional statements**.
3. $\sim (P \Rightarrow Q) = P \wedge \sim Q$

Finally, consider the negation of $P \Rightarrow Q$. $\sim (P \Rightarrow Q)$ says "$P \Rightarrow Q$ is *false*". The only way $P \Rightarrow Q$ can be false is if P is true and Q is false.

DIFFICULTY OF COUNTING THINGS: Amazing Race IKEA challenge, start at 2:45 -- http://www.youtube.com/watch?v=Or8Qs9mc7o8

Today we revisit the most basic kind of mathematics, counting. Much of our counting will be concerned with lists.

Definition. A **list** is an ordered sequence of objects (called **entries** in the list). The **length** of a list is simply the number of entries. A list is typically written enclosed in parentheses, with objects separated by commas. Ex: (a,b,c,d,e) is a list of length 5.
NOTE: order matters in a list, so $(a, b, c, d, e) \neq (b, d, e, c, a)$

NOTE: objects can be repeated in a list: (a, a, b, c) is a list of length 4.

QUES: Is it possible for a list to have length 0?
Definition. The **empty list**, or list with no entries, is the only list with length 0.

Example 1: Make a list of length 3 in which the first entry comes from the set $\{a, b, c\}$, the second entry comes from the set $\{3, 4\}$, and the third entry comes from the set $\{a, x\}$.
Collect examples from the class.
In general, we will be very concerned with counting the number of different lists that are possible, given certain restrictions (like those in example 1).

Example 2: How many lists are there that satisfy the conditions of Example 1?
TREE DIAGRAM: Sketch a tree diagram showing how to build every such list.

Can we make a general rule for the number of possible lists?

Multiplication Principle. Suppose in making a list of length *n* that there are $a_1$possible choices for the first entry, a_2 possible choices for the second entry, $a_3$possible choices for the third entry, and so on. The the number of different lists that can be made in this way is the product $a_1 \cdot a_2 \cdot a_3 \cdot ... \cdot a_n$

Example 3: A standard license plate consists of three letters followed by four numbers. For example JRB-4412 and MMX-8901 are two different standard license places. How many different standard license plates are possible?

Note that in some lists, we are allowed to repeat entries: For example, BAB-1112 is a perfectly good license plate, although the entries 'B' and '1' are both repeated. In some situations, however, we may look at lists in which repetition is not allowed. For example, suppose we put the names of everyone in the class in a hat, and we make a list of people in the class by drawing the names out of the hat one by one - each person will appear just once in the list, with no repetition.

Example 4: Consider making lists from the set {A, B, C, D, E, F, G}. How many length-4 lists are possible if:
a) repetition is allowed? *"repetitive lists"*
b) repetition is NOT allowed? *"non-repetitive lists"*
c) repetition is NOT allowed and the list must contain an *E*?
d) repetition is allowed and the list must contain an E?

NOTE: You may be more familiar with the phrases "with replacement" (= repetitive list), and "without replacement" (= non-repetitive list).

For c), consider 4 cases - in which E appears as entry 1, 2, 3, and 4 resp.. NOTE: We don't want to count any lists twice -- do these cases overlap at all?

For d), consider all lists, then subtract those with NO E's. NOTE: a strategy like c) is tempting, but there is overlap between lists with E in various positions.

FACTORIALS. As we work more with non-repetitive lists, we'll need some more mathematical tools to simplify notation. You may already have been exposed to the factorial function - here, I want you to pay special attention to the **definition** of factorial - it may be different from the **formula** that you are used to (although it gives the same answer)

Definition. If n is a non-negative integer, then ***n* factorial,** written $n!$, is the number of non-repetitive lists of length n that can be made from n symbols.

Example 5. **Using the definition**, calculate 3!, 2!, 1!, 0!. What is 4! ?

RULE: 0! = 1, 1! = 1, and for $n > 1, n! = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$

What if we making a non-repetitive lists from a set of 8 symbols, but the list is only allowed to have length 5? How many entries are possible?
First calculate. Then show how this can be obtained using the factorial function.

Theorem. The number of non-repetitive lists taken from a set of n symbols, with length k, is given by $\frac{n!}{(n-k)!}$

EXERCISES.
Example 6. This problem involves making lists of length 7 from the set {0, 1, 2, 3, 4, 5, 6, 7}.
a) How many such lists are there if repetition is allowed?
b) How many such lists are there if repetition is allowed *and* the first three entries must be odd?
c) How many such lists are there if repetition is not allowed?
d) How many such lists are there if repetition is not allowed *and* the first three entries must be odd?
e) How many such lists are there in which repetition **is** allowed, and the list **must** contain at least one repeated number?

Example 7. a) For which values of n does $n!$ have n or fewer digits?
b) Using only pencil and paper, calculate $\frac{201!}{199!}$
Example 8. a) How many 6-digit positive integers are there in which there are no repeated digits, and all digits are odd?
b) How many 4-digit positive integers are there in which there are no repeated digits, and all digits are even?
NOTE: The number 0426 is NOT considered a 4-digit positive integer, since it is equal to 426.

Example 9. There are two 0's at the end of 10!=3,628,800. Determine the number of 0's at the end of 100!.

Lecture 9- 3.3 Counting Subsets, 3.4 Pascal's Triangle and the Binomial Theorem

NOTE: If possible, try to return the written work from Chp 4 & 5 PRIOR to Exam #2 (so they can get some feedback on proofs)

n choose *k*, Pascal's Triangle, Binomial Theorem

Last time we talked about counting *lists*. Today we talk about counting *subsets*.

CLASS:
Example 1. In this problem we work with the set $A = \{a, b, c, d, e\}$
a) Write down at least 5 different length-3 *lists* taken from the set A. How many such lists are there?
b) Write down at least 5 different *subsets* of A of cardinality 3. How many such subsets are there?

Collect sample answers to a) on the board, then the total 120 (from the formula). Now collect as many answers to b) as possible - how many are there?
QUESTION: What's the difference between ***lists*** *and* ***subsets****?*
We have a formula for the number of lists. Now we're going to try to use that to find a formula for the number of subsets.

Length-3 lists taken from A

abc	abd	abe	acd	ace	ade	bcd	bce	bde	cde
acb	adb	aeb	adc	aec	aed	bdc	bec	bed	ced
bac	bad	bae	cad	cae	dae	cbd	cbe	dbe	dce
bca	bda	bea	cda	cea	dea	cdb	ceb	deb	dec
cba	dba	eba	dca	eca	eda	dcb	ecb	edb	edc
cab	dab	eab	dac	eac	ead	dbc	ebc	ebd	ecd

Notice that the first row actually collects all 3-element **subsets** of A. Underneath each entry is simply the rearrangements of that set, giving different lists.
QUESTION: If we know the total number of LISTS, how can we figure out the total number of SUBSETS? *When we count the number of lists, we are counting each subset multiple times.*
In the box, how many times does each subset show up? *Once for each rearrangement of the 3 elements.*
How many rearrangements are there for a set with 3 elements? n!

Definition. If *n* and *k* are integers, then $\binom{n}{k}$ is the number of k-elements subsets from a set with *n* elements. $\binom{n}{k}$ is also written C(n,k), or ${}_nC_k$, and read "*n* choose *k*".

CLASS:
Example 2. How many 4-element subsets does the set {a,b,c,d,e,f,g} have? *To find the answer, consider the following:*

a) How many lists are there of length 4 from this set?
b) For each subset with 4 elements, how many times is it repeated among the lists of length 4?

Formula. If $n, k \in \mathbb{Z}$ and $0 \leq k \leq n$, then $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Otherwise $\binom{n}{k} = 0$

CLASS:
Example3.
a) How many 2-element subsets can be chosen from a set with 6 elements?
b) Determine $|\{X \subseteq B : B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \text{ and } |X| = 5\}|$
c) A department consists of 5 men and 7 women. From this department you select a committee with 3 men and 2 women. In how many ways can this be done?

