0 Introduction to Discrete Math

Welcome to Discrete Math! In this class we are going to study a **wide variety** of topics, but at the heart of all of them are

- Logical Thinking
- Problem solving (potentially with open ended questions)
- Exploration, Experiment and Conjecture

Today we are going to see some examples of the types of problems we'll encounter in this class.

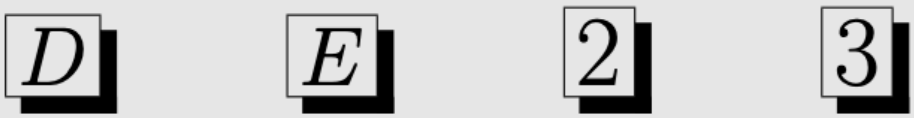
For Monday's class, make sure you setup your access to our textbook and READ Sections 1.1, 1.2 and complete the (Participation Activities and Challenge Reading Activities) **before** 2:30pm on Monday start of class.

Problem 1:

Let's start with a logical thinking question.

Mathematical Outing ⋆ ⋆ ⋆

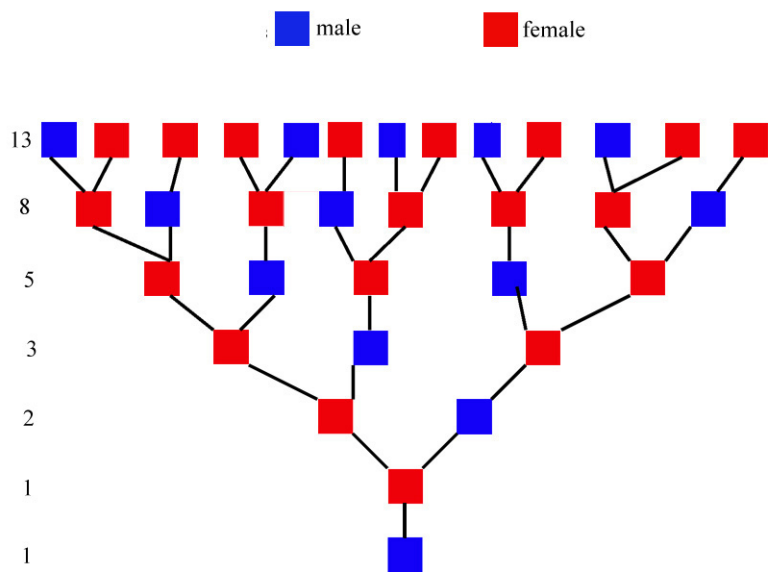
Each of the four cards below has a digit printed on one side and a letter printed on the other side. Imagine that a classmate makes the assertion that "If there is a vowel on one side of a card then there is an odd number on the other side." Which cards *must* be turned over to check whether or not this is a true statement?



This type of statement: "IF _____ THEN _____" is called a **conditional** statement. You'll read about these next week.

Where in real life do you see conditional statements like this?

Problem 2: What do you know about the genetics about bees? There's lots of fascinating stuff, but we're going to focus on how bees reproduce and study their family tree. It turns out that male and female bees have a different number of chromosomes. Male bees have 13 chromosomes and female bees have 26. This is because every female bee has two parents (mother and father who each contribute 13 chromosomes) but every male bee has only 1 parent (just its mother). Check out the family tree below and see if you understand what it's representing and then think about the following questions.



The blue square at the bottom represents a male bee. It has one parent. How many

- grandparents does it have?
- great grandparents?
- great great grandparents?

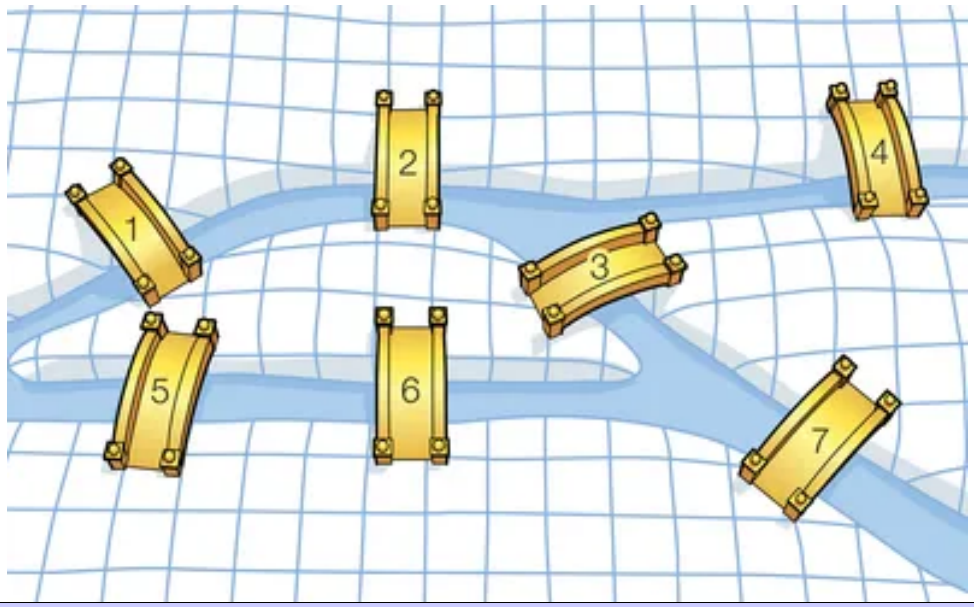
This picture represents what is called a **tree**. Do you think this is a reasonable name for this? Are there other names you might choose?

How many bees would there be in the next level of this tree? The number after that? Do you see a pattern with the numbers on the left?

If you found a pattern, how confident are you that the pattern will continue forever. (Would you wager your life savings? What could you do to increase your certainty to this 100% level?)

Exciting Bonus: If you look at the numbers on the left, they are increasing, at what rate do they roughly increase at each step?

Problem 3:



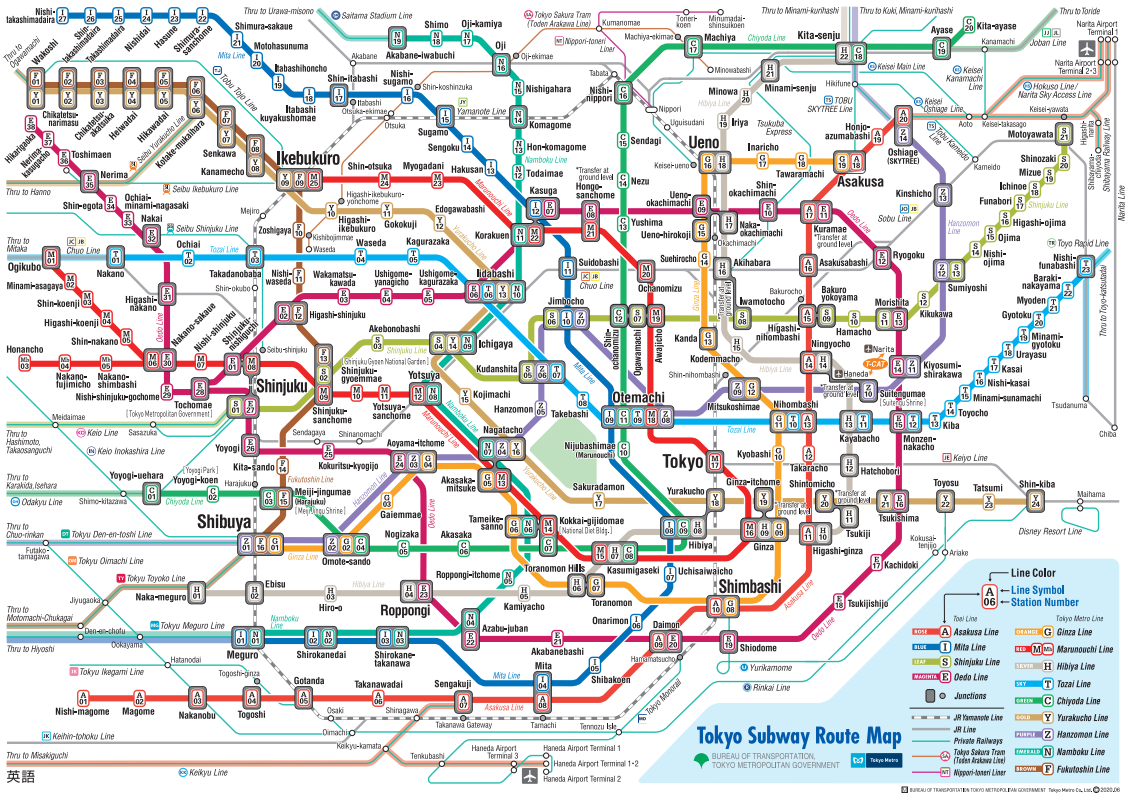
You travel to a new city and discover that there are 7 bridges. You want to walk across all 7 of them, but you don't want to walk over any bridge more than once.

- Is this possible?
- If so, where should you start?
- If not, why is it impossible?

(For the purposes of this problem, just restrict yourself to this picture, there's no way to walk around outside of the frame of this picture.)

This picture represents what is known as a **graph or network**, because there are different objects (islands, riverbanks, etc) called **nodes** that are connected with bridges (called edges.) Can you think of other examples of **graphs or networks?**

(some more examples of graphs)



1 Mathematical Statements and Propositions

In this packet we will
- Learn what mathematical propositions are;
- Determine whether simple mathematical propositions are true or false;
- Understand logical connectives and truth tables;
- Learn how to tell if two statements are **logically equivalent**, meaning they have the same truth tables.
- Use DeMorgan's Laws to negate
- Learn about implications, how to recognize them in words, and negate them.

As always, in this class, you will be expected to **read** and complete the embedded textbook exercises before we cover the relevant material in the packets.

1.1 Propositions and Logical Operations

Class Example:

One of the following is NOT a mathematical proposition: which one? For the propositions, determine the truth value of each.

- There are 8 days in a week or "chocolate" has 9 letters.
- Some weeks have 7 days and $3 < 5$
- Is 2 positive or negative?
- $4 < 5$ and it is not the case that 5 is even.

In the reading we learned about:

conjunction which means _____;

disjunction which means _____;

negation which means _____;

In this class, we will just use "and" and "or";

In this class, OR is always taken to be (inclusive / exclusive) (circle one)

You learned that for compound propositions, e.g.

$$p \text{ and } (q \text{ or } r)$$

you can build a _____ to keep track of the **truth values**;

(You also learned about XOR (or exclusive or) - this won't come up that much in this class, but is useful in Computer Science)

Some pointers: Remember that OR is inclusive, "p OR q" will be true if either (or both) statements are true.

Group Example

Below is a list of propositions, each of which is given as an english sentence. Discuss the truth value of each proposition with the members of your group. This worksheet will not be collected. The goal is to get you discussing mathematical statements (and their truth), so **go slowly**. Do not move on from a question until everyone in the group is on the same page. I would rather you spend the entire time discussing the first three propositions, than race through it to get to the end.

1. $7 < \pi$ or $10 < 3^2$.
2. It is not the case that $7 < \pi$.
3. $10 < 3^2$ or it is not the case that $7 < \pi$.
4. $2^9 = 512$ and it is not the case that $10 < 3^2$.
5. It is not the case that $7 < \pi$ or $10 < 3^2$.
6. It is not the case that $7 < \pi$, or $10 < 3^2$.
7. It is not the case that $7 < \pi$, and ($10 < 3^2$ or $2^9 = 512$).

Translating Between Math and English

Let's practice translating between English sentences and symbolic expressions. Also we will be practicing using the symbol $\neg$ which means "the negation of" or "it is not the case that"

Let p and q denote the statements "We won our first game" and "We won our second game."

Rewrite each of the following statements using the symbols $p, q, \wedge, \vee, \neg$.

a.) We won both of our first two games.

b.) We lost both of our first two games.

c.) We won at least one of our first two games.

d.) We lost at least one of our first two games.

e.) We didn't win both of our first two games.

Our goal later this week will be to see how to tell if statements like this are **equivalent**. Two of the above are conveying the same information, but in different ways. Do you see which two?

1.2 Evaluating Compound Propositions

Truth Tables

Sometimes it is helpful to break a statement up into pieces and analyze them separately. The idea is that if we want to determine whether something like $(p \wedge q) \vee r$ is true or false, we can analyze each piece separately. Like this:

"Hmm, I want to know if $(blah) \vee R$ is true. Well I guess since OR is INCLUSIVE, I can just check if r is true or if blah is true. Oh, but what is blah? Oh I see, blah = $p \wedge q$. Oh, ok .... "

We can formalize this with a **truth table.** And fill in the contents below. Let's do it!

p	q	r			

Questions:

Why are there 8 rows in this table?