QUESTION: Suppose we increase the size of the original set by 1. What happens to the number of k-element subsets?
We know from our work above that $\binom{5}{3} = 10$. *List them!* What happens if we throw another element into the set A? Now, when we build 3-element subsets, we get the following:
1. keep the subsets of size 3 - how many are there? $\binom{5}{3}$.
2. Take a subset of size 2, and throw in the new element. How many? $\binom{5}{3}$
Putting this together, we get: $\binom{6}{3} = \binom{5}{3} + \binom{5}{2}$

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

We can use this rule to organize these numbers, as follows:
Sketch Pascal's Triangle. Try writing out the row for $\binom{5}{k}$ *first? Then move down to the next row? Do this with the bin coe's, then with the actual numbers.*
Complete the first 3-4 rows, ask the class to fill in the next row.
Ask the class to find $\binom{6}{4}$ using Pascal's triangle

Pascal's Triangle

$$
\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0} \quad \binom{1}{1} \\
\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2} \\
\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3} \\
\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4} \\
\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5} \\
\binom{6}{0} \quad \binom{6}{1} \quad \binom{6}{2} \quad \binom{6}{3} \quad \binom{6}{4} \quad \binom{6}{5} \quad \binom{6}{6} \\
\binom{7}{0} \quad \binom{7}{1} \quad \binom{7}{2} \quad \binom{7}{3} \quad \binom{7}{4} \quad \binom{7}{5} \quad \binom{7}{6} \quad \binom{7}{7} \\
\cdots \quad \vdots \quad \cdots
\end{array}
\qquad
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
\cdots \quad \vdots \quad \cdots
\end{array}
$$

AN UNEXPECTED CONNECTION: RAISING BINOMIALS TO POWERS.

Example 4: Multiply, and simplify your answer: $(x + y)^3$.

Examine coefficients - they match the row in Pascal's Triangle with n=3.

Example 5: Multiply, and simplify your answer: $(x + y)^6$

Binomial Theorem. If *n* is a non-negative integer, then the coefficients of the expanded form of $(x + y)^n$ match the *n*th row in Pascal's Triangle. In particular, the term containing $x^{n-k}y^k$ has coefficient $\binom{n}{k}$. Alternatively: $(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + ... + \binom{n}{n-1}x^1y^{n-1} + \binom{n}{n}y^n$.

Example 6. What is the coefficient of the term x^5y^3 in the expansion of $(x + y)^8$?

Lecture 10 - Chapter 4

NOTE: If possible, try to return the written work from Chp 4 & 5 PRIOR to Exam #2 (so they can get some feedback on proofs)
NOTE: Consider splitting this lecture into 2 days - one on definitions etc, the next introducing proof

Theorem, proof, definition, proposition, lemma, corollary, even, odd, parity, divides, divisor, multiple, *prime, composite, greatest common divisor, least common multiple, the division algorithm,* direct proof

Today we begin the main project of this course - proving things. It will help to keep in mind the meanings of three related words, *theorem, proof* and *definition*.

A **theorem** is a statement that is true, and has been proved to be true.
A **proof** of a theorem is a written verification that a theorem is definitely and unequivocally true.
A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word, phrase, or symbol

Proof is about communication.

A proof should be understandable and convincing to anyone with the requisite background knowledge. This includes an understanding of the mathematical words, phrases and symbols that appear. *It is of paramount importance that the person writing the proof and the person reading it agree on the exact meanings of all words and symbols used in the proof!* Because of this, definitions will be *extremely important* when completing proofs!

> Words that mean the same thing as “Theorem”, but are used in special ways:
> - a statement that is true (and proven), but is not as significant as a theorem is sometimes called a **proposition**.
> - a **lemma** is a theorem whose main purpose is to help prove another theorem (a “little theorem, used along the way”)
> - a **corollary** is a result that is an immediate consequence of a theorem or proposition (“a little something extra, that we get for free, having completed the theorem”)

It all comes down to the definitions.

DEFINITIONS.
A proof must be absolutely convincing - ambiguity must be avoided. We all must agree on the ***exact*** definitions of each term. In Chapter 1, we discussed the meanings of:
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\in$, $\subseteq$
and we’ll be using them throughout the rest of the book. In many cases, figuring out how to get started on a proof involves *going back to the definition* - this gives you something concrete to work with. This can

be especially important for common words that you understand intuitively! Before we start proving things, we're going to talk about concrete definitions for some terms you already know:

Definition. An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.
Definition. An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

Discuss - give examples of even and odd numbers, find the corresponding "a".

Definition. Two integers have the **same parity** if they are both even or both odd. Otherwise they have **opposite parity**.

CLARIFY: Defn's usually have form "xxx is **blank** if yyy", when we really mean "xxx is **blank** if and only if yyy"

Definition. Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

Definition. A natural number n is **prime** if it has exactly two distinct positive divisors, 1 and n.
Definition. A natural number n is **composite** if it factors as $n = ab$ where $a, b > 1$.

Definition. The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b. The **least common multiple** of non-zero integers a and b, denoted lcm(a,b), is the smallest positive integer that is a multiple of both a and b.

Question: If we add two integers, do we get an integer? What about subtract? What about multiply? Divide?
Fact. Suppose a and b are integers. Then so are $a+b$, $a-b$, and ab.

Two Facts *that we will accept (for now) without proof:*

Ex: How many times does 5 go into 32? What's the remainder?

Theorem (The Division Algorithm). Given integers a and b with $b>0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

What does it say? Basically, it says that we when we divide a by b it will go in a certain number of times q and leave a remainder r (which is less than b). Furthermore, the answer is unique - given a and b, there is only one pair of number q and r that will work.

Theorem. Every natural number greater than 1 has a unique factorization into primes.
Ex: what is the prime factorization of 12? Of 1176? (ANS: 12=2*2*3, 1176=2*2*2*3*7*7)

Do we define EVERYTHING? Not in this class -- here, there are some things that we accept and use freely. They include: addition, subtraction, multiplication, division, standard properties of arithmetic and algebra (for use in solving equations and simplifying expressions), the order "<" on various kinds of numbers, and so on. Here is another one:
?? Insert Section somewhere: WHAT AM I ALLOWED TO USE IN PROOFS:
Definitions given in class or in the book, plus
Basic mathematical knowledge including:
- the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and the meaning of $\in$, $\subseteq$
- arithmetic for numbers in the above sets, facts about addition, subtraction, multiplication, division, exponents, and so on
- algebra (for example for solving equations and simplifying expressions)
- the meaning of "<"

DIRECT PROOF.
OBSERVE: *Almost all theorems (but not all!) have the form "If P, then Q"*

Today, we look at the most basic way of proving a statement of the form:
Proposition. If P then Q.

We want to prove that such a statement is TRUE. *Recall truth table*. Notice that if P is false, then "If P then Q" is automatically true - so we don't have to worry about this case. In fact, the only case that concerns us is when P is true - we need to show that:
the condition of P being true, forces Q to be true also

Outline for Direct Proof
Proposition. If P, then Q.
Proof. Suppose P.
…
Therefore Q.

Proposition. If x is odd, then x^2 is odd.

Setup on board, leave blank space in middle: Proof. Suppose x is odd. (SPACE)... Therefore x^2 *is odd.*
All we have to do is fill in the middle!
*What does x being odd **mean**, anyway? USE THE DEFN*

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by the definition of odd number.

Now, how is it that we're going to conclude the final line? The only way we know how -by USING THE DEFN! Add penultimate step, add justification to final step:

$x^2 = 2b + 1$ for some $b \in \mathbb{Z}$.

Therefore x^2 is odd, by the definition of odd number.

NOTE: we are already using "a" to mean one number here - so we should use another letter "b" this time.

Now we just need to bring the two parts together. We have an expression for x, now lets calculate x^2.

Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.

So $x^2 = 2b + 1$, where b is the integer $b = 2a^2 + 2a$.

Take a look at the complete proof (rewrite it?).

Proposition. If x is odd, then x^2 is odd.

Proof. Suppose x is odd. Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by the definition of odd number. Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$, so $x^2 = 2b + 1$, where b is the integer $b = 2a^2 + 2a$. Therefore x^2 is odd, by the definition of odd number.

Proposition. Let *a*, *b* and *c* be integers. If $a|b$ and $b|c$, then $a|c$.

Give setup. Ask everyone to complete the middle individually? WRITE IT NEATLY! Then pair up, swap papers, read carefully. ASK QUESTIONS! Format for this?

OR

Pair up, work on it together?

USING CASES

Proposition. If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

First, is this even true? SCRATCH WORK: Try it for n=1,2,3,4,5,6….

Notice the calculation works differently depending on whether n is odd or even - if n is odd $(-1)^n = -1$*, if n is even* $(-1)^n = 1$. *In the proof, we examine these two cases separately. Setup like this*:

Proof. Suppose $n \in \mathbb{N}$. Then *n* is either odd or even. Consider these two cases separately.

Case 1. *n* is odd. Then…

Case 2. *n* is even. Then…

We often use the fact that a number is either even or odd (but not both) -- but this relies on our intuitive understanding. How can we prove it? The definitions of even and odd do not seem obviously connected in the same way…

Proposition. If a number is not even, then it is odd.

Proof. Use this as an opportunity to discuss Divison Algorithm.

Lecture 11 - Chapter 5: Contrapositive Proof

Contrapositive proof, congruence modulo n

?? START WITH THIS - TRY TO PROVE DIRECTLY?

Proposition 1. Suppose $x \in \mathbb{Z}$. *If* $x^2 - 6x + 5$ *is even, then x is odd.*

RECALL: What is the **contrapositive** of $P \Rightarrow Q$? $\sim Q \Rightarrow \sim P$. Are these equivalent? It is sometimes helpful to prove the contrapositive, instead of the original statement.

Outline for Contrapositive Proof
Proposition. If P, then Q.
Proof. Suppose $\sim Q$.
…
Therefore $\sim P$.

Proposition 1. Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then *x* is odd.

Proposition 2. Suppose $x, y \in \mathbb{Z}$. If 5 does not divide *xy*, then 5 does not divide *x* and 5 does not divide *y*.

CONGRUENCE
Definition. Given integers *a* and *b* and an $n \in \mathbb{N}$, we say that *a* and *b* are **congruent modulo n** if $n|(a - b)$. We express this as $a \equiv b \ (mod\ n)$.

Example 3. True or False?
a) $9 \equiv 1 \ (mod\ 4)$
b) $6 \equiv 10 \ (mod\ 4)$
c) $14 \equiv 8 \ (mod\ 4)$
d) $20 \equiv 4 \ (mod\ 8)$
e) $17 \equiv -4 \ (mod\ 3)$

NOTE: In practice, this means that a and b have the same remainder when divided by n.

Proposition 4. Let $a, b \in \mathbb{Z}$ and an $n \in \mathbb{N}$. If $a \equiv b (mod\, n)$, then $a^2 \equiv b^2\ (mod\, n)$.
(Direct Proof)

Proposition 5. Suppose $a, b \in \mathbb{Z}$ and an $n \in \mathbb{N}$. If $\sim (12a \equiv 12b\ (mod\, n))$, then $\sim\ (n|12)$.

?? Mathematical writing guidelines ??

Lecture 12 - Chapter 6: Proof by Contradiction

Proof by contradiction

? Is the number 1 even or odd? FACT. 1 is odd. We will accept this without proof, as we accept all basic mathematical knowledge.

Proposition. If $a, b \in \mathbb{Z}$ then $a^2 - 4b \neq 2$.
Suppose this is false - what would go wrong? Let's see.
Proof. Suppose the proposition is false.
Then there exist integers *a* and *b* for which $a^2 - 4b \neq 2$
Solve for a^2, conclude a is even, substitute 2c for a, divide to show 1 is even.
Therefore 1 is even. BUT we already know 1 is odd. Impossible!
Therefore the proposition must be true.

OBSERVE:
- we wanted to prove the proposition P was TRUE.
- we "imagined" the proposition was false - we *assumed* $\sim P$
- we proved a proposition *1 is even*, which conflicts with our prior knowledge *1 is odd*. In essence, we proved the statement $(1\ is\ odd) \wedge\sim (1\ is\ odd)$, which has the form $C \wedge\sim C$. Note that whether C is true or false, $C \wedge\sim C$ is FALSE. A statement like this, that cannot be true is called a **contradiction**.

Definition. A statement which cannot be true (all rows in the truth table are False) is called a **contradiction**.

LOGICAL VALIDITY OF PROOF BY CONTRADICTION
Why is this line of reasoning valid, and why does it prove P?
NOTE: To see this, first consider the statement $\sim P \Rightarrow (C \wedge\sim C)$. First, this is the statement we proved above (we assumed $\sim P$, and proved $(C \wedge\sim C)$). Second, look at the truth table for $\sim P \Rightarrow (C \wedge\sim C)$. Note that it is true ONLY when P is true -- that is, it logically equivalent to P.

P	C	$\sim P$	$C \wedge \sim C$	$(\sim P) \Rightarrow (C \wedge \sim C)$
T	T	F	F	**T**
T	F	F	F	**T**
F	T	T	F	**F**
F	F	T	F	**F**

Outline for Proof by Contradiction
Proposition. P.

Proof. Suppose $\sim P$.
…
Therefore $C \wedge \sim C$.

NOTE: Unlike our other proof methods, Proof by Contradiction works for statements of ANY form (not just $P \Rightarrow Q$*).*
NOTE: When embarking on a proof by contradiction, it's not necessarily clear "what the contradiction will be" -- that is, what is the statement C for which we prove $(C \wedge \sim C)$*.*

We can prove some very significant mathematical facts with this method!
?Sketch square of length 1 -- Greeks considered this!

Theorem. The number $\sqrt{2}$ is irrational.

Definition. A real number *x* is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$.

A real number *x* is **irrational** if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

Proof. Suppose false.
2=a/b for some integers a,b
Let this fraction be fully reduced.
Then a *and* b *are NOT both even.*
Show a^2 is even, therefore a is even (this was Chapter 5, exercise 1 in the book).
plug in a=2c, square & cancel 2, to show b^2 is even, therefore b is even.
So a and b ARE both even. Contradiction.

Proposition: $\sqrt{10}$ is irrational.

Fact. Every natural number greater than 1 has a unique factorization into primes.
Example 1: Factor 1176 into primes.
$(1176 = 2^3 * 3 * 7^2)$

Theorem. There are infinitely many prime numbers.
Proof. Suppose there are finitely many. Make a list of them! Discuss the list - what is p1, p2, p3, etc, up to pn. Take the product and add 1, call it *a*. Note that *a* can be factored into primes -- so there is at least one prime *p_k* divides it, a=c*p_k, for some integer c. Divide both sides by p_k -- note that the right side is an integer plus 1/p_k, which is NOT an integer. Therefore c is not an integer. Contradiction.

NOTES ON USING PROOF BY CONTRADICTION:
- To prove a statement of the form $P \Rightarrow Q$ using contradiction, start by assuming $P \wedge \sim Q$ (and then prove $C \wedge \sim C$).
- To prove a statement of the form $\forall x P(x)$ using contradiction, start by assuming $\exists x \sim P(x)$ (and then prove $C \wedge \sim C$).

Lecture 16 - Chapter 7: If-and-only-if proofs, existence proofs

division algorithm, if-and-only-if proofs, existence proofs

Recall: Theorem (The Division Algorithm). Given two integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

NOTE: If we divide ANY integer a by 2, we either have a remainder of 0 or 1. Thus every integer a is either of the form $a = 2b$ or $a = 2b + 1$.
Example 1: What are the possible remainders when an integer a is divided by 5? In which cases does 5 divide a? Complete the following: *Any integer can be written in one of the following 5 forms:*

____

GROUPS (assign groups)
Proposition. If n is an integer, then $4|n^2$ or $4|(n^2 - 1)$.
*HINT: What are the different remainders when **n** is divided by 4? These give you cases to consider.*

Many of the proofs we have considered have been of statements of the form $P \Rightarrow Q$. What happens if, instead, we need to prove a statement $P \Leftrightarrow Q$?

QUES: What does $P \Leftrightarrow Q$ mean?

Outline for If-and-only-if Proof

Proposition. $P \Leftrightarrow Q$
Proof.
[Prove $P \Rightarrow Q$ using direct, contrapositive, or contradiction proof.]
[Prove $Q \Rightarrow P$ using direct, contrapositive, or contradiction proof.]

NOTE: This is really like writing two proofs in one. It is important that you start a new paragraph when you finish the first part and start the second. Since $Q \Rightarrow P$ is the *converse* of $P \Rightarrow Q$, we often use the word *Conversely* to begin the second part - this is a good reminder to the reader that one section is done and another beginning (you can also restate what you are trying to prove at this point).

Proposition. An integer n is even if and only if n^2 *is even.*

GROUPS:
Prove without using Euclid's Lemma:
Proposition. For an integer a, $3|a^2$ if and only if $3|a$.