Are there any rows where we can immediately fill in the last column?

What are some uses of truth tables that you can think of?

If you have any trouble filling out truth tables, please come and talk to me in office hours, or over email. We won't be doing too much with truth tables this semester, but it's important for you to be able to fill in the entries slowly and carefully.

1.3 Logical Equivalence

Sometimes a statement might be hard to wrap your head around (or hard for you to communicate it to a computer) Consider statements like:

"It is not the case that either Alice is friends with Bob or that if Bob is friends with Charlie then Dave has no friends."

Holy cow! That makes my brain hurt. The middle part would be complicated enough, but that pesky "not the case that" makes things even more complicated. For example, let's see if we can intuitively decide how to "simplify" the statement:

"It is not the case that (Adam likes chocolate or tea)."

"It is not the case that (Adam likes chocolate and tea)."

These are examples of two of **DeMorgan's Laws:**

$$\neg(p \wedge q) = \neg p \vee \neg q$$

$$\neg(p \vee q) = \neg p \wedge \neg q$$

These laws can help us simplify compound statements.

1.4 Conditional Statements

And just what are you implying....

There is a new law in town that says:

If you work weekends then you must have form X on file.

Below is a table that shows data for two companies. Which companies are **in compliance** with the new law?

Company 1

	Weekends	*Form X*
Alice		✓
Bob	✓	✓
Carol		
Dave	✓	✓
Earl	✓	✓

Company 2

	Weekends	*Form X*
Alice	✓	
Bob	✓	✓
Carol		✓
Dave		
Earl		✓

Sometimes we want to make **conditional** statements. For example:

"If you don't complete any work in this class then you will not receive a passing grade." (A true statement)

"If you complete all the work in class then you will receive an A+" (A false statement)

"If x is a whole number then $4x$ is an even number." (A true statement.)

These are all examples of "implications" or "conditional statements." We denote such statements as $p \implies q$. p is called the **hypothesis** and q is called the **conclusion.**

In the reading you will also read about the terms **converse, contrapositive, inverse and biconditional** These are important, but I don't want us to get too bogged down with these. These will come up naturally throughout the course, especially when we start learning about proofs. The main two I want us to focus on are converse and contrapositive:

The converse of $p \implies q$ is _____

The contrapositive of $p \implies q$ is _____

Story Time:

Before we fill out the truth table for $p \implies q$ let's think about what things mean. Consider the following statement I could make:

$p \implies q$: "If it's Tuesday, then I go rock climbing."

Under which of the following situations would you say that this sentence is FALSE? (In other words, when would you call Adam out as a liar?)

	Adam is:
It's Tuesday and Adam goes rock climbing.	[Telling the truth / A liar]
It's Tuesday and Adam does not go rock climbing.	[Telling the truth / A liar]
It's not Tuesday and Adam goes rock climbing.	[Telling the truth / A liar]
It's not Tuesday and Adam does not go rock climbing.	[Telling the truth / A liar]

The statement above can be reformulated in several ways, which of the following are correct reformulations of "If it's Tuesday then I go rock climbing."?

- I climb every Tuesday
- I only climb on Tuesdays
- I don't climb on Wednesday
- Every Tuesday I climb
- If I climb, then it's Tuesday

p	q	$p \implies q$	$\neg(p \implies q)$	

Questions:

Why are there 4 rows in this table?

Does this feel "weird" at all? (Honestly, that's normal, it still feels a little weird to me!)

What are some main ideas to keep track of when filling out truth tables that involve $\implies$?

Fill in the blank: We see from the table that

$$\neg(p \implies q) =$$

Class Practice: Are these statements true or false?

1. If $7 < \pi$, then $10 < 3^2$.

2. If $2^9 = 512$, then $7 < \pi$.

3. $2^5 = 32$ implies that Adam lives in San Diego.

4. $2^5 = 16$ implies that Adam lives in Salt Lake City.

Group Activity: For each of the following, identify the hypothesis and conclusion: (Warning some of these statements are false, but that's ok - even if a proposition is false, we can still study it logically. (see note at the end of the section))

- $q \implies r$

  Hypothesis Conclusion Converse Contrapositive

- All birds lay eggs

  (First rewrite as "IF _____ THEN _____)

  Hypothesis Conclusion Converse Contrapositive

- All mammals are dogs

  (First rewrite as "IF _____ THEN _____)

  Hypothesis Conclusion Converse Contrapositive

- Only California residents live in San Diego

  (First rewrite as "IF _____ THEN _____)

  Hypothesis Conclusion Converse Contrapositive

- Only San Diego residents lives in California

  (First rewrite as "IF _____ THEN _____)

  Hypothesis Conclusion Converse Contrapositive

(Fireside Chat) Now you are probably thinking: Hey, Professor, why would we want to waste our time studying propositions that are false? That's a valid complaint, but here's maybe some way to think about this. Suppose you're writing some computer code, or writing an essay, or writing a mathematical proof, and somehow everything is coming out "wrong". Maybe the computer is returning false, but you really think it should be true. Well the best solution is to get into the details and really understand things like hypotheses, conclusions and see how they interact. Actually by practicing with statements (both true and false) you get more practice and experience doing exactly this sort of thing!

1.5 Homework Problems

Due: Monday Feb. 7th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Each week I will give many problems for practice preparing for the quizzes

- Some of the problems will be from the textbook. I have decided to show the solutions to these problems so you can check your answers. The goal of homework is to give you practice solving problems and help you prepare for the quizzes. I will also give some additional problems for you to work through. I'll provide some solutions or hints for some of t these problems.

1. Work on the following textbook problems. You don't need to write out solutions to ALL of these, but please solve a total of at least 9 of these problems. Try to write down your solutions first, and then check the answers. If you made mistakes, make a note about what you learned and mark this on your paper. I will be grading these homework problems for completion. The notes that you write down can be helpful as you work on the quiz.

   1.1.1, 1.1.2, 1.1.3, 1.1.4,

   1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.7

   1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.10,

   1.4.2

2. In this packet we haven't focused too much on the "biconditional" or "if and only if" that you read about in the book. We will be working with statements like this throughout the semester, and will get practice proving them. For each of the 8 statements below, decide whether it is true or false. (For all of these, x is a real number.) For any FALSES that you find, please write a short sentence explaining why.

STATEMENT	THE CONVERSE OF THE STATEMENT
If $x > 0$ then $x^2 > 0$. (T/F)	If $x^2 > 0$ then $x > 0$. (T/F)
If Jack can legally purchase alcohol then Jack is at least 14 years old. (T/F)	If Jack is at least 14 years old then Jack can legally purchase alcohol (T/F)
If $2a$ is an integer, then a is an integer (T/F)	If a is an integer then $2a$ is an integer (T/F)
If $a > 0$ then the equation $x^2 = a$ has a solution. (T/F)	If the equation $x^2 = a$ has a solution then $a > 0$. (T/F)
If $a \geq 0$ then the equation $x^2 = a$ has a solution. (T/F)	If the equation $x^2 = a$ has a solution then $a \geq 0$. (T/F)

   You should have seen in this problem that:

   - It is possible for a statement to be true, but for the converse to be false. (And vice versa). Can you think of other examples of statements that are true but whose converse is false? Can you think of any about animals? Or geography? or even and odd numbers?
   - If a statement and its converse are both true (like they were in the last problem), that is, if $p \implies q$ AND $q \implies p$. We would write this as $p \iff q$ and this means that p and q are **equivalent.** Are any of the above statements **equivalent**. Can you think of any other equivalent statements?
   - There's no need to write out explicit answers to these bullet points, but these questions are the types of questions I want you to think about as you read things in this class. These sorts of question might turn up on a quiz. The goal of homework is always for practicing mathematics.

3. Which of the following is equivalent to the statement $(x-1)(x-2)=0$?

   - $x=1$
   - $x=2$
   - $x=1$ and $x=2$
   - $x=1$ or $x=2$

   Write your answer by writing down what is below and filling in the blank:

   $$(x-1)(x-2)=0 \iff \underline{\hspace{6cm}}.$$

4. Soon we will learn about something called "quantifiers". The main quantifiers we will use are "there exists" and "for all".

"There exists" occurs in statements that assert the existence of something. E.g. There exists a number that is bigger than 5. There is a blue whale that weighs 4000 tons. There is a flying reindeer named Todd. Some whale is friendly. One reindeer likes chocolate.

"For all" asserts that something is true for ALL of something. E.g. Every positive integer is either even or odd. All reindeer are called Todd. Every whale weighs less than 4000 tons. All integers are prime numbers. All movies have hidden meanings.

   For now, consider the following statements and think whether you think it is a "there exists" statement or a "for all" statement. You'll get full credit for turning this in, so don't worry so much about getting this correct - my goal is to help us build intuition as to what type of statement we have.

Note: I'm not asking you to say if these are True or False, just asking if they are saying "there exists" or "for all". You can write TE or FA for each one. Just do your best!

   A. There is a student in this class who has seen a Spiderman movie.

   B. Dr. Boocher has hiked one trail in Torrey Pines

   C. Dr. Boocher has hiked all the trails in Torrey Pines

   D. There is a trail in Torrey Pines that Dr. Boocher has hiked.

   E. All students in this class love Spiderman

   F. There exists a character in the movie Mean Girls called Karen Smith.

   G. There is a famous mathematician named Karen Smith. (true!)

   H. Every character in Mean Girls is named after a mathematician.

   I. Someone who lives in California likes surfing

   J. Everyone who lives in California likes surfing

   K. If x lives in California then x likes surfing.

   L. No one who lives in California likes surfing.

   M. Everyone who lives in California does not like surfing.

5. Consider the "for all" statement:

   p: "Everyone in this class likes chocolate."

   What is the negation of this statement (in words)? Is it a "for all" or a "there exists" statement?

6. Consider the "there exists" statement:

   q: "There is someone in our class whose favorite number is 14"

   What is the negation of this statement (in words)? Is it a "for all" or a "there exists" statement? Could you write down the negation in words? *

*Answers: 4. TE,TE,FA,TE,FA,TE,TE,FA,TE, FA, FA, FA, FA. 5. It will be a TE. The negation of "everyone likes chocolate" is "there is someone who doesn't like chocolate. 6. It will be a FA. The negation of "Someone's favorite number is 14" is "everyone's favorite number is a number other than 14."

1.6 Chapter 1 Extras

If time allows we will sometimes go over these questions:

1) Select the statement that is not a proposition.

   a. 5 + 4 = 88

   b. It will be sunny tomorrow.

   c. Take out the trash.

   d. Chocolate is the best flavor.

2) p = T, q = F, and r = F.
   Select the expression that evaluates to true.

   a. $p \wedge q$

   b. $\neg p$

   c. $q \vee r$

   d. $p \vee r$

3) p = F, q = T, and r = T.
   Select the expression that evaluates to false.

   a. $\neg q$

   b. $q \vee r$

   c. $q \wedge r$

   d. $p \vee r$

4) The propositional variables s and m represent the two propositions:

   s: It is sunny today.
   m: I will bring my umbrella.

   Select the logical expression that represents the statement: "Despite the fact that it is sunny today, I will bring my umbrella."

   a. s

   b. $s \wedge m$

   c. $s \vee m$

   d. $\neg m$

5) p = T, q = F, and r = T.
   Select the expression that evaluates to false.

   a. $p \vee \neg q$

   b. $p \vee q \vee r$

   c. $\neg(p \wedge \neg q)$

   d. $\neg(p \wedge q \wedge r)$

6) p = F, q = T, and r = T.
   Select the expression that evaluates to true.

   a. $\neg(q \vee r)$

   b. $(\neg p \wedge r) \vee q$

   c. $(\neg q \vee r) \wedge p$

   d. $p \vee \neg q \vee \neg r$

7) The propositional variables f, h, and p represent the propositions:

   f: The student got an A on the final.
   h: The student turned in all the homework.
   p: The student is on academic probation

   Select the logical expression that represents the statement: "The student is not on academic probation and the student got an A on the final or turned in all the homework."

   a. $\neg p \wedge (f \vee h)$

   b. $(\neg p \wedge f) \vee h$

   c. $\neg p \wedge f \wedge h$

   d. $\neg(p \wedge f) \vee h$

8) Select the converse of $p \to q$.

   a. $p \to q$

   b. $q \to p$

   c. $\neg p \to \neg q$

   d. $\neg q \to \neg p$

9) Which statement is the contrapositive of:
   "If $x = 4$, then $3x = 12$."

   a. If $x = 4$, then $3x = 12$.

   b. If $3x = 12$, then $x = 4$.

   c. If $n \neq 12$, then $3x \neq 12$.

   d. $3x \neq 12$, then $x \neq 4$.