OPTIONAL ADDITIONAL PROBLEM:
Proposition. Suppose a and b are integers. Then $a \equiv b (mod\ 6)$ if and only if $a \equiv b (mod\ 2)$ and $a \equiv b (mod\ 3)$.

Existence proofs. How do we prove a statement of the form $\exists x\ P(x)$? All we have to do is actually produce an example and show that it satisfies P(x). Sometimes this is easy, sometimes hard!

Proposition. There exists an even prime number.

Proof. Consider the number 2. 2 is an even number, since $2 = 2 \cdot 1$ for the integer 1 (by the definition of even number). 2 is divisible by exactly two different natural numbers, 1 and 2, and so 2 is prime (by the definition of prime number). Therefore 2 is an even prime number.

GROUPS:
Proposition. There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.
HINT: 1729
HINT2: 1,12 and 9,10

??Proposition. There exist irrational numbers x and y such that x^y is rational.

Lecture 17 - Chapter 8: Proofs involving sets

NOTE: Need 30 min class time for group work on projects on 10/30/14

PROJECT GROUP WORK - 30 min - see "PROJECT GROUP ASSIGNMENT #1"
Assign groups - see spreadsheet/printout

Many proofs involve sets of one kind or another - today we talk about common situations that show up when proving things about sets.

Review: Main definitions from Chapter 1
Defn. $A \times B = \{(x, y) : x \in A, y \in B\}$
Defn. $A \cup B = \{x : (x \in A) \vee (x \in B)\}$
Defn. $A \cap B = \{x : (x \in A) \wedge (x \in B)\}$
Defn. $A - B = \{x : (x \in A) \wedge (x \notin B)\}$
Defn. $\overline{A} = U - A$
Defn. $P(A) = \{X : X \subseteq A\}$

How to prove $a \in A$.
In general, this involves showing that the given object a satisfies the definition of the set A.

Example. a. If $a = \{2, 12, 17\}$ and $A = \{X \in P(\mathbb{N}) : |X| = 3\}$, then prove $a \in A$.
b. If $C = \{3x^3 + 2 : x \in \mathbb{Z}\}$, then prove $-22 \in C$.

a. NOTE: need to show two things - that a is in P(N), and that the size is 3.
b. What does this set look like? List some of the members.

How to prove $A \subseteq B$.
Recall that $A \subseteq B$ means that every member of A is also a member of B.

To prove $A \not\subseteq B$, simply find a particular example a such that $a \in A$ but $a \notin B$.

How to prove $A \subseteq B$
To prove $A \subseteq B$, prove the statement: if $a \in A$, then $a \in B$.

Direct Proof	**Contrapositive Proof**
Proof. Suppose $a \in A$. … Therefore $a \in B$. Thus $a \in A$ implies $a \in B$, and so $A \subseteq B$.	*Proof.* Suppose $a \notin B$. … Therefore $a \notin A$. Thus $a \notin B$ implies $a \notin A$, and so $A \subseteq B$.

Example 8.5. Prove that $\{x \in \mathbb{Z}: 18|x\} \subseteq \{x \in \mathbb{Z}: 6|x\}$

Example 8.8. Prove that if A and B are sets, then $P(A) \cup P(B) \subseteq P(A \cup B)$.

NOTE: "Union" - split into cases, one where x in first, one in second.

NOTE: "Intersection" - doesn't need cases - instead, assume x is in both.

Example 8.9. Suppose that A and B are sets. If $P(A) \subseteq P(B)$ then $A \subseteq B$.

How to prove A=B

Proof.

[Prove $A \subseteq B$.]

[Prove $B \subseteq A$.]

Therefore, since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$.

Example 8.12. Given sets A, B and C, prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Lecture 17 - Chapter 9: Disproof

Example. Is each proposition true or false?

1. Every even natural number is the sum of two odd natural numbers.
2. Every even natural number is the sum of two perfect squares.
3. Every even natural number is the sum of two primes.

So far, all our proofs have had the same general setup: You are given a proposition, and you prove it is true. What if you were actually given a false proposition? You will never be able to prove that it's true - BUT you might be able to prove that it's false. Does this actually happen? YES! Consider the following classification of all statements:

THREE TYPES OF STATEMENTS:

Known to be true (Theorems & propositions)	**Truth unknown** (Conjectures)	**Known to be false**
Examples: • Pythagorean theorem • Fermat's last theorem (Section 2.1) • The square of an odd number is odd. • The series $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges.	Examples: • All perfect numbers are even. • Any even number greater than 2 is the sum of two primes. (Goldbach's conjecture, Section 2.1) • There are infinitely many prime numbers of form $2^n - 1$, with $n \in \mathbb{N}$.	Examples: • All prime numbers are odd. • Some quadratic equations have three solutions. • $0 = 1$ • There exist natural numbers a, b and c for which $a^3 + b^3 = c^3$.

Definition. A statement whose truth is unknown is called a **conjecture.**

Most mathematicians spend their time working on the middle type - trying to prove something is true, or prove it's false.

Definition. When we prove a statement P is false, we call this a **disproof** of P.
How to Disprove P: Prove $\sim P$.

CHEAT SHEET: How to disprove a statement of the form:

- To disprove $\forall x\, P(x)$, give an example of an x that makes $P(x)$ false (such an x is called a **counterexample**).
- To disprove $P(x) \Rightarrow Q(x)$, give an example of an x that makes $P(x)$ true but $Q(x)$ false.
- To disprove $\exists x\, P(x)$, prove the statement $\forall x, \ \sim P(x)$.
- To disprove P by contradiction, assume P is true and deduce a contradiction $C \wedge \sim C$.

Example. Prove or disprove each conjecture.

Conjecture. For every $n \in \mathbb{Z}$, the integer $f(n) = n^2 - n + 11$ is prime.
HINT: Try it for a few different numbers n.

Conjecture. If A, B and C are sets, then $A - (B \cap C) = (A - B) \cap (A - C)$.
HINT: It might help to look at Venn diagrams for the expressions on each side of the equation.

Conjecture. If A and B are sets, then $P(A) - P(B) \subseteq P(A - B)$.

Lecture 18 & 19 - Chapter 10: Induction

Induction, basis step, inductive step, inductive hypothesis

NOTE: After teaching this the first time, I suggest: spending 3 days on Induction.
Day 1: Overview - what do we use induction for? "Mr. Reitz loves" example, definition of Induction, first proof (sum of first n odd numbers is n^2). Maybe introduce second example (base case n=0)
Day 2: Quick review. Introduce next example, NOTE base case . Group work - up to 3 examples.
Day 3: Strong induction.

Today we look at an idea called mathematical induction - you may have used for it.

What kind of statements do we use induction for?

Given statement P(n) involving number n, want to prove P(n) is true for every natural number. Thus induction is used to prove statements of the form $\forall n\ P(n)$.
NOTE: not ALWAYS needed.

Example: $\forall n,\ n^2 = (n+1)^2 - 2n - 1$.

DO YOU BELIEVE IT? (how would we test it?)
How can we prove it? ALGEBRA - works regardless of which number n is involved.
Why can't we always use this method? Sometimes, we have expressions that we CANNOT SIMPLIFY USING ALGEBRA (for example, sums!)

Two parts to induction: First, the big idea of induction - how does it work? What's the outline of a proof? Second, the details involved in an actual proof (often algebra!).

1. What's the big idea?

We're going to talk about a sorta silly question:

Example: Which numbers does Mr. Reitz love?

Hint: I'm not going to give you a list! BUT I will give you the following two Rules to work with:

P(n): Mr. Reitz loves the number *n*.
Rule 1: $P(1)$ is true *(that is, Mr. Reitz loves the number 1)*.
Rule 2: $P(k) \Rightarrow P(k+1)$ *(that is, if Mr. Reitz loves a number k, then he also loves the number k+1)*.

QUESTIONS:

1. Does Mr. Reitz love the number 1? How do you know?
2. Does he love the number 2? How do you know?
3. Does he love the number 5? How do you know? *Prove that he loves the number 5.*
4. Could we still prove that Mr. Reitz loves the number 5 if we were missing Rule 2? What if we were missing Rule 1?

5. Does Mr. Reitz love the number 20? What about 50? What about 4,102,987?
6. Which numbers does Mr. Reitz love?

*From Rules 1 and 2, it follows that Mr. Reitz loves **every** natural number.*

GENERAL SETUP FOR PROOF BY INDUCTION

We want to prove that some statement P(n) (sometimes written S_n) is true for all natural number n, that is, we want to prove a statement of the form:

$\forall n \in \mathbb{N},\ P(n)$

In the above example, *P(n): Mr. Reitz loves the number n.*

If, for whatever reason, this is difficult or impossible to prove directly, then we can prove it **by induction**:

Outline for Proof by Induction

Proposition. $\forall n \in \mathbb{N},\ P(n)$ *Proof.* **Base step.** Prove $P(1)$ **Inductive step.** Prove that for any given natural number k, $P(k) \Rightarrow P(k+1)$. It follows by mathematical induction that for every n, *P(n)* is true.

Definition. **Mathematical induction** (or simply **induction**) is a method for proving a statement of the form $\forall n \in \mathbb{N},\ P(n)$, by proving two associated statements: 1. *P(1)* and 2. for any k,$P(k) \Rightarrow P(k+1)$.

The case P(1) is called the **basis step** or **base step**.

The case $P(k) \Rightarrow P(k+1)$ is called the **inductive step**.

The assumption (in the inductive step) that $P(k)$ is true is called the **inductive assumption**.

WHY DO WE NEED INDUCTION?

Conjecture: The sum of the first n odd numbers is equal to n^2.

Try it for n=1,2,3,4, etc.

Make a chart:

n	sum of the first n odd numbers	
1	1	1
2	1+3=	4
3	1+3+5=	9
4	1+3+5+7=	16
...	...	

n	$1 + 3 + 5 + 7 + ... + (2n - 1) =$	n^2

Proposition. $\forall n \in \mathbb{N},\ 1 + 3 + 5 + ... + (2n - 1) = n^2$

NOTE: P(n): $1 + 3 + 5 + ... + (2n - 1) = n^2$
Proof. Base step. First we show that it is true for n=1. P(1): 1=1^2, clearly true.
Inductive step. For a given natural number *k*, suppose P(k) is true.
...
Therefore P(k+1) is true.
It follows by induction that $\forall n \in \mathbb{N},\ 1 + 3 + 5 + ... + (2n - 1) = n^2$

Proposition. If *n* is a non-negative integer, then $5|(n^5 - n)$
NOTE: Here, the basis step involves n=0, not n=1 - that's fine!

Proposition. $\forall n \in \mathbb{N},\ 4|(5^n - 1)$

Proposition. If $n \in \mathbb{N}$, then $(1 + x)^n \geq 1 + nx$ for all $x \in \mathbb{R}$ with $x > -1$.
Review some rules of inequalities? Can add/subtract both sides, multiply/divide by positive quant, can make large side larger, small side smaller

Proposition 10.1. Suppose $a_1, a_2, a_3, ..., a_n$ are *n* integers, where $n \geq 2$. If *p* is prime and $p|a_1 \cdot a_2 \cdot a_3 \cdot ... \cdot a_n$, then $p|a_i$ for at least one of the a_i.
NOTE: The base case is Euler's lemma -- do not ask class to prove, just refer to it (if we want to prove it, we need gcd, and fact: if p does NOT divide a then gcd(p,a)=1. Also need Proposition 7.1 (p124): then there are k,l s.t. 1=pk+al.)

Lecture 20 - Chapter 10 cont'd: Strong Induction

Strong induction

MAT 2440 text may be a good source for Strong Induction problems (rec by Adam Ibrahim)

Recursion is a method for defining a sequence of numbers by giving one or more initial values (base cases), together with a rule for generating new members of the sequence from past members (the inductive case)

Example. Consider the sequence of numbers $B_1, B_2, B_3, B_4, ...$ defined by the following three rules:

a. $B_1 = 4$

b. $B_2 = 12$

c. $for\ n \geq 3,\ B_n = B_{n-1} - 2B_{n-2}$

Write down the first few terms of Bn
Rule c is called a ***recursive*** *definition. Recursion is a method for* ***defining*** *things, induction is a method for* ***proving*** *things. Recursion and induction go together nicely!*

Proposition. For all n, $4|B_n$.
Proceed by induction. Where does it fail?

Sometimes it is the case that, in order to prove P(k+1), we need to rely not just on P(k) but also on earlier instances (for example, P(k-1)). In this case, the inductive hypothesis of P(k) is not enough. When this occurs, we rely on an alternative technique called **strong induction**. The only difference is that our inductive assumption includes not just P(k), but also P(1), P(2), P(3),... up to P(k).

Outline for Proof by Strong Induction

> Proposition. $\forall n \in \mathbb{N},\ P(n)$
> *Proof.*
> **Base step.** Prove $P(1)$ *(or the first several P(n), as necessary)*
> **Inductive step.** Prove that for any given natural number k,
> $(P(1) \wedge P(2) \wedge P(3) \wedge ... \wedge P(k)) \Rightarrow P(k+1)$.
> It follows by mathematical induction that for every n, *P(n)* is true.

Proposition. For all n, B_n is divisible by 4.
Proceed by induction. Where does it fail?

Definition. The Fibonacci sequence is the sequence of numbers F_n which is defined by: $F_1 = 1,\ F_2 = 1$, and $for\ n \geq 3,\ F_n = F_{n-1} + F_{n-2}$

Write down the first few terms in the sequence. 1, 1, 2, 3, 5, 8, 13, 21, …

Now consider $(F_{n+1})^2 - F_{n+1}F_n - (F_n)^2$

Proposition. For every natural number *n*, $(F_{n+1})^2 - F_{n+1}F_n - (F_n)^2 = (-1)^n$

Proposition. *The sum of the squares of the first n Fibonacci numbers is equal to* $F_n \cdot F_{n+1}$.

$1^2 + 1^2 + 2^2 + ... + (F_n)^2 = F_n \cdot F_{n+1}$

MORE EXAMPLES:

Proposition: If n is an integer greater than 1 then n can be written as a product of primes *(HINT: Consider two cases, when n+1 is prime, and when it is composite)*

Proposition: Every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.

Proposition: Consider a game in which two players take turns removing any positive number of matches they want from one of two piles of matches. The player who removes the last match wins the game. Show that if the two piles contain the same number of matches initially, the second player can always guarantee a win.

Proposition: the Euler characteristic (χ=V−E+F, where V, E, and F are the number of vertices, edges, and faces, including the exterior face, of the graph) of a planar graph is always 2.

CLASS:

Proposition. if $n \in \mathbb{N}$, then $12|(n^4 - n^2)$.

NOTE: It's tough because, from P(k), adding the correct terms to obtain P(k+1) doesn't give something divisible by 12. BUT if we start earlier - from P(k-5) - then it works.

Proposition. if $n \in \mathbb{N}$, then $12|(n^4 - n^2)$.
HINT: prove P(n-5)->P(n+1)

Defn: graph, tree,
Proposition. If a tree has *n* vertices, then it has *n-1* edges.

Lecture 22 - Sec 11.0, 11.1

Relations

In your math education so far, some ideas have been very far-reaching - showing up in almost every class: numbers. Variables. Functions. Other ideas are very specific, show up in one (or a few) classes but not much farther -- the chain rule, the quadratic formula, etc. Today we are going to talk about one of the "big ideas". It's a way of looking at things you've been studying for a long time, things that have a appeared in every math class you've ever taken, but you may not have ever noticed how these ideas are similar to each other. The idea is called **relations**.

Example. A relation is just a way of describing how things are related to each other. For example:

a. $5 < 7$ b. $-3 \geq -14$ c. $y = x^2$ d. $a \in A$ e. $\sqrt{2} \notin \mathbb{Z}$
f. $A \subseteq B$ g. $3|24$ h. $5 \equiv 21 \ (mod\ 4)$ i. $4 \neq 3$

Pretty much all of mathematics is about one kind of relation or another. (*Much of algebra is studying how we can preserve the "=" relation, while manipulating expressions).* Today we are going to take step back from studying individual relations and start to look at expressions as a whole.

Example. Consider the set $A = \{1, 2, 3, 4, 5\}$, and the relation '<' (less than). Make a complete list of correct comparisons of members of A according to '<'. *(for example:* $1 < 2$, $2 < 5$, $3 < 4$, *etc.).*

Note that each use of '<' involves two numbers -- and as long we know that we are talking about 'less than', we don't really need to write '<' each time. Let's turn this list into a SET, by making it a set of ordered pairs.