10) Select the statement that is false.

    a. If 3 is a prime number, then 5 is a prime number.

    b. If 4 is a prime number, then 6 is a prime number.

    c. If 4 is a prime number, then 5 is a prime number.

    d. If 3 is a prime number, then 6 is a prime number.

11) The propositional variables b, v, and s represent the propositions:

    b: Alice rode her bike today.
    v: Alice overslept today.
    s: It is sunny today.

    Select the logical expression that represents the statement: "Alice rode her bike today only if it was sunny today and she did not oversleep."

    a. $b \to s \to \neg v$

    b. $b \to (s \wedge \neg v)$

    c. $s \wedge (\neg v \to b)$

    d. $(s \wedge \neg v) \to b$

12) p = T, q = F, and r = T.
    Select the expression that evaluates to false.

    a. $\neg(q \wedge r) \to p$

    b. $(p \wedge r) \to q$

    c. $(q \wedge r) \to p$

    d. $(q \wedge r) \to \neg p$

13) p = F, q = T, and r = T.
Select the expression that evaluates to true.

a. $\neg(q \vee p) \leftrightarrow r$

b. $(\neg p \wedge r) \rightarrow q$

c. $(q \vee \neg r) \rightarrow p$

d. $q \leftrightarrow (p \wedge r)$

14) Select the proposition that is a tautology.

a. $(p \wedge q) \rightarrow \neg p$

b. $(p \vee q) \rightarrow p$

c. $(p \wedge q) \leftrightarrow p$

d. $(p \wedge q) \rightarrow p$

15) Select the proposition that is a contradiction.

a. $\neg(p \vee q) \wedge p$

b. $(p \vee q) \wedge p$

c. $(\neg p \wedge q) \leftrightarrow p$

d. $(\neg p \wedge \neg q) \rightarrow p$

16) Select the proposition that is logically equivalent to $\neg p \rightarrow q$.

a. $p \wedge \neg q$

b. $p \vee q$

c. $\neg p \vee q$

d. $\neg p \wedge q$

17) Use De Morgan's law to select the statement that is equivalent to:
"It is not true that the employee received a large bonus and has a big office."

a. The employee received a big bonus or has a big office.

b. The employee did not receive a big bonus and does not have a big office.

c. The employee did not receive a big bonus or does not have a big office.

d. The employee received a big bonus and has a big office.

18) Use De Morgan's law to select the statement that is equivalent to:
"It is not true that the patient has high blood pressure or influenza."

a. The patient has high blood pressure or has influenza.

b. The patient does not have high blood pressure and does not have influenza.

c. The patient does not have high blood pressure or does not have influenza.

d. The patient has high blood pressure and has influenza.

Exercises

1. Decide whether the following statements are true or false.
a) The number 1776 is a perfect square.
b) It is the case that $3^3 + 4^3 + 5^3$ is equal to 6^3.
c) A triangle with sides of length 3, 4, and 5 has an area of 6.
d) There are at least two prime numbers between 11^2 and 12^2.
e) A cube has six faces, eight vertices, and ten edges.

2. Find an integer value of n for which the open sentence "$n^2 - n + 11$ is a prime number" is true. Find another value for n that makes it false.

3. Find all positive integers k for which the open sentence "$2^k + 1$ is a multiple of 3" is false. (Just check $k = 1, 2, \ldots, 8$ and describe the pattern.)

4. Find all real numbers x for which the open sentence $30(x - 20) = 20(x - 10)$ is true. By the way, this is commonly known as "solving the equation."

5. State the domain of the variables n, k and x in the previous three exercises.

6. In what way does the logical connective OR come into play when solving the equation $(x + 3)(x^2 - 9) = 0$?

7. Decide whether each statement is true or false.
a) There exists a real number x such that $e^x = 2$.
b) There exist positive integers p and q such that $p/q = \pi$.
c) There does not exist an integer k such that $k^2 + 2$ is divisible by 5.
d) For all real numbers m, the line having slope m and y-intercept 1 intersects the circle of radius 1 centered at the origin in exactly two points.
e) For every positive integer n, there exists a smaller positive integer.
f) There exists a unique two-digit number that is twice the product of its digits.
g) There exists a unique line passing through any two distinct points.

13. Let P be the statement "The cat is outside," let Q be the statement "The dog is outside," and let R be the statement "It is bright and sunny today." Translate the following statements into logical syntax.
a) The cat and dog are both inside, as it is raining today.
b) The cat is outside even though it is raining today.
c) At least one pet is outside on this sunny day.
d) It is not the case that the dog is outside in the sunshine.
e) The cat and dog are in different locations.

16. Demonstrate that $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

17. Negate each of the following statements.
a) Triangle ABC has a perimeter of 12 and an area of 6.
b) The number k is an integer such that k is even or $k \leq 10$.
c) I am older than Al but younger than Betty.
d) It is not the case that $2x < y$ and $2y < x$.
e) Jack will answer this question or the next one.
f) There is a new car behind at least one of the doors.

23. Demonstrate that $(P \wedge \neg Q) \vee (\neg P \vee Q)$ is a tautology.

24. Verify that $((P \vee \neg Q) \wedge \neg R) \wedge (R \vee (Q \wedge \neg P))$ is a contradiction.

25. Suppose that statement P is a contradiction. Show that $(P \vee Q) \wedge (P \vee \neg Q)$ is also a contradiction.

Quiz 1

1. In the implication $P \vee R \longrightarrow Q \wedge R$, What is the hypothesis?

   (a) P
   (b) Q
   (c) R
   (d) $Q \wedge R$
   (e) $P \vee R$
   (f) $\neg Q \vee R$

2. Which of the following is equivalent to $\neg(P \longrightarrow Q)$:

   (a) $Q \longrightarrow \neg P$
   (b) $\neg P \longrightarrow \neg Q$
   (c) $\neg Q \vee \neg P$
   (d) $Q \wedge \neg P$
   (e) $\neg Q \vee \neg P$
   (f) $P \wedge \neg Q$

3. Write the contrapositive of "If we go swimming then we will need sunscreen."

4. Which of the following is the negation of "Joe and Jill live on campus"

   (a) Neither Joe nor Jill live on campus
   (b) Either Joe doesn't live on campus or Jill doesn't live on campus
   (c) No students live on campus.

5. Consider the statements:

   p: There are bears in the mountains

   q: Hiking is safe on trail 4.

   r: There are lakes in the mountains

   Express the propositions below in terms of $p, q, r, \neg, \longrightarrow$

   (a) There are neither bears nor lakes in the mountains but hiking is safe on trail 4.

   (b) If there are lakes in the mountains then there are bears in the mountains.

   (c) Hiking is safe on trail 4 when there are no bears in the mountains

   (d) (this one is tough but you can do it!) If there are lakes in the mountains then hiking on trail 4 is safe only if there are no bears.

6. Fill in the truth entries in the row of the truth table below.

P	Q	R	$P \wedge Q$	$P \vee Q$	$\neg P$	$R \longrightarrow P$	$\neg Q \longrightarrow R \vee P$
T	F	F					

Warmup:

Our goal is to decide whether the statements below are saying:

A) If it is raining then the grass is wet

B) If the grass is wet then it is raining.

Match the statements below with either A or B

1. When it is raining the grass gets wet.
2. The only time the grass gets wet is when it is raining
3. The grass gets wet if it is raining
4. The grass gets wet only if it is raining
5. The grass gets wet when it is raining
6. It it raining whenever the grass is wet

2 Quantifying Mathematical Statements

Let's go back to our two companies. They discover there are some new requirements:

A : Every employee must have access to health care.

B : Some employee must attend the government annual meeting.

Which of the companies below is in compliance with these policies. Why?

Company 1

	Health Care Access	*Annual Meeting*
Alice	✓	✓
Bob	✓	✓
Carol		
Dave	✓	✓
Earl	✓	✓

Company 2

	Health Care Access	*Annual Meeting*
Fern	✓	
Graeme	✓	
Hyacinth		
Iona		
Jackie		✓

These are examples of using the **quantifiers** $\forall$ which means _____ and $\exists$ which means _____.

If A and B are the statements:

$h(x) : x$ has access to health care

$m(x) : x$ attends the annual meeting

then let's write statements A and B from above:

If I wanted to start an argument the first week of class, I could have asked whether or not the following sentence is a mathematical statement:

$$\boxed{x \text{ is positive.}}$$

The reason, an argument might arise is because, this statement as it currently reads is not yet complete. We don't know what x is, and as such there isn't a **well-defined** truth value. Consider the following statements:

"Let x be a solution to $1 - 2x = 5$. Then $\boxed{x \text{ is positive.}}$"

"Let $x = y^2$ where y is a negative real number. Then $\boxed{x \text{ is positive.}}$"

"There exists a real number x such that $\boxed{x \text{ is positive.}}$"

These **ARE** mathematical statements, because we have quantified the statement. For the rest of this chapter we will be going deeper into how we can quantify statements likes this.

Class Example:

Let $P(x) := x^2 - x - 1 \geq 0$. Unless otherwise stated, the domain of x will be assumed to be the set of all real numbers.

Determine the truth value of the following statements:

- $P(1)$
- $P(0)$
- $P(2) \vee P(1)$
- $\forall x P(x)$
- $\exists x P(x)$
- $\neg(\forall x P(x))$
- $\neg(\exists x P(x))$
- $\forall x \ \ (x > 100 \implies P(x))$
- $\forall x \ \ (P(x) \implies x > 0)$.

In this class we will often use different sets of numbers. The main ones we'll use are

$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ the set of **integers**. (number is "Zahl" in German)

$\mathbb{N} = \{1, 2, 3, \ldots\}$ the set of **positive integers**, often called the set of **natural numbers.**

2.1 A word about the domain of the variables

Consider the statement:

$$\exists x(x + x = 1)$$

Is this true if the domain is the set of all integers?

Is this true if the domain is the set of all real numbers?

And now... cue the fanfare...

Our first mathematical definition!

Definition:

A positive integer n is called **prime** is $n > 1$ and the only factors of n are itself and 1.

For example, the first few prime numbers are: $2, 3, 5, 7, 11, 13, \ldots$

Cool example: The Sieve of Eratosthenes Would you like to generate all the prime numbers up to a certain point? Well here's an ancient method that will do it!

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Some questions we will explore about primes:

- How many prime numbers are there? Is there a biggest one?
- Are there any patterns in the primes?
- (Famous Open Question) How many primes are exactly one more than a **square number**.

$$1^2 + 1 = 2 \text{ is prime}$$

$$2^2 + 1 = 5 \text{ is prime}$$

$$4^2 + 1 = 17 \text{ is prime}$$

$$6^2 + 1 = 37 \text{ is prime}$$

$$10^2 + 1 = 101 \text{ is prime}$$

$$2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101, 8837, 12101, 13457,$$
$$14401, 15377, 15877, 16901, 17957, 21317, 22501, 24337, 25601, 28901, 30977, 32401, 33857, 41617, 42437,$$
$$44101, 50177, ?$$

no one knows if this list goes on forever.

Let $Q(x) \coloneqq x$ is prime. For instance, $Q(2)$ is true $Q(4)$ is false.

Consider our two examples from class

$$P(x) \coloneqq x^2 - x - 1 \geq 0 \qquad \text{and} \qquad Q(x) \coloneqq x \text{ is prime}$$

Let's have the domain of the following be the set of positive integers $\mathbb{N}$.

1. Invent a true proposition using exactly one of these predicates and exactly one quantifier. Explain in a sentence why your proposition is true. Let's list some possibilities:

2. Invent a false proposition using exactly one of these predicates and exactly one quantifier.

3. Invent a true proposition using both of these predicates and exactly one quantifier. You may use any of the logical operations of $\wedge$, $\vee$, $\longrightarrow$, and $\neg$. Specify the domain of your quantified variable.

4. Invent a false proposition using both of these predicates and exactly one quantifier. You may use any of the logical operations of $\wedge$, $\vee$, $\longrightarrow$, and $\neg$. Specify the domain of your quantified variable.