Consider the set $R = \{ (1, 2),\ (2, 5),\ (3, 4),\ \dots \}$
The set R tells us everything about the < relation on A. If we didn't know the meaning of <, but we knew how to use the set R, we could still solve problems involving <.
a. How could we use the set R to determine whether 3<4?
b. How could we use the set R to determine whether 5<2?

FACT: The set R, which is a subset of $A \times A$, completely describes relation < for A.

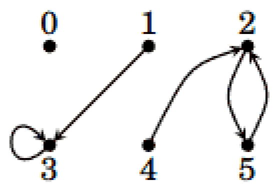
Definition. A **relation** on a set A is a subset $R \subseteq A \times A$. We often abbreviate the statement $(x, y) \in R$ as xRy. The statement $(x, y) \notin R$ is abbreviated $\sim xRy$ or $x \not{R} y$.

Example. Let $A = \{1, 2, 3, 4\}$, and consider the set
$R = \{(1, 1), (2, 1), (2, 2), (3, 3), (3, 2), (3, 1), (4, 4), (4, 3), (4, 2), (4, 1)\} \subseteq A \times A$.
1. True or false: a. 1R1 b. 2R1 c. 1R2 d. 4R4 e. 2R4
2. What does R mean? (*What familiar relation does R represent?)*

Example. Let $A = \{1, 2, 3, 4\}$, and consider the set
$S = \{(1,1), (1,3), (3,1), (3,3), (2,2), (2,4), (4,2), (4,4)\} \subseteq A \times A$.
What does S mean?

REPRESENTING A RELATION WITH A GRAPH
We can make a picture of a relation R on A by making a point for each element of A, and for each $(x, y) \in R$ drawing an arrow from x to y.
Ex: Draw a picture of the relation S

Example. Here is a picture of a relation U on a set B.



Find the sets B and U.

NOTE: relations can be infinite, too!
Example. Consider the set $R = \{(x, x) : x \in \mathbb{R}\}$. What does R represent?

Sec 11.1 - Properties of Relations

Definition. Suppose R is a relation on a set A.

1. Relation R is **reflexive** if xRx for every $x \in A$: $\forall x \in A,\ xRx$
2. Relation R is **symmetric** if xRy implies yRx for all $x, y \in A$: $\forall x, y \in A,\ xRy \Rightarrow yRx$
3. Relation R is **transitive** if whenever xRy and yRz, then also xRz:
   $\forall x, y, z \in A,\ ((xRy \wedge yRz) \Rightarrow xRz)$
4. Relation R is **antisymmetric** if for $x, y \in A$, xRy and yRx implies $x = y$:
   $\forall x, y \in A,\ (xRy \wedge yRx) \Rightarrow x = y$
5. Relation R is **irreflexive** if $\sim xRx$ for all $x \in A$: $\forall x \in A,\ \sim xRx$

Example. Consider the set $A = \mathbb{Z}$, the integers. For each of the following relations, determine if it is reflexive, symmetric, transitive, antisymmetric or irreflexive

a. $<$ b. $\leq$ c. $=$ d. $\neq$

CLASS:
Example. Let $A = \{b, c, d, e\}$ and
$R = \{(b,b),\ (b,c),\ (c,b),\ (c,c),\ (d,d),\ (b,d),\ (d,b),\ (c,d),\ (d,c)\}$
Determine whether R is reflexive, symmetric, transitive, antisymmetric or irreflexive
NOTE: might help to realize that "xRy" means "both x and y are consonants". Sketch a graph! Look at relations.

Lecture 23 - Sec 11.2, 11.3, 11.4

Equivalence relations, equivalence classes,

Definition. A relation R on a set A is an **equivalence relation** if it is reflexive, symmetric and transitive.

CLASS (have each group draw graph on board, give answers to b, c -- then at the end, have each discuss results?)
Example 1. Your group will be assigned one of the relations below on the set $A = \{-1, 1, 2, 3, 4\}$.
a. Draw a diagram of the relation.
b. Determine whether the relation is an equivalence relation (be prepared to explain).
c. State in a few words what the relation represents.

R_1= {(-1,-1), (1,1), (2,2), (3,3), (4,4), (-1,1),(1,-1),(-1,3),(3,-1),(1,3),(3,1),(2,4),(4,2)}
R_2= {(-1,1),(-1,2),(-1,3),(-1,4),(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)}
R_3= {(-1,-1), (1,1), (1,2),(2,1),(2,2),(2,3),(3,2),
(3,3),(1,3),(3,1),(4,4),(1,4),(4,1),(2,4),(4,2),(3,4),(4,3)}
R_4= {(2,2),(3,3),(-1,-1),(4,4),(1,1)}
R_5= (4,4),(4,3),(4,2),(4,1),(4,-1),(3,3),(3,2),(3,1),(3,-1),(2,2),(2,1),(2,-1),(1,1),(1,-1),(-1,-1)}

ANS: R1: YES, "has the same parity", R2: NO, "less than", R3: YES, "has the same sign", R4: YES, "is equal to", R5: NO "greater than or equal to"

Equivalence relations are important because they divide up your set into groups -- where everything within a group is related to everything else in that group. We call these groups **equivalence classes**.

QUESTION: What are the equivalence classes for R1?

Definition. Suppose R is an equivalence relation on a set A. Given an element $a \in A$, the **equivalence class containing *a*** is the subset $\{x \in A: xRa\}$ of A consisting of all elements that are related to a. This is denoted $[a]$, so the equivalence class containing a is $[a] = \{x \in A: xRa\}$
NOTE: beware! a is an element, but [a] is a SET - a collection of elements of A.

Example 2. a. For equivalence relation R_1, what is [1]? What is [4]? What is [-1]?
b. For each equivalence relation in Example 1, list the equivalence classes.

NOTE: For R1, [1]={-1,1,3}. This set {-1,1,3} can be referred to as [1], or as [-1], or as [3] -- these all mean the same thing, the equivalence class of odd numbers.

Definition. A **partition** of a set A is a set of non-empty subsets of A such that the union of all the subsets equals A, and the intersection of two different subsets is $\emptyset$.
*Basically, a **partition** is a division of A into subsets.*

Theorem. Suppose R is an equivalence relation on a set A. Then the set $\{[a]: a \in A\}$ of equivalence classes of R forms a partition of A.

NOTE: This theorem just says that dividing a set up into subsets is the same as having an equivalence relation on the set -- it's just gives another way of looking at things. You will find in mathematics that it sometimes helps to think of things in terms of the equivalence relation (how individual members of A are related), and sometimes in terms of the partition (the sets that A is divided into)

CLASS.
Example 3.

RECALL: Given integers a and b and an $n \in \mathbb{N}$, then $a \equiv b \ (mod\ n)$if $n|(a - b)$. *We say "a and b are congruent modulo n."*

Consider the equivalence relation R on the integers given by aRb if and only if $a \equiv b \ (mod\ 4)$.
1. True or false: a. 4R8 b. 4R9 c.5R7 d. 5R9 e. 3R11 f. 2R18
2. How can you tell whether two numbers are congruent mod 4?
3. Is R reflexive? Prove your answer.
4. Is R symmetric? Prove your answer.
5. Is R transitive? Prove your answer.
6. Is R an equivalence relation?
7. What is the equivalence class [4] = ?
8. How many equivalence classes are there? List them.

Example 4. a. How many equivalence classes will there be for the equivalence relation $a \equiv b \ (mod\ 5)$? List the classes.
b. For a given natural number n, how many different equivalence classes will there be for the equivalence relation $a \equiv b \ (mod\ n)$?

NOTE: Have NOT covered Sec 11.4 arithmetic of equivalence classes, showing +/ are well-defined. SKIP? OR DELAY A DAY TO COVER? Maybe ask Andrew about algebra course*

Example 5

For the relation $a \equiv b \ (mod\ 5)$, there are five equivalence classes. We could refer to them as [0], [1], [2], [3], [4] (is this the only way to refer to them?). These five equivalence classes form a set, which we will refer to as $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$. Even though the elements of $\mathbb{Z}_5$ are sets, and not numbers, we can still add and multiply them using these rules:
1. $[a] + [b] = [a + b]$
2. $[a] \cdot [b] = [a \cdot b]$

Example:
a. [2]+[1]=
b. [2] $\cdot$ [2] $=$
c. [2]+[3]=

d.Write down the addition and multiplication tables for $\mathbb{Z}_5$

The key question: Does this work? The proposition below says “YES”
Proposition. These rules are “well defined”. (that is, they give the same answer, regardless of the representative of each equivalence class that we choose)

Beware - in part c, what is [5] in Z5? We would instead write [2]+[3]=[0].

QUESTION: When we add equivalence classes, does it matter which representative we choose?

Lecture 25 - Sec 11.5, 12.1, 12.2

function, domain, codomain, range, injective, surjective, bijective

NOTE: A relation does not always have to be a subset of AxA:
Definition. A **relation from a set *A* to a set *B*** is a subset $R \subseteq A \times B$.

FUNCTIONS.
Now we talk about a big topic, functions. Let's start with a familiar example.

Example 1. Consider the function $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$. The graph of *f* is just a relation $R \subseteq \mathbb{R} \times \mathbb{R}$ -- it is the set $R = \{(x, x^2): x \in \mathbb{R}\}$.
Sketch the graph.
In fact, a function is just a special kind of relation.

WHAT MAKES A FUNCTION SPECIAL?
A function is a relation that satisfies a special property:

Definition. A **function** *f* from *A* to *B* (written $f: A \to B$) is a relation $f \subseteq A \times B$ satisfying the property that for each $a \in A$ there is exactly one $b \in B$ such that (a, b) is in the relation *f*. The statement $(a, b) \in f$ is abbreviated $f(a) = b$.

NOTE: Because each a has only one b, we think of "putting in a" (a is the input), and "getting out b" (b is the output).

Example 2. Given the sets $A = \{a, b, c, d\}$ and $B = \{3, 4, 5, 6\}$, consider the following subset *f* of $A \times B$: $f = \{(a, 3), (b, 5), (c, 6), (d, 5)\}$
a. Is *f* a function?
b. What is *f(a)*? *f(c)*?
c. Draw a diagram of *f*.

Definition. The set A is called the **domain** of *f* (the set of "input values"). The set B is called the **codomain** of *f*. The **range** is the set $\{f(a): a \in A\}$, the set of "output values".
Think of the codomain as a sort of "target" for the outputs - not everything in the codomain gets "hit" by an input.

Example 2 cont'd
d. What is the domain, the codomain, and the range of *f*.

What are the domain, codomain, and range in Example 1 above?

Definition. A function $f: A \to B$ is

- **injective** (or **one-to-one**) if for every $x, y \in A$, $x \neq y$ implies $f(x) \neq f(y)$.
- **surjective** (or **onto**) if for every $b \in B$ there is an $a \in A$ with $f(a) = b$.
- **bijective** if *f* is both injective and surjective.

Example 2 cont'd.
g. Is the function *f* in Example 2 above injective? surjective?
h. Create a new function from A to B (in example 2) that is both injective and surjective.

GROUPS (assign a different function to each group).
Example 3.
Is each of these sets a function? Why or why not? If it is a function, what is the domain, codomain and range? *BONUS: Is it injective? surjective?*

1. The set $S = \{(x, \sin x) : x \in \mathbb{R}\}$.
2. The set $T = \{(2a, a) : a \in \mathbb{N}\}$.

   The following two examples are based on the set $A = \{1, 2\}$
   and its powerset $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
3. The relation R_1 from *P(A)* to *A* giving "the largest element":

   $R_1 = \{(\{1, 2\}, 2), (\{2\}, 2), (\{1\}, 1), (\emptyset, \emptyset)\}$
4. The relation R_2 from *A* to *P(A)* expressing "is an element of":

   $R_2 = \{(1, \{1\}), (2, \{2\}), (1, \{1, 2\}), (2, \{1, 2\})\}$.

How to prove a function $f: A \to B$ is injective

Direct Proof	**Contrapositive Proof**
Proof. Suppose $x, y \in A$ and $x \neq y$. … Therefore $f(x) \neq f(y)$.	*Proof.* Suppose $x, y \in A$ and $f(x) = f(y)$. … Therefore $x = y$.

Often the contrapositive approach is easier (you start with an equation, which you can work with)...

How to prove a function $f: A \to B$ is surjective

Proof. Suppose $b \in B$. [Find $a \in A$ for which $f(a) = b$.]

GROUPS (each group does both)
Example 4.
For each function, determine whether it is injective, surjective or both. Prove your answer.
1. The function $f: \mathbb{R} - \{0\} \to \mathbb{R}$ defined by $f(x) = \frac{1}{x} + 1$

2. The function $g: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $g(m, n) = m + n$
What is the domain/range? What does injective/surjective mean in this case? think about PAIRS of numbers

Lecture 26 - Sec 12.3, 12.4

the pigeonhole principle, composition of functions

CORRECTION - OOPSY!
We have been using an incorrect definition -- the definition that we call **antisymmetric** is actually known by another word, **asymmetric.** The actual definition of **antisymmetric** is slightly different:
Definition. A relation R on A is **asymmetric** if for $x, y \in A$, xRy implies $\sim yRx$.

Example: $<$ is asymmetric

Definition. A relation R on A is **antisymmetric** if for $x, y \in A$, xRy and $x \neq y$ implies $\sim yRx$.

Example: $\leq$ is antisymmetric

A surprisingly powerful theorem related to pigeons.

Suppose you have a set A of pigeons, and a set B or pigeonholes, and all the pigeons fly into pigeonholes. Think of this as describing a function $f: A \to B$, where pigeon x flies into pigeonhole f(x).
Question: What can you tell me about the situation where |A|>|B|?
Question: What can you tell me about the situation where |A|<|B|?

Example 1.

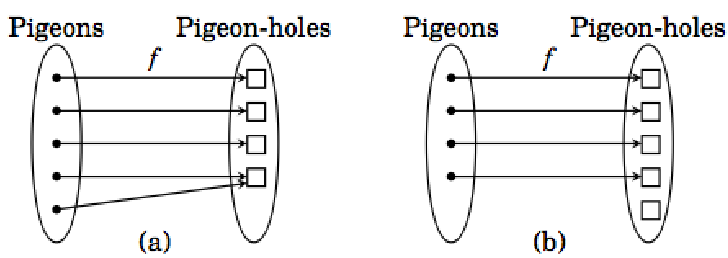


Figure 12.4. The pigeonhole principle

Theorem (The Pigeonhole Principle). Suppose A and B are finite sets and $f: A \to B$ is any function. Then:
1. If $|A| > |B|$, then f is not injective.
2. If $|A| < |B|$, then f is not surjective.

This is surprisingly powerful fact.

Example 2. There are at least two people in Brooklyn with exactly the same number of hairs on their heads.

Proof. Consider the function f that inputs a Brooklyn resident and outputs the number of hairs on their head. What is A? What is B?

How many hairs on human head? Average 100,000 (certainly LESS THAN 1 million)
Population of Brooklyn? 2.5 million.

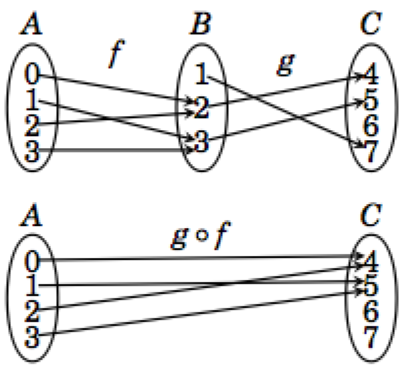
Example 3. a. Consider A={5,7,12,11,17,50,51,80,90,100}. Find two different subsets with the same sum.
b. Suppose A is any set of 10 integers between 1 and 100. Then there exist distinct subsets $X, Y \subseteq A$ with $X \neq Y$ for which the sum of elements in X equals the sum of elements in Y.

Let X={5,80} and Y={7,11,17,50}

SECTION 12.4 - COMPOSITION OF FUNCTIONS

Definition. Suppose $f: A \to B$ and $g: B \to C$ are functions, and the codomain of *f* equals the domain of *g*. Then the **composition** of *f* with *g* is a function from A to C, written $g \circ f: A \to C$, and defined $g \circ f\,(x) = g(f(x))$.

Example 4.



Example 5. Let $f: \mathbb{R} \to \mathbb{R}$ be defined $f(x) = x^2 + x$ and $g: \mathbb{R} \to \mathbb{R}$ be defined $g(x) = x + 1$. Find formulas for $g \circ f$ and $f \circ g$.