Class Example:

Consider the statements: $E(x) : x$ is enrolled in the class $T(x) : x$ took the test

How would we say

1. Someone who is enrolled in the class took the test.
2. All students took the test.
3. All students enrolled in the class took the test.
4. Everyone who took the test is enrolled in the class.
5. At least one student who is enrolled in the class did not take the test.

Next week we are going to explore how to make more complicated statements with quantifiers, including things like:

- There is no largest integer
- n is prime
- x has a multiplicative inverse
- If x is nonzero then x has a multiplicative inverse.

2.2 Negations and Quantifiers

Let's talk about negations of quantifiers: The main rules are

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x)$$

$$\neg(\exists x P(x)) \equiv \forall x \neg P(x)$$

Look at what happened here: To negate a quantified statement, we switched the quantifier and negated the statement. You try a few:

Write down the negation of:

"Everyone at the movie likes popcorn".

The **negation is:**

"Someone at the zoo doesn't like penguins."

The **negation is:**

What about more complicated examples? Suppose I wanted to negate $\forall x(blah)$. What would the negation be?

Use this idea to negate the following:

$\neg(\forall x(P \wedge Q))$

Now let's work in groups on the following problems:

1. Translate each of the following into logical expressions, using

   P(x) "x is perfect."

   a) Everyone is perfect

   b) No one is perfect (Hint: you might want to start with $\neg\exists x$

   c) Not everyone is perfect (is part b saying the same thing as part a?)

2. Translate these statements into English where $R(x)$ is "x is a rabbit" and $H(x)$ is "x hops" and the domain of discourse consists of all animals.

   a) $\forall x(R(x) \longrightarrow H(x))$

   b) $\forall x(R(x) \wedge H(x))$

   c) $\exists x(\neg R(x) \wedge H(x))$

3. Advice for this problem: Ok, take a big breath! On this problem there are a LOT of statements, way too many to get through in the time we have. I've made these to give you opportunities to practice with quantifiers in both directions. For example, you might want to pick a random one from the right and try to phrase it in English (and see if your teammates agree) or you might want to take a statement from the left and try and match it with the symbols on the right. Decide as a team how long you want to spend working on this problem (you want to have time to get to the other ones as well) and then take turns saying what you think each statement means. I'll be around to help!

(Happy Valentine's Day!) Let $L(x, y)$ be the statement x loves y, where the domain for x and y consists of all people in the world. For example: $L(\text{Lisa, Mark})$ means that Lisa loves Mark and $\neg L(\text{Mark, Lisa})$ means that Mark does not love Lisa. (Notice the negation symbol there... love can be that way sometimes...) Use quantifiers to express each of these statements. Some possible statements are on the right. You can try to match these with your choices!

a. There is somebody whom Lydia does not love

b. There is somebody who doesn't love Lydia

c. Everyone loves Jerry

d. Everyone loves themselves

e. Jerry loves everyone

$\forall x\ L(x, \text{Jerry})$

$\exists x\ L(x, \text{Jerry})$

$\exists x\ L(\text{Jerry}, x)$

$\forall x\ L(\text{Jerry}, x)$

$\forall x\ L(x, x)$

$\exists x\ L(x, x)$

$\exists x\ L(x, \text{Lydia})$

$\exists x\ L(\text{Lydia}, x)$

$\exists x\ \neg L(x, \text{Lydia})$

$\exists x\ \neg L(\text{Lydia}, x)$

These next ones are more challenging - work very slowly on these. You've got this!

a. There is someone who loves everyone

b. There is someone whom everyone loves

c. Everyone is loved by somebody

d. Everyone loves somebody

e. There is someone whom no one loves (write the quantifiers for this one)

f. There is someone who loves no one (write the quantifiers for this one)

g. Nobody loves everybody (write the quantifiers for this one)

$\forall x \exists y\ L(x, y)$

$\exists y \forall x\ L(x, y)$

$\exists x \forall y\ L(x, y)$

$\forall y \exists x\ L(x, y)$

4. **Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.**

a) $\forall x \exists y (x^2 = y)$ **b)** $\forall x \exists y (x = y^2)$

c) $\exists x \forall y (xy = 0)$ **d)** $\exists x \exists y (x + y \neq y + x)$

e) $\forall x (x \neq 0 \rightarrow \exists y (xy = 1))$

f) $\exists x \forall y (y \neq 0 \rightarrow xy = 1)$

g) $\forall x \exists y (x + y = 1)$

h) $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$

i) $\forall x \exists y (x + y = 2 \wedge 2x - y = 1)$

j) $\forall x \forall y \exists z (z = (x + y)/2)$

Some items from the quiz:

- Are the following statements equivalent, or is one the converse of the other?

  A) If we go to school then we need to get up early

  B) We need to get up early If we go to school.

- What is the negation of $P \longrightarrow Q$?

Otherwise, the quiz went well. The median score was 83%.

We are now going to discuss what happens when we have **nested quantifiers**, that is, we have more than one quantifier in a statement. We'll do this with lots of examples. I recommend re-reading the zyBooks after this class and finishing the challenge activity from these sections.

The four types of nested quantifiers we will study are

$$\forall\forall, \qquad \exists\exists, \qquad \exists\forall, \qquad \forall\exists$$

Domain of discourse: $\{2, 4, 10, 24\}$

$$\forall x \forall y, \quad x + y \text{ is even}$$

Domain of discourse: $\{2, 3, 5, 7, 11\}$

$$\forall x \forall y, \quad x + y \text{ is even}$$

Domain of discourse: $\{3, 5, 7\}$

$$\exists x \exists y, \quad x + y \text{ is even}$$

Domain of discourse: $\{2, 3\}$

$$\exists x \exists y, \quad x + y \text{ is even}$$

Domain of discourse: $\{2, 3\}$

$$\exists x \exists y, \quad (y \neq x) \wedge (x + y \text{ is even })$$

Domain of discourse: $\mathbb{N}$ (positive integers)

$$\exists x \exists y, \quad x = y^2 + 5$$

$$\exists x \exists y, \quad x = -y^2 + 5$$

$$\exists x \exists y, \quad x = -y^2 - 5$$

Domain of discourse: $\mathbb{N}$ positive integers.

$$\exists x \exists y, \exists z \quad x^2 + y^2 = z^2$$

Quiz Questions:
$\forall x \forall y$: $(x+y)^2 = x^2 + y^2$.
$\exists x \exists y$: $(x+y)^2 = x^2 + y^2$.

Story Time: Domain of discourse: $\mathbb{N}$ (positive integers)

$$\exists x, \exists y, \exists z, \exists n \quad (n > 2) \wedge x^n + y^n = z^n.$$

It was first **conjectured** in 1637 that the answer to this question above was NO. That no matter how you looked, you could never find a solution to the above. What do you think? Do you think you could find, say a whole number solution to $x^3 + y^3 = z^3$. Or $x^7 + y^7 = z^7$?
Here's another one, it was also conjectured by hundreds of years that there was NO solution (in $\mathbb{N}$) to

$$x^4 + y^4 + w^4 = z^4.$$

Do you think there is a solution to these equations?

Some general takeaways:

- If you want to show that a statement like $\exists x \exists P(x,y)$ is TRUE...

- If you want to show that a statement like $\exists x \exists P(x,y)$ is FALSE....

- If you want to show that a statement like $\forall x \forall P(x,y)$ is TRUE...

- If you want to show that a statement like $\forall x \forall P(x,y)$ is FALSE...

Domain of discourse: $\{2,4,6,8,10\}$

$$\exists x \forall y \quad x + y = 12$$

$$\forall x \exists y \quad x + y = 12$$

$$\exists x \forall y \quad xy > 15$$

$$\forall x \exists y \quad xy > 15$$

Quiz Questions: Domain of discourse, all real numbers:

$$\forall x \exists y \quad 3x + 4y = 5$$

Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.

a) $\forall x \exists y (x^2 = y)$
b) $\forall x \exists y (x = y^2)$
c) $\exists x \forall y (xy = 0)$
d) $\exists x \exists y (x + y \neq y + x)$
e) $\forall x (x \neq 0 \rightarrow \exists y (xy = 1))$
f) $\exists x \forall y (y \neq 0 \rightarrow xy = 1)$
g) $\forall x \exists y (x + y = 1)$
h) $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$
i) $\forall x \exists y (x + y = 2 \wedge 2x - y = 1)$
j) $\forall x \forall y \exists z (z = (x+y)/2)$

The book talks about how to negate nested quantifiers using DeMorgan's Laws, I won't put any of those questions on the quiz. We'll get practice with this throughout the semester.

Warmup: Let $R(x, y)$ represent the statement x loves y. Below are different statements. What is each statement saying?

1. $\exists x R(x, Ann) \wedge \exists x R(x, Bob)$
2. $\exists x (R(x, Ann) \wedge R(x, Bob))$
3. $\exists x R(x, Ann) \wedge \exists y R(y, Bob)$
4. $\exists x \exists y R(x, Ann) \wedge \exists y R(y, Bob)$

The statement below says "Someone loves Ann."

$$\exists x R(x, Ann).$$

A student tried to modify this statement to encode "There are two people who love Ann.":

$$\exists x \exists y (R(x, Ann) \wedge R(x, Ann))$$

What is wrong with the student's statement? How could it be fixed?

2.3 Truth values for quantified statements with more than one quantifier

Consider the following predicate, and determine the truth value of each proposition below. If the proposition is false, give a counterexample or explain your reasoning. x and y are taken from the **domain of real numbers.**

$$P(x, y) : y = x^2$$

1. $\forall x \, \forall y \, P(x, y)$
2. $\exists x \, \exists y \, P(x, y)$
3. $\forall x \, \exists y \, P(x, y)$
4. $\exists y \, \forall x \, P(x, y)$
5. $\exists x \, \forall y \, P(x, y)$
6. $\forall y \, \exists x \, P(x, y)$

If you finish early, try inventing your own predicate with two free variables. Then go through these again. Or you could use the same predicate, but change the domain to integers.

STOP

2.4 Translation from math to english

Each predicate below has one (or several) free variable(s) coming from the specified domain. When translated into english, each predicate is a common mathematical definition. Determine what each predicate is defining. The first one is completed as an example

1. x, y are positive integers. $P_2(x) : \exists y \, (x = 2 \cdot y)$. "$x$ is even"
2. x, y are positive integers. $P_3(x) : \exists y \, (x = 3 \cdot y)$.
3. x, y, z are positive integers. $T(x, y) : \exists z \, (x^2 + y^2 = z^2)$.
4. x, y, d are positive integers. $R(x, d) : \exists y \, (x = d \cdot y)$.
5. x, y, d are positive integers. $S(x) : (x > 1) \wedge (\forall d (R(x, d) \rightarrow (d = 1 \vee d = x)))$.

STOP

2.5 Translation from english to math

(These questions are related to our first "mini-project"!) In the following questions, a mathematical definition is given. See if you can translate each definition into a predicate. Specify the domain of all variables (free and bound). You may use any of the predicates above to assist you.

6. "x is odd." *(Hint: every odd number is one more than an even number.)*
7. "x has remainder 1 when divided by 12."
8. "x has remainder r when divided by 12."
9. "x has remainder r when divided by d."
10. "x is a product of exactly two prime numbers."

STOP

2.6 Homework Problems

Due: Friday February 11th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Each week I will give many problems for practice preparing for the quizzes

- Some of the problems will be from the textbook. I have decided to show the solutions to these problems so you can check your answers. The goal of homework is to give you practice solving problems and help you prepare for the quizzes. I will also give some additional problems for you to work through. I'll provide some solutions or hints for some of t these problems.

1. Work on the following textbook problems. You don't need to write out solutions to ALL of these, but please solve a total of **at least 9** of these problems. Try to write down your solutions first, and then check the answers. If you made mistakes, make a note about what you learned and mark this on your paper. I will be grading these homework problems for completion. The notes that you write down can be helpful as you work on the quiz.

   (I know this seems like a lot of problems, but my goal is to pick out problems that will help you get **practice**. That's why I only require you to submit some of these. I also realize that many of these problems have a gazillion parts. It's completely ok if you don't do every one of these parts. But remember, the more practice, the more fluency we'll have!

   2.1.1, 2.1.2, 2.1.3, 2.1.4

   2.2.1abcd, 2.2.2, 2.2.6, 2.2.8 (optional, but recommended: 2.2.3, 2.2.4, 2.2.5, 2.2.9)

   2.3.1, 2.3.2, 2.3.3

   2.4.2, 2.4.3, 2.4.4,

   2.5.2abcd, 2.5.4abcfg, (for a challenge: 2.5.6)

   Additional Problems

2. One of the skills we want to develop in this class is the skill of **problem solving** especially with problems we might never have solved before. How do we get better at problems like this? By practicing! So that's what we'll do.

   Problem: For what real numbers a does the equation

   $$(x-3)(x+5) = a$$

   have a **unique solution?**

   On this homework I'm not so much interested in your solution, (for instance there's probably a solution online you could copy down, I'm not sure), but I'm interested in hearing your thoughts about this problem.

   - Does the problem make sense? What does the word unique mean? If the problem doesn't make sense, what can you do about it (ask friends, go to office hours, draw a picture?)
   - What are some things you can try to get started. Could you let $a = 0$? What would the solutions to the equation be in that case? Would you say there's a unique solution in that case? Does that help make sense of what "unique" means? What if $a = 100$?
   - Are you discovering that maybe you have trouble solving equations like $(x-3)(x+5) = 100$? That's ok - think back, how do you solve **quadratic equations? key words: graphing, FOILing out, factoring, quadratic formula.**

- What can a graphing calculator do? If you let $a = 10$ what would you be looking for on the graph? What would the word "unique" mean?
- Some students tried to factor this and noticed that "unique solution" would mean "the same factor occurs twice". What would that repeated factor have to be? Could it be $(x+3)$? $(x+2)$? Why do you know? Hint: look at the middle term of the quadratic.

On this assignment please describe your approach to this problem. If you were stuck, that's ok - but say what you tried. Did you graph? Did you multiply it out? How long did you struggle? Did you talk with friends? Which of the above techniques did you try? after the fact, which of these were ideas that you think might have helped?

There's no right or wrong answer of course - but in this course we will see challenging problems that we haven't seen before. And one thing we will need to practice is to practice feeling "stuck" and being creative about how we find solutions. We get better at problem solving by practicing!

3. Quiz Problem: Do this problem on a separate sheet of paper. You will turn this is as part of your quiz. You may ask about this problem in office hours and you may work with your classmates. You may NOT post this question online or look for solutions on the internet. If you're stuck, just let me know - I'm here to help!

Are the following statements true or false?

The domain for this problem is the set of all real numbers:

Statement 1: $\forall x \forall y$: $(x+y)^2 = x^2 + y^2$.

Statement 2: $\exists x \exists y$: $(x+y)^2 = x^2 + y^2$.

Statement 3: $\forall x \exists y$: $3x + 4y = 5$.

- If it is true, explain why.
- If it is false, explain why.
- Be specific and as clear as possible.
- If you are claiming that something is true for all x then you need to argue why this is true for all x. This might require a few short sentences. For instance, if I asked you to explain why $\forall x \exists y (x + y = 0)$ I might write:

  "I am being asked to show that for all real numbers x there is a real number y with the property that $x + y = 0$. I can just let $y = -x$. Then $x + y$ will equal $x + (-x) = 0$. This is a general argument, but if you want to see an example, suppose that $x = 15$ then I would let $y = -15$ and then sure enough $x + y = 15 + (-15) = 0$."

- If you are claiming that something exists, you can just give that example. For instance, if I said to explain why $\exists x (x^2 + 4 = 13)$. You could just write: "Such an x exists, since e.g. $x = 3$ satisfies $x^2 + 4 = 13$."
- Similarly if you are showing that something does not hold for all x, you can just clarify this by giving a single counterexample. For example, if I asked you to prove that the following statement was false: $\forall x (x^2 < 50)$ you could write:

  "This statement is false because it is NOT true that x^2 is always less than 50. For instance, if we let $x = 20$ then $x^2 = 400$ which is bigger than 50. So the original statement is false."

- Feel free to use these models as an example for this problem.

Quiz 2

Name: _____

1. Using the table below, determine whether or not the statements on the right are True or False. The domain for x is the set of names, Ann, Bob and Joe.

Names	A(x)	B(x)	C(x)	D(x)
Ann	F	F	F	F
Bob	T	F	T	F
Joe	F	F	F	T

$\forall x(A(x) \vee B(x))$

$\forall x(C(x) \longrightarrow A(x))$

$\exists x(B(x))$

2. Let $Q(x)$ be the statement "x likes math." (Domain of discourse is all students on earth). Which of the following is equivalent to $\forall x\ \neg Q(x)$?
   (a) All students like math.
   (b) Someone doesn't like math
   (c) No students like math

3. Let $Q(x)$ be the statement "x likes math." (Domain of discourse is all students on earth). Which of the following is equivalent to $\neg \forall x Q(x)$?
   (a) All students like math.
   (b) Someone doesn't like math
   (c) No students like math

4. Which of the following is the negation of $(\forall x P(x)) \longrightarrow Q$
   (a) $\neg Q \longrightarrow \neg(\forall x P(x))$
   (b) $Q \longrightarrow \forall x \neg P(x))$
   (c) $Q \wedge \forall x \neg P(x)$
   (d) $Q \vee \neg(\forall x P(x))$
   (e) $\forall x P(x) \wedge \neg Q$

5. Let $L(x, y)$ be the statement x loves y. Which of the following is represented by: $\forall x \exists y L(x, y)$
   (a) Someone loves everyone
   (b) Everyone loves someone
   (c) Everyone loves everyone
   (d) Someone is loved by everyone
   (e) Everyone is loved by someone
   (f) Someone loves someone

6. If the domain of discourse is $\{3, 5, 7, 10\}$ which of the following are true? Circle all that are true:
   (a) $\exists x \exists y \quad x + 2y = 130$
   (b) $\exists x \exists y \quad x < y$
   (c) $\forall x \forall y \quad x < y^2$
   (d) $\exists x \forall y \quad x \leq y$
   (e) $\exists x \forall y \quad x \leq y$

3 Definitions and Proofs Day 1!

In the reading we learned some definitions. Let's review those here:

An integer n is called **even** if

An integer n is called **odd** if

Let a and b be integers. We say that $a\|b$ (read "a divides b") if

1. Some practice:
   (a) Which is true: $6|3$ or $3|6$ (or both)?

   (b) Are there any numbers a and b (different) with $a|b$ and $b|a$?

   (c) What is $2|b$ saying about the number b?

   (d) The statement "If $2|n$ and $2|m$ then $2|(n+m)$" is saying what familiar property about numbers?

   (e) If n is an integer, is the number $4n+3$ even or odd. Why? can you use the definition?

   (f) If n is an integer, is the number $4n-3$ even or odd. Why? can you use the definition?

   (g) If n is an integer, is the number $4n^2+14n+2$ even or odd. Why? can you use the definition?

   (h) If n is an integer, is the number $n(n+1)$ even or odd? (This one will be harder to match with the definition - but talk it through with your group.)

STOP

2. It might seem surprising to you, that we could every prove something is true for ALL positive integers, since there are infinitely many. Once you get the hang of writing proofs you'll see that it's not so bad. In this problem we'll explore how to write a proof that:

   "The equation $x^2 = 4y + 3$ has no solutions if x and y are positive integers."

   How do you think you could ever show that an equation like this has NO solutions? You can't possibly check all possibilities since there are infinitely many. What we need is an argument, that will work no matter what.

STOP

3. **Definition:** We say that a positive integer n is a **Torero number** if

   - n has at least 2 different prime factors
   - n is even

   (a) For each of the first 25 positive integers, determine whether or not they are Torero numbers. (You don't have to write a justification, just make sure you understand what the properties are).

   (b) The following statement is false. Explain why, by giving a counterexample.

   "If x is a positive integer that is even then x is a Torero number."

   (c) The following statement is true. Explain why in your own words:

   "If n is a Torero number, then $4n+3$ is NOT a Torero number."

   (d) The following statement is true. Explain why, in your own words:

   "If n is a Torero number then, n has at least 4 different factors."

   (e) (Optional) The following statement is true. Explain why, in your own words:

   "If p is a prime, then for any natural number n, p^n is NOT Torero."

   (f) Write down your own true statement about Torero numbers. Your statement should be something like: "If x is a Torero number then .... "

Writing our Own Proofs!

There is a supplemental reading (optional, but highly recommended in our google drive folder with the worksheets. It is all about proof, and I think it presents some topics very clearly.

Our goal this week and next is to practice writing mathematical proofs. The goal is to write clear, correct proofs that justify the statement. I'll present some in class and you'll work on your own in groups as well. You may want to read ahead in the book.

Warmup: Read the following statements and see what you think about them. Do any of these seem more interesting to you? What would you need to do to **prove** or **justify** your answer.

1. Given 101 points in the plane, no three of which lie on the same line, explain why there exists a line through one of the points that neatly divides the remaining points in half, with fifty points on either side.
2. There exist 1000 positive integers in a row, none of which are prime. (These numbers are called **composite numbers** is a positive integer that is not prime.)
3. Ten children at a part collect a total of 74 pieces of candy from a piñata. Prove there is some child who received at least 8 pieces of candy.
4. There are infinitely many primes.
5. Your friend tells you that there is a perfect square that is bigger than 10 and that is exactly one more than a prime number. Show that your friend is not correct. (This will require writing a proof!)
6. Show that if n is an even integer and $n > 2$ then n is equal to the sum of two primes numbers.

Do you have any ideas about how to solve the problems above?

Here are some more problems that you might find intriguing:

---

7. If p is prime then $(p-1)!+1$ is divisible by p. (Quite hard!)
8. If n is an integer then there is always a prime p between n and $2n$. That is, there is a prime p such that $n < p < 2n$. (Very hard!)
9. Can you a positive integer solution to the equation $x^2 - 7y^2 = 1$. Can you find more than one? Can you find more than 20?

Before we learn how to solve challenging problems like the ones above, we will get lots of practice by working with more familiar concepts.

10. The equation $x^2 = 4y + 3$ has no solutions if x and y are required to be positive integers.

11. If x and y are integers and $x + y$ is even then $x - y$ is even.

12. If m is a positive integer such that $3m + 7$ is odd, then $5m - 10$ is even.

13. If k is a positive integer such $5k - 1$ is even. Prove that $9k + 13$ is even.

14. Suppose that n and m are integers and $n \neq 0$. If $n \mid m$ then $n \mid m^2$. Is the converse true?

Writing our own proofs, day 2:

In the last class we saw an example of what is called a **direct proof.** where we started with the _____ proceeded step by step to the _____.

We will spend some time in class today writing some direct proofs in groups. I will assign you one of the two problems:

1. If m is a positive integer such that $3m + 7$ is odd, then $5m - 10$ is even.
2. If k is a positive integer such $k - 1$ is even. Prove that $k^2 + 2k$ is even.

We will work for 10 minutes on these and then share our work.

STOP

Now for something using the divisibility. Remember:

$\heartsuit \mid \triangle$ means that "there is an integer k such that:

1. Suppose that n and m are integers and $n \neq 0$. Prove that if $n \mid m$ then $n \mid m^2$.
2. Suppose that m and x are integers and $m \neq 0$. Prove that if $m|(x-3)$ then m divides $x^2 - 9$.

STOP

Definition:

A number a is called rational if there exist integers m, n such that $n \neq 0$ and $a = \frac{m}{n}$.

Read the following two statements and think about how we might start a direct proof. One should feel more natural than the other.

1. Prove that if r and s are rational numbers then so is $r + s$. (This is proven in the zybooks. Let's take a look.)
2. Prove that if a is not rational then $a + 7$ is not rational.

Proof by Contrapositive

For Friday's reading, you will be reading two sections with lots more examples of proofs, including a method called "proving the contrapositive." Here are the main highlights be on the look for while you are reading.

- Imagine we are trying to prove that $P \longrightarrow Q$.
- It turns out that this is **logically equivalent** to the contrapositive, $\neg Q \longrightarrow \neg P$
- So we can prove either the original statement or the **contrapositive**.
- WARNING: the contrapositive - not the converse
- Why bother? Well the contrapositive may be easier to work with. Let's see an example.

Here are two examples of problems we could prove by contraposition:

1. Let β be an irrational number. Use proof by contrapositive to prove that $\beta - 4$ is also irrational.
2. Prove that if $x^3 + 5x = 40$ then $x < 3$.

8. State the contrapositive of each of the following implications. Then decide whether you would prefer to prove the original statement or the contrapositive. (You do *not* actually need to prove these statements.)

a) Let m and n be positive integers. Prove that if m^3 is not divisible by n^3, then m is not divisible by n.

b) Show that for a real number x, if $x > 1$ then $3^x > 3x$.

c) For finite sets A and B, prove that if $A \not\subseteq B$ then $|A| \geq 1$.

d) If all the sides of a triangle have different lengths, then all of its angles have different sizes.

Chapter 3 Homework Problems

Due: Friday February 18th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

1. Book Problems:

   3.1.1, 3.1.2, 3.1.4, 3.1.6,

   3.2.1, 3.2.2a, 3.2.3abe, 3.2.4, 3.2.5 (pick a few of these and make sure you can solve these)

   3.3.1cd

   3.3.3

2. This section of the book mostly focuses on the giving definitions and the structure of proofs. The quiz this week will ask you e.g. to explain why -5 is odd, by using the definition. It might ask you what $5 \mid 65$ is saying and whether or not it is true. To give you practice with these things, here's a new definition:

   Definition: We say that a positive integer n is a **Torero number** if

   - n has at least 2 different prime factors
   - n is even

   (a) For each of the first 25 positive integers, determine whether or not they are Torero numbers. (You don't have to write a justification, just make sure you understand what the properties are).

   (b) The following statement is false. Explain why, by giving a counterexample.

   "If x is a positive integer that is even then x is a Torero number."

   (c) The following statement is true. Explain why in your own words:

   "If n is a Torero number, then $4n+3$ is NOT a Torero number."

   (d) The following statement is true. Explain why, in your own words:

   "If n is a Torero number then, n has at least 4 different factors."

   (e) (Optional) The following statement is true. Explain why, in your own words:

   "If p is a prime, then for any natural number n, p^n is NOT Torero."

   (f) Write down your own true statement about Torero numbers. Your statement should be something like: "If x is a Torero number then .... "

   On the quiz, I might ask you questions about Torero numbers. You can use this homework to write your answers.

3. In class we showed that the equation $x^2 = 4y+3$ has NO solutions if x and y are positive integers. In this problem I want you to explore what sorts of solutions the following equations have. You should find that some of these DO have solutions, and some do not. For the ones that have solutions, write down one solution, and for the ones that do NOT have solutions, can you think of an argument that might explain why? Let me know your thoughts!

   - $x^2 = 4y+3$
   - $x^2 = 5y+3$
   - $x^2 = 6y+3$
   - $x^2 = 7y+4$

Quiz 3

Name: _____

1. This problem is about using **definitions.** Please complete the following sentences.

By definition, to say an integer $x + y$ is even means that

By definition, to say an integer $w - 2k$ is odd means that

By definition, to say that xw divides z means that

2. For each of the following, circle the statements that are TRUE.

1. Providing one example when the statement holds is sufficient to prove an existential statement.
2. Showing that a statement holds for a few cases is sufficient to prove a universal statement.
3. Providing one counterexample is sufficient to disprove a universal statement.
4. Proof by exhaustion can be used to prove a universally quantified statement with a finite domain.

3. Which of the following is meant by the true statement: $4|28$?

a.) 7

b.) 4 divided by 28

c.) 28 divided by 4

d.) 28 is an integer multiple of 4.

4. Which of the following are counterexamples to the statement:

"If $4|x^2$ then $4|x$"

(CIRCLE ALL THAT APPLY)

- $x = 1$
- $x = 2$
- $x = 6$
- $x = 4$
- $x = -4$
- $x = 16$

Quiz 3

Name: _____

1. This problem is about using **definitions.** Please complete the following sentences.

By definition, to say an integer $x + y + z$ is even means that

By definition, to say an integer $3w + 2k$ is odd means that

By definition, to say that $a - b$ divides z means that

2. For each of the following, circle the statements that are TRUE.

1. Providing one example when the statement holds is sufficient to prove an existential statement.
2. Showing that a statement holds for a few cases is sufficient to prove a universal statement.
3. Providing one counterexample is sufficient to disprove a universal statement.
4. Proof by exhaustion can be used to prove a universally quantified statement with a finite domain.

3. Which of the following is meant by the true statement: $4|28$?

a.) 7

b.) 4 divided by 28

c.) 28 divided by 4

d.) 28 is an integer multiple of 4.

4. Which of the following are counterexamples to the statement:

"If $4|x^2$ then $4|x$"

(CIRCLE ALL THAT APPLY)

- $x = 1$
- $x = 2$
- $x = 6$
- $x = 4$
- $x = -4$
- $x = 16$

Quiz 3

Name: _____

1. This problem is about using **definitions.** Please complete the following sentences.

By definition, to say an integer xyz is even means that

By definition, to say an integer $3z + 2k$ is odd means that

By definition, to say that ab divides z means that

2. For each of the following, circle the statements that are TRUE.

1. Providing one example when the statement holds is sufficient to prove an existential statement.
2. Showing that a statement holds for a few cases is sufficient to prove a universal statement.
3. Providing one counterexample is sufficient to disprove a universal statement.
4. Proof by exhaustion can be used to prove a universally quantified statement with a finite domain.

3. Which of the following is meant by the true statement: $4|28$?

a.) 7

b.) 4 divided by 28

c.) 28 divided by 4

d.) 28 is an integer multiple of 4.

4. Which of the following are counterexamples to the statement:

"If $4|x^2$ then $4|x$"

(CIRCLE ALL THAT APPLY)

- $x = 1$
- $x = 2$
- $x = 6$
- $x = 4$
- $x = -4$
- $x = 16$

Proof by Contrapositive and Contradiction

As a warmup let's prove the following lemma. (A lemma is a minor mathematical statement that is often used in support of a larger argument. We will use it later today to prove that $\sqrt{2}$ is irrational.

Lemma: Suppose that n is an integer. If n^2 is even then n is even.

Proof: Let _____ We will prove the contrapositive which states that IF _____ THEN _____. We will now start that proof.

Suppose that _____.

Extra Practice: Prove that if n^2 is odd then n is odd. At the end of the semester on our final exam, this would be a very reasonable problem to ask you to do in a timed setting.

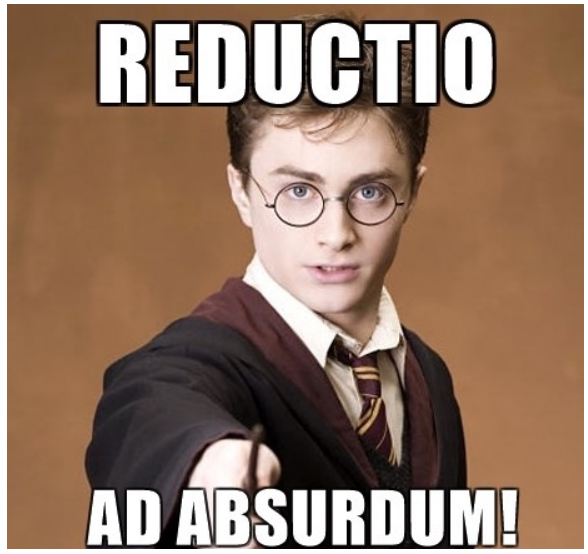
Now let's prove an "if and only if" statement. Such statements are best thought of with the $\iff$ notation, which reminds us that there are TWO statements, one going in each direction.

Another very important method of proof is called **Proof by Contradiction**. This is sometimes called Reductio Ad Absurdum in philosophy classes, and follows this rough format: "Ok, so suppose your hypotheses were true, but the conclusion **failed**. If I can show you that this leads to some absurd statement, then I'll have convinced you that the conclusion must actually be **true.**"

"Oh, sure - and by absurd statement you mean something we know can't be true. Something like

'$1 + 1 = 4$.' or 'x is even and odd at the same time.'

"Yep!"



Proposition: There does not exist a largest natural number.

Proof: We will argue by contradiction. Suppose that N is a number that is the largest natural number. This means that $N \geq m$ for every _____. But this cannot be true, because _____ is another natural number and if it were really true that N was $\geq$ **every** natural number, then that would mean $N \geq$ _____. Which would imply that

_____

We have reached a contradiction, so our original supposition must have been incorrect. Therefore there can be no largest natural number. $\square$

Proposition: There is no smallest positive rational number.

Proof: We will argue by contradiction. Suppose that there *were* a smallest rational number, call it x. Then

[can you fill in the proof? can you think of how we can get a contradiction]

And now a big Theorem (a Theorem is a larger or important true mathematical statement)

Theorem: The square root of 2 is irrational. I.e. there is no rational number that is a solution to the equation

$$x^2 = 2.$$

Proof: We will argue by contradiction. Suppose that there *were* a

We are going to investigate some "if and only if statements" in this class. I like to think about it with a double arrow. Let's see which directions you think are true:

The domain of discourse for all of this is the set of positive integers

Statement 1:

$$x, y, z \text{ is a solution to } x^2 + y^2 = z^2 \quad \boxed{} \quad x = 3, y = 4, z = 5$$

Statement 2:

$$x, y, z \text{ is a solution to } x^2 + y^2 = z^2 mbox \boxed{} \quad x = n, y = n + 1, z = n + 2 \text{ for some } n \in \mathbb{N}.$$

Statement 3:

$$x, y, z \text{ is a solution to } x^2 + y^2 = z^2 \quad \boxed{} \quad x =, y = k + 1, z = k + 2 \text{ for some } k \in \mathbb{N}.$$

This one is fun! Suppose that x, y are positive real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$ then $12x^2 + 10y^2 < 24xy$.

Chapter 4 Homework Problems

Due: Wednesday February 23rd

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

This week we will do something different. There will be no homework due, but instead, you will work on some proof problems and turn them in as a take-home quiz.

Instead of homework, I recommend you take a look at the mini project and get started on that.

Quiz 4:

Please write out proofs for the following problems. You may work together with your classmates, but I expect you to write your own solutions in your own words.

- Please rewrite each statement on your paper before your proof;
- make sure that you introduce each variable that you use;
- make sure everything you write is a complete sentence;
- I recommend beginning ALL of these proofs by writing "Let ..." and then introduce your variables. This is important.
- If you are going to argue by contrapositive, after introducing your variables, I recommend writing 'We will prove the statement by proving the contrapositive, which states...."
- some (or most) of the problems below might require proof by contrapositive.

The problems:

1. Suppose that b is an integer. Prove that if $9|b$ then $3|(15+2b)$.
2. Suppose that n is an integer. Prove that if n^2-2n-1 is even then n is odd.
3. Suppose x and y are real numbers. Prove that if $x+2y$ is irrational then either x is irrational or y is irrational.
4. Suppose x is a real number. If $x^5+4x^4+3x+4=100$ then $x<2$

Please write neatly and leave at least several inches of space after each problem so I can write feedback.

The proofs will be graded on the following rubric:

- 5 points: Your proof is complete mathematically. It could appear in a textbook as an example of a solid proof. All of your variables are clarified. If you are arguing by contrapositive, you have stated this. Your proof makes your assumptions clear and it is comfortable for the reader to follow your steps to reach the conclusion. Even when using mathematical equations or inequalities, your writing still consists of complete sentences.
- 4 points: Your proof is mathematically correct, with perhaps one or two minor issues. Your writing is still clear, but there is a sentence or two that could be further clarified.
- 3 points: Your proof has portions that are challenging to follow and does not meet the standards for receiving 4 or more points.
- 0 points: You have submitted only some symbols, equations, with little or no justification.

Some extra practice:

1. Disprove the assertion that "For positive integers m, if $m+1$ and $5m+1$ are both perfect squares, then $m = 3$."
2. Find a disproof of the statement: "For real numbers x and y, if $x^2 + 3x = y^2 + 3y$ then it follows that $x = y$.
3. Prove that if x, y are positive real numbers then $\frac{x}{y} + \frac{y}{x} \geq 2$.
4. Show that a positive integer n is even if and only if n^2 ends with one of the digits, $0, 4, 6$.
5. Prove that if $x^3 + 5x = 40$ then $x < 3$.
6. If $x^2 + y^2 = z^2$ then either x or y must be even.
7. $\sqrt{2}$ is irrational.
8. Given 102 points in the plane, no three of which lie on the same line, prove that there exists a line passing through two of the points which divides the remaining points in half, with fifty points on each side of the line.

Quiz 4:

Please write out proofs for the following problems. You may work together with your classmates, but I expect you to write your own solutions in your own words.

- Please rewrite each statement on your paper before your proof;
- make sure that you introduce each variable that you use;
- make sure everything you write is a complete sentence;
- I recommend beginning ALL of these proofs by writing "Let ..." and then introduce your variables. This is important.
- If you are going to argue by contrapositive, after introducing your variables, I recommend writing 'We will prove the statement by proving the contrapositive, which states...."
- some (or most) of the problems below might require proof by contrapositive.

The problems:

1. Suppose that b is an integer. Prove that if $9|b$ then $3|(15+2b)$.
2. Suppose that n is an integer. Prove that if n^2-2n-1 is even then n is odd.
3. Suppose x and y are real numbers. Prove that if $x+2y$ is irrational then either x is irrational or y is irrational.
4. Suppose x is a real number. If $x^5+4x^4+3x+4=100$ then $x<2$

Please write neatly and leave at least several inches of space after each problem so I can write feedback.

The proofs will be graded on the following rubric:

- 5 points: Your proof is complete mathematically. It could appear in a textbook as an example of a solid proof. All of your variables are clarified. If you are arguing by contrapositive, you have stated this. Your proof makes your assumptions clear and it is comfortable for the reader to follow your steps to reach the conclusion. Even when using mathematical equations or inequalities, your writing still consists of complete sentences.
- 4 points: Your proof is mathematically correct, with perhaps one or two minor issues. Your writing is still clear, but there is a sentence or two that could be further clarified.
- 3 points: Your proof has portions that are challenging to follow and does not meet the standards for receiving 4 or more points.
- 0 points: You have submitted only some symbols, equations, with little or no justification.

Solutions to the quiz.

Overall Comments:

D. You need to start your proofs by introducing your variables. For instance, "Let b be an integer." In addition you should say "Suppose that..." or "Assume that ..." when you state your hypotheses.

S. Remember that a proof is a communication and uses complete sentences. This means that sentences need to have beginnings, punctuation, etc.

P Proofs should start with the word "Proof". This is so that we know you are transitioning from the statement of the fact to the proof of the fact.

A It is important to not "assume what you are trying to prove." This happened e.g. in 1) when some people worked with the expression:

$$3|(15+2b)$$

and then simplified to get to something that was true. This is understandable, but logically we want to start with our premises and then end with our conclusion. It's completely ok to do something like: "Let's look at $15+2b$ and see if $3|(15+2b)$ is true. Ok,

$$15+2b = 15+18k = \ldots''$$

and then continue from there. It's not clear as a proof if you start working with the expression $3|(15+2b)$.

1. The student proof below is excellent, the only small issue is that the word "Proof" should be written on the second line. The first line is the statement, so it should be labeled as "Fact" or "Theorem" or "Proposition". Note how the writer clearly defined every letter and guided ther read from the hypothesis (about b) to the conclusion about $15 + 2b$.

1) Proof: If $9|b$ for some integer b, then $3|(15+2b)$
Suppose that b is an integer and that $9|b$. Since $9|b$, $b=9k$ for some integer k.

$$b=9k$$
$$2b=18k$$
$$15+2b=15+18k$$
$$15+2b=3(5+6k)$$

$\therefore$ Since k is an integer, $5+6k$ is an integer. This shows that $15+2b=3(\text{an integer})$ which means that $3|(15+2b)$ by definition.

Major Errors that I saw while grading:

A Most people correctly interpreted $9|b$ as meaning "b is an integer multiple of 9." But it was common to then not do the same thing with $(15+2b)$. I saw attempts to treat the expression $3|(15+2b)$ like an equation that could be modified. Remember this is what we are trying to prove, so it should appear only at the very end of our proof.

DI In your proof you used a letter to represent two different things. For instance, you might have written:

$$15 + 2(9k) = 3k$$

when really you meant: "I want to see is there is some (likely different) integer j so that

$$15 + 2(9k) = 3j."$$

Minor Errors that I saw while grading:

H It is helpful for the reader to help them see exactly what you are doing, and to be able to go back and see the information. For instance, in the proof above you can clearly see the equation:

$$15 + 2b = 3(5 + 6k).$$

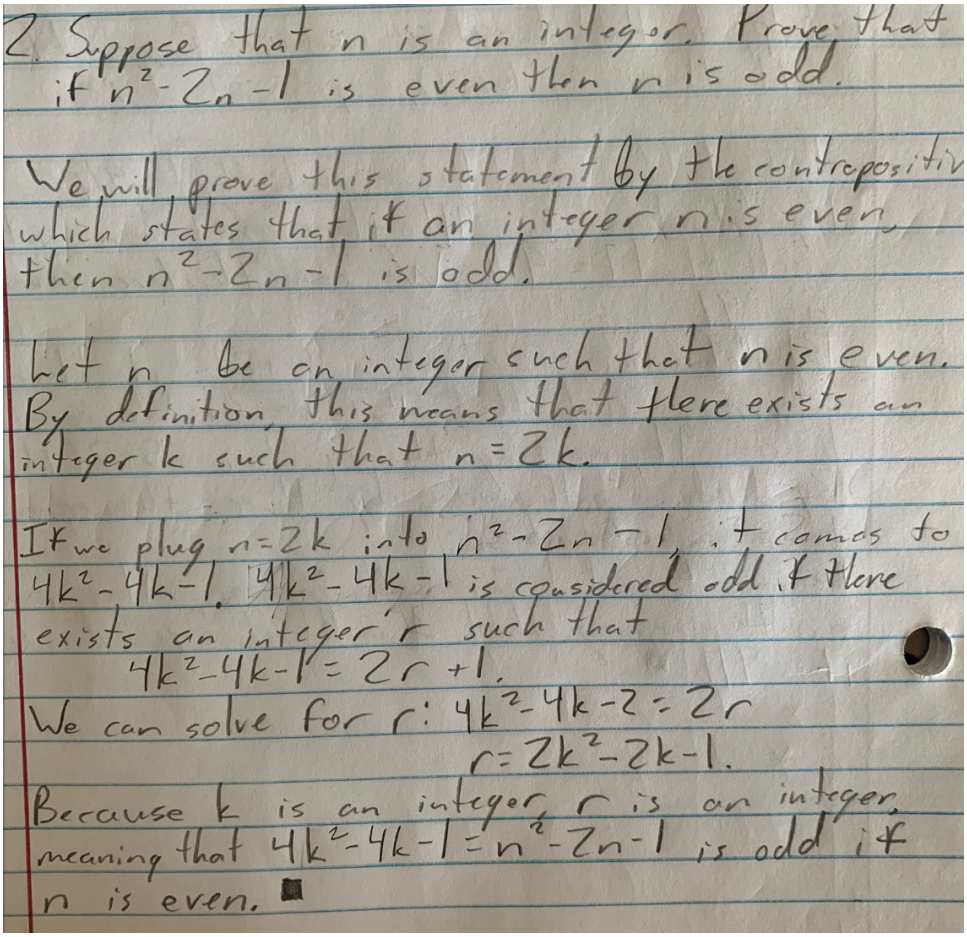
This helps the reader connect $15 + 2b$ with "divisible by 3" which is what we wanted to look at. It was common for some proofs to just have something like:

$$15 + 2(9k)$$
$$= 15 + 18k$$
$$= 3(5 + 6k)$$

the reader would be helped if you just wrote this instead as:

$$15 + 2b = 15 + 2(9k)$$
$$= 15 + 18k$$
$$= 3(5 + 6k)$$

2. The student proof below is very well-written and is almost completely correct, but has a serious issue somewhere. Can you see where? See if you can determine the issue before reading. Then check out the 1st item in the major errors section.



2. Suppose that n is an integer. Prove that if n^2-2n-1 is even then n is odd.

We will prove this statement by the contrapositiv which states that if an integer n is even, then n^2-2n-1 is odd.

Let n be an integer such that n is even. By definition, this means that there exists an integer k such that $n=2k$.

If we plug $n=2k$ into n^2-2n-1, it comes to $4k^2-4k-1$. $4k^2-4k-1$ is considered odd if there exists an integer r such that

$$4k^2-4k-1=2r+1.$$

We can solve for r: $4k^2-4k-2=2r$

$$r=2k^2-2k-1.$$

Because k is an integer, r is an integer, meaning that $4k^2-4k-1=n^2-2n-1$ is odd if n is even. ■

Minor Errors that I saw while grading: P You are missing the word proof. W You have written even or odd in a place where you meant the other.

Major Errors that I saw while grading:

1. To show that a number is odd, by using the definition, it is necessary to show that the number is in the form $2k+1$. I know it seems like $2k-1$ is close, or even the same. But when we are matching definitions we need to match them 100%. You can think about it as a computer program. The computer is looking for

   - 2 times
   - an integer
   - +1

   In this case, the computer would read -1 and not know that this means the integer is odd, there is more work to do. The correct way to correct this is to just "borrow" a little bit inside the parentheses. Let's see how this works in general. Say you have something like $x = 6n-1$ and you want to write it as $2(int)+1$. Well we could just do

   $$x = 6n-1 = 6n-2+1 = 2(3n-1)+1.$$

   Notice in the middle I took the -1 and rewrote it as $(-2)+1$ so I could get the +1 explicitly.

2. Some proofs didn't connect the algebraic expressions to the quantity we want to study. If e.g. you write correctly that $n = 2k$, then you need to tell the reader that you are about to study the number n^2-2n-1 (as

opposed to any other number). Also it's important to connect this result at the end of the statement so that you remind the reader that you have done what you said you would. Notice the student proof above, how they indicate exactly what they are plugging in, and then at the end they connect it to $n^2 - 2n - 1$ again. When in doubt use equations rather than just expressions. Write:

$$n^2 - 2n - 1 = (2k)^2 - (2k) - 1 = \ldots$$

rather than just starting in the middle.

3. Some people tried factoring out a negative to deal with the -1. Let's see if/why this may/may not work. Suppose I want to show that x is odd, and I have some expression $x = 2k - 1$. While it's certainly true that

$$-x = -2k + 1$$

$$-x = 2(-k) + 1$$

this provides a proof that $-x$ is odd. It does not show that x is odd.

3.

3) Suppose x and y are real numbers. Prove that if $x+2y$ is irrational, then either x is irrational or y is irrational.

Proof: I will argue by contradiction, which states that if x is rational and y is rational then $x+2y$ is rational.

Let x and y be rational numbers where $x=\frac{a}{b}$ and $y=\frac{c}{d}$, where a, b, c, and d are integers and $b \neq 0$ and $d \neq 0$.

Then, $\left(\frac{a}{b}\right)+2\left(\frac{c}{d}\right) = \frac{a}{b}+\frac{2c}{d}$

$= \frac{ad}{bd}+\frac{2cb}{bd} = \frac{ad+2cb}{bd}$

The fraction $\frac{ad+2cb}{bd}$ is rational because the numerator is an integer, and the denominator is also an integer that $\neq 0$. Therefore, $x+2y$ is rational, which is my goal. So my original supposition must be correct. ∎

Major Errors that I saw while grading:

RAT To show that a number is rational you must show 2 things,

1) that it can be written as one fraction, with the numerator and denominator both integers.

2) that the denominator of this new fraction is nonzero.

1. To argue by contrapositive the correct hypothesis is the negation of "x or y is irrational" which is x is rational AND y is rational. Remember that negating will switch AND/OR.

2. If you wrote a proof that used that x was rational but you didn't know that y was rational. (Maybe you had the incorrect statement of the contrapositive?) then be very careful: I saw some arguments like: "If x is rational then $x = m/n$ for some integers m, n and $n \neq 0$. Then

$$x + 2y = \frac{m}{n} + 2y = \frac{m + 2ny}{n}$$

and this is rational since the numerator and denominator are integers....

> if we don't know that y is an integer, (maybe it's π or $\sqrt{2}$?) then we can't conclude that the numerator is an integer.

Z There needs to be some justification that the denominator of your resulting fraction is nonzero. Remember that since x and y are rational, this means their denominators are nonzero, and you can use this.

4.

Suppose x is a real number. If $x^5+4x^4+3x+4=100$ then $x<2$

Proof by Contrapositive: We will prove that statement by proving the contrapositive, which states that if $x \geq 2$, then $x^5+4x^4+3x+4 \neq 100$.

Using the lowest possible number x could be since $x \geq 2$, we will let $x=2$

Since $x=2$, we can say $2^5+4(2)^4+3^{(2)}+4 \neq 100$

$$32+4(16)+6+4 \neq 100$$

$$32+64+6+4 \neq 100$$

$$96+10 \neq 100$$

$$106 \neq 100$$

Since x's lowest possible value, 2, results in 106 which is greater than 100, we can assume that every other possible value of x, which can only get bigger, will not equal 100.

Therefore, by contrapositive, if $x^5+4x^4+3x+4=100$, then $x<2$ ∎

Major Errors that I saw while grading:

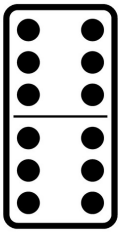
IQ Your proof only discusses what happens when $x = 2$. You need to include something about what happens for $x \geq 2$. I wasn't too picky about this, so long as you gave some indication that "If $x \geq 2$ then the values will increase because the polynomial has all positive coefficients" or something like that.

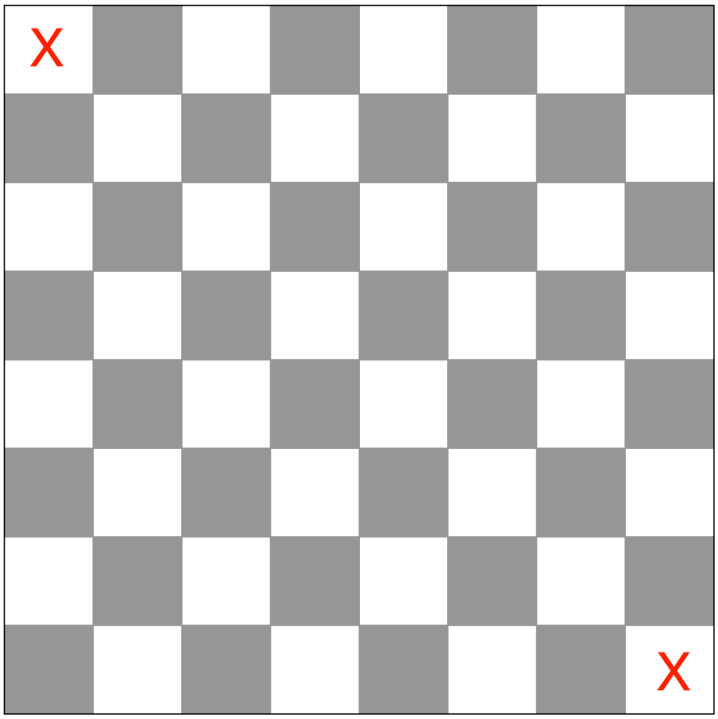
Minor Errors that I saw while grading:

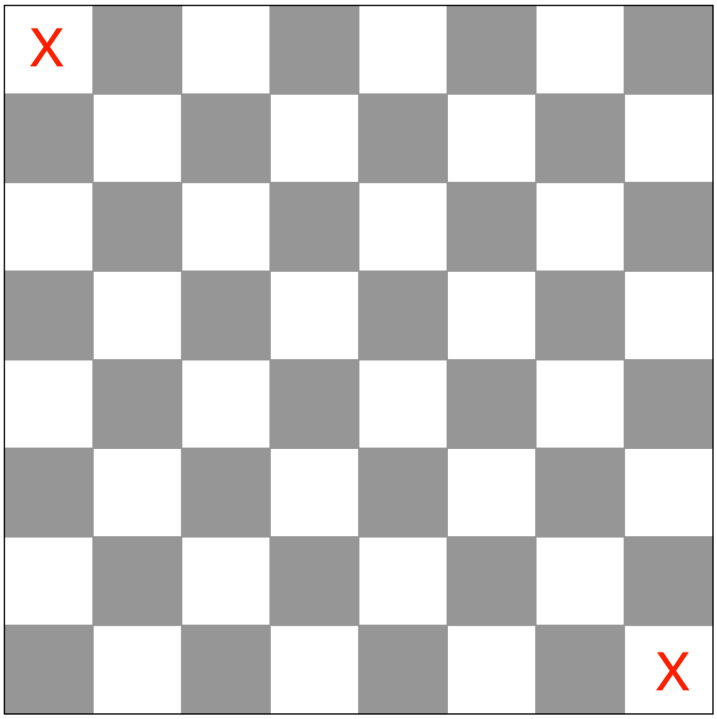
1. Some students didn't give a convincing final sentence for their proof. Just because 106 is not equal to 100 isn't quite convincing for me. This isn't to be nitpicky, but for instance,if you wrote "$y > 50$ and since 50 is not equal to 100, this mean y cannot equal 100." this wouldn't be true.What's important is the relationship between $y, 106$ and 100.

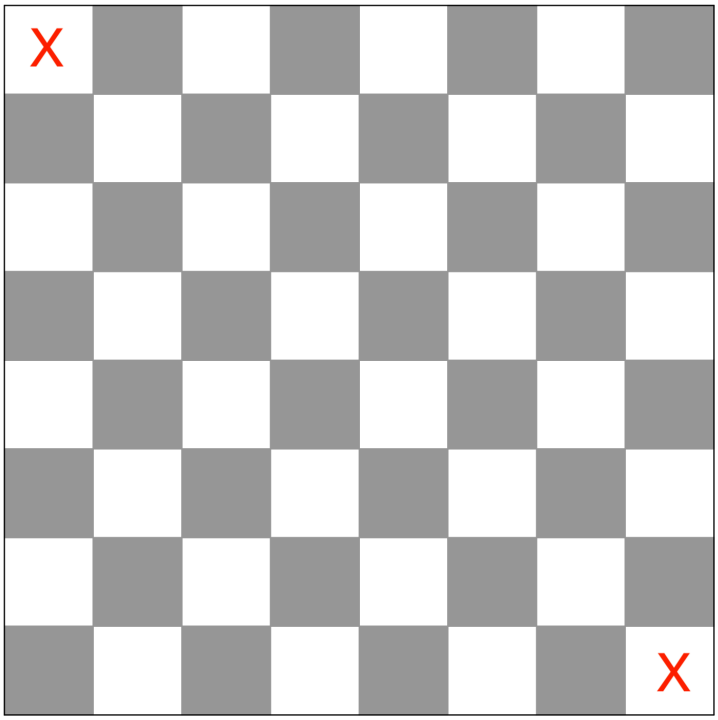
An exploratory Proof!

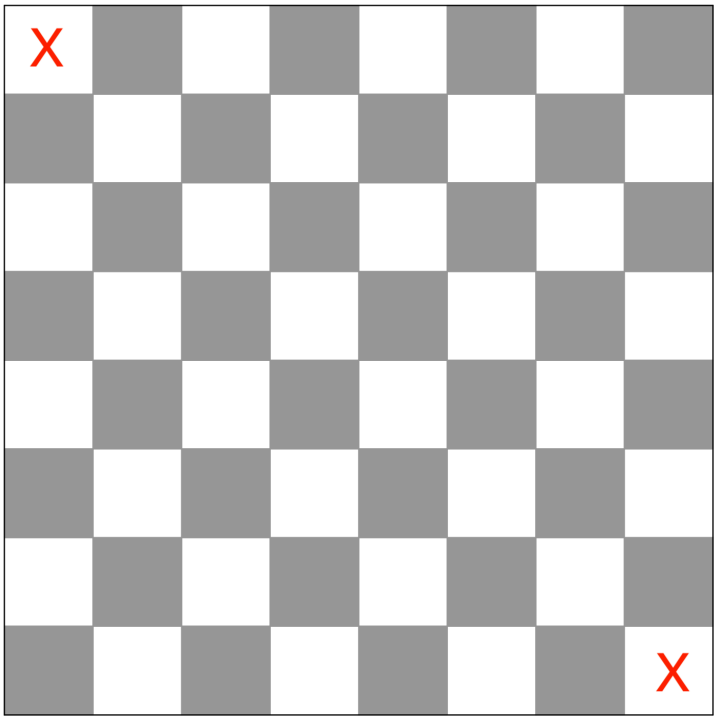
Can you cover this checkerboard that is missing two corners with 2×1 dominoes?

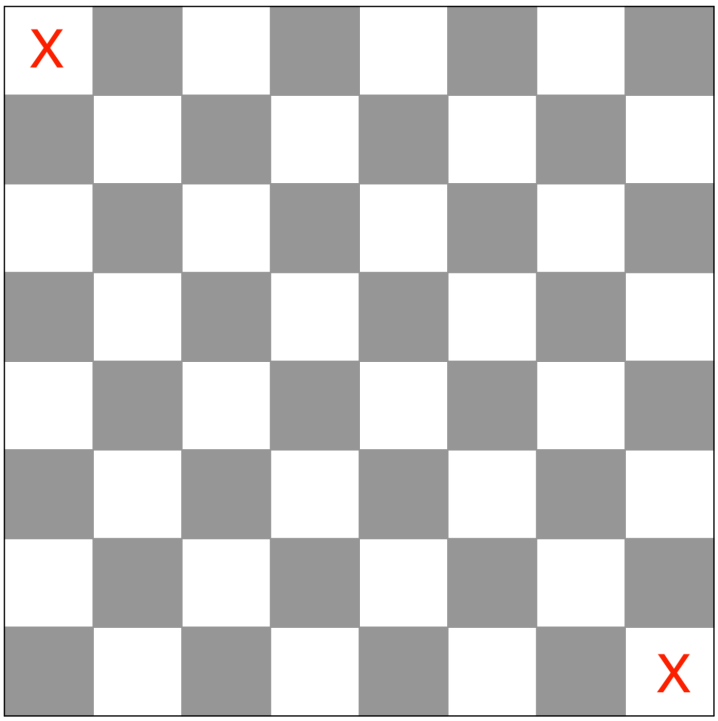


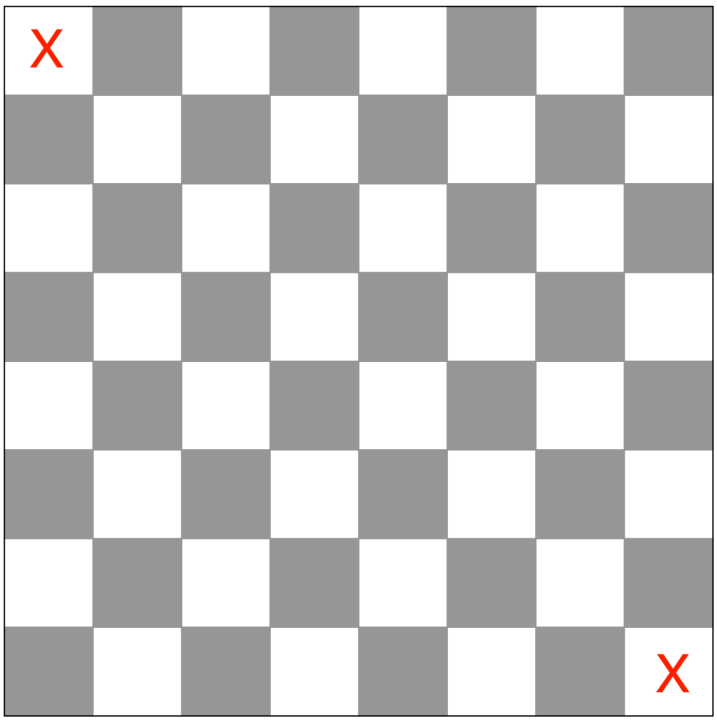


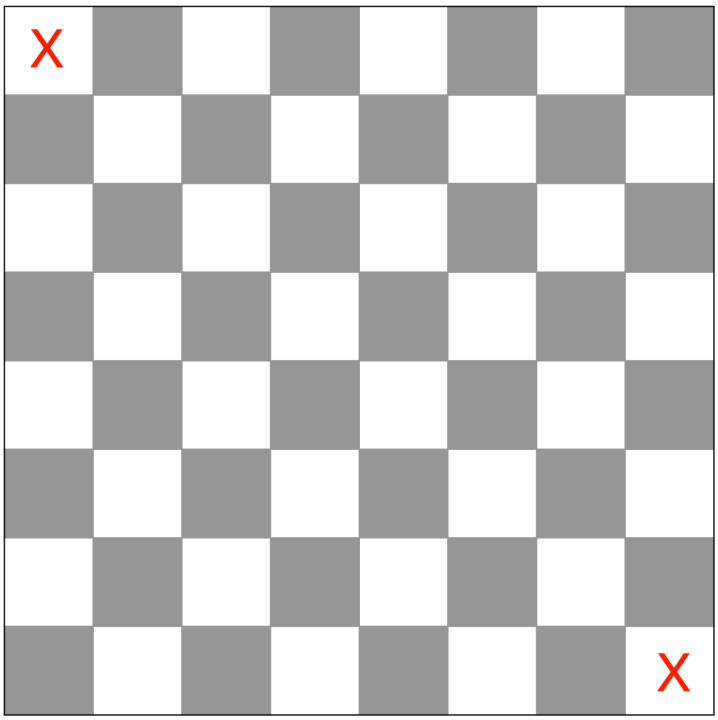