CLASS:
Example 6. Given sets *A = {0, 1, 2, 3, 4}* and *B = { a, b, c, d}*, consider the functions $f: A \to B$ and $g: B \to A$ given by *f = { (0,a), (1,a), (2,a), (3,b), (4,d) }* and *g = { (a,3), (b,1), (c,2), (d,3) }*. Find $g \circ f$ (either by giving a set of ordered pairs, or drawing a diagram with arrows).

Example 7. Consider the functions $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(m, n) = m \;\; + 2mn$ and $g: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(x) = (x + 7, x^2)$. Find formulas for $g \circ f$ and $f \circ g$.

Lecture 27 - Sec 12.5, 12.6

inverse functions, image, preimage

Definition. Given a set A, the **identity function** on A is the function defined as $i_A(x) = x$ for every x in A. $i_A = \{ (x, x) : x \in A\}$

Definition. Given a relation R from A to B, the **inverse relation of *R*** is the relation from B to A defined as $R^{-1} = \{(y, x): (x, y) \in R\}$.
Switch all of the pairs (x,y) in R to get R inverse.

We are going to be concerned in particular with relations that are functions.

Example 1. Consider the sets A={a,b,c} and B={1,2,3}. For each function from A to B, find the inverse relation. Is the inverse relation a function from B to A?

a. f = { (a,2), (b,3), (c,1) }
b. g = { (a,2), (b,3), (c,3) }

Question: Under what circumstances will the inverse relation of a function from A to B be a function from B to A?

Theorem. Let $f: A \to B$ be a function. Then f is a bijection if and only if the inverse relation f^{-1} is a function from B to A.

Question: What happens if you first apply f, then f inverse?

Theorem. If $f: A \to B$ is a bijection then its **inverse** is the function $f^{-1}: B \to A$ which satisfies $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

Example 2. The function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + 1$ is a bijection.
a. Find f(1). Find f(2). Give two ordered pairs that must be in the relation f.
b. Now give me two ordered pairs that must be in the inverse function f^{-1}.
c. Find a formula for the inverse f^{-1}. Check your work by calculating $f^{-1} \circ f(x)$ and $f \circ f^{-1}(x)$.

QUES: What's the process for finding the inverse?
1. *replace f(x) with y.*
2. *Switch all y's and x's.*
3. *Solve for y.*

Example 3. The function $g: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(m, n) = (m + n, m + 2n)$ is a bijection. Find a formula for the inverse g^{-1}. Check your work by calculating $g^{-1} \circ g(x)$.

Example 4. Prove that the function $g: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(m, n) = (m + n, m + 2n)$ is a bijection.

Some notation that you will run into in future math classes -- taking “f of a SET” even when f is a function whose domain is numbers.

Definition. Suppose $f: A \to B$ is a function.
a. If $X \subseteq A$, the **image** of *X* is the set $f(X) = \{f(x): x \in X\} \subseteq B$.
b. If $Y \subseteq B$, the **preimage** of *Y* is the set $f^{-1}(Y) = \{x \in A: f(x) \in Y\} \subseteq A$.
NOTE: The preimage can be taken ***even if the inverse is not a function****.*

Example 5. Consider the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
a. Let X = {-1, 1, 2, 5}. Find $f(X)$.
b. Let Y = {4, 9, -9, 5}. Find $f^{-1}(Y)$.
c. Find $f([-2, 3])$. *Recall: [0,3] is the closed interval including all real numbers between 0 and 3.*
d. Find $f^{-1}([0, 9])$.
e. Find $f^{-1}([-2, -1])$.
Could skip c,d,e

Lecture 28 - 13.1
cardinality

CARDINALITY OF SETS
What does cardinality mean?

Basic questions about cardinality of sets:
a. What is the cardinality of a set?
b. When do two sets have the same cardinality?
c. When does one set have smaller cardinality than another set?

Example 2.
Given sets A = {a, b, c, d} and B = {0, 2, 4, 6, 8}
a. Find |A| and |B|.
b. True or false: |A| = |B|, |A| < |B|, |A|>|B|

Example 3.
Given sets $\mathbb{N}$ and $\mathbb{Z}$
a. Find $|\mathbb{N}|$ and $|\mathbb{Z}|$.
b. True or false: $|\mathbb{N}| = |\mathbb{Z}|$ $|\mathbb{N}| < |\mathbb{Z}|$, $|\mathbb{N}| > |\mathbb{Z}|$

NOTE: To answer part a, we would need some kind of "infinite numbers", which we don't currently have! So we go on to part b. Here we come to the work of Georg Cantor -- about 130 year ago,he became first person to find a way to seriously address these questions EVEN WITHOUT having "infinite numbers" to work with.

Example 4. You are in kindergarten. So far, you have learned to count to 3. One day, your teacher draws 5 people and 5 houses on the board. She asks the class "Are there the same number of people and houses?"

Definition. Two sets A and B have the **same cardinality**, written $|A| = |B|$, if there exists a bijection $f: A \to B$. If no such bijection exists, then the sets have **unequal cardinalities**, that is, $|A| \neq |B|$.

Find a bijection between N and Z.

Example 5. True or false: $|\mathbb{N}| = |E|$, where E is the set of even natural numbers.
Example 6. Do the intervals of real numbers $(0, 1)$ and $(1, \infty)$ have the same cardinality?
Example 7. True or false: $|\mathbb{N}| = |\mathbb{R}|$.

From: Alcock & Simpson, *Ideas from mathematics education: an introduction for mathematicians*

Definitions

A function $f: \mathbb{R} \to \mathbb{R}$ is said to be increasing if for all $x, y \in \mathbb{R}$, ($x > y$ implies $f(x) > f(y)$).

A function $f: \mathbb{R} \to \mathbb{R}$ is said to have a global maximum at a real number c if for all $x \in \mathbb{R}$ such that $x \neq c$, $f(x) < f(c)$.

Task

Suppose *f* is an increasing function. Prove that there is no real number *c* that is a global maximum for *f*.

NOTE: At some point, include the full list of logical equivalences on p 48.
NOTE: Discuss "necessary" vs "sufficient"

NOTES AND IDEAS:
From Thomas Tradler -
(MAYBE @BEGINNING OF "PROOFS" SECTION?) Recall the MIU riddle from Godel Escher Bach - working in a formal system - how to prove stuff?
Maybe use this riddle / use other stuff from GEB / at least recommend GEB to all?
(NOTE: OpenCourseware did a GEB course in 2007 I think)
(?? MIU RIDDLE - challenge - have students read the rules, complete one or two exercises, then design their own exercises? Start with this string, end with this string? extra credit for first correct solution posted?)

Suman - recommends Devlin "Intro to Mathematical Thinking" (cheap!) - also course on Coursera
https://www.coursera.org/course/maththink
http://www.amazon.com/Introduction-Mathematical-Thinking-Keith-Devlin/dp/0615653634

The BOOK OF PROOF site has a page with sample tests (maybe use these for review?):
http://www.people.vcu.edu/~rhammack/math300/tests/index.html

IDEA: openlab assignment - easiest/hardest ideas so far
IDEA: openlab assignment once we start proof - Consider the Intro part of Chapter 3 in Alcock & Simpson (see below for link). Assign the same proof to students (prove an increasing function can have no maximum). Then have them read about the two alternative approaches, identify their own approach -- end with an open question?

Andrew: build in some basic math concepts/reminders (e.g. exponents and so on)

Alcock & Simpson, *Ideas from mathematics education: an introduction for mathematicians*
Book on Math Education, esp. ideas influenced by education research (Free pdf, has Chapter 3 on proofs, used by NYU Math Ed Seminar 2013)
https://dspace.lboro.ac.uk/dspace-jspui/handle/2134/8846

?OpenLab assignment - work on proof/problem, then read result, then post on it? OR each person prepare written solution, bring to class - then do project in pairs in class to review/discuss solutions? OR after discussing solutions, read excerpts from paper (stream-of-consciousness descriptions from each case study student)

IDEA (Leo): in class, instead of having groups prove a theorem, give them the theorem and ask them to formulate a reason for each step - explain WHY this step is here. If a group has a minority opinion, they should include it! The example he used was irrationality of radical 2 (he even suggested showing that proof at the board, then assigning similar for radical 3 - *not sure whether groups should complete it, or have it provided?*)

TOOLS FOR GENERATING DIRECTED GRAPHS:
http://bl.ocks.org/rkirsling/5001347 (decent, but reflexive links not clear)

http://www.sagemath.org/ (looks good, but needs to be installed - open source!)
Online version: https://cloud.sagemath.com/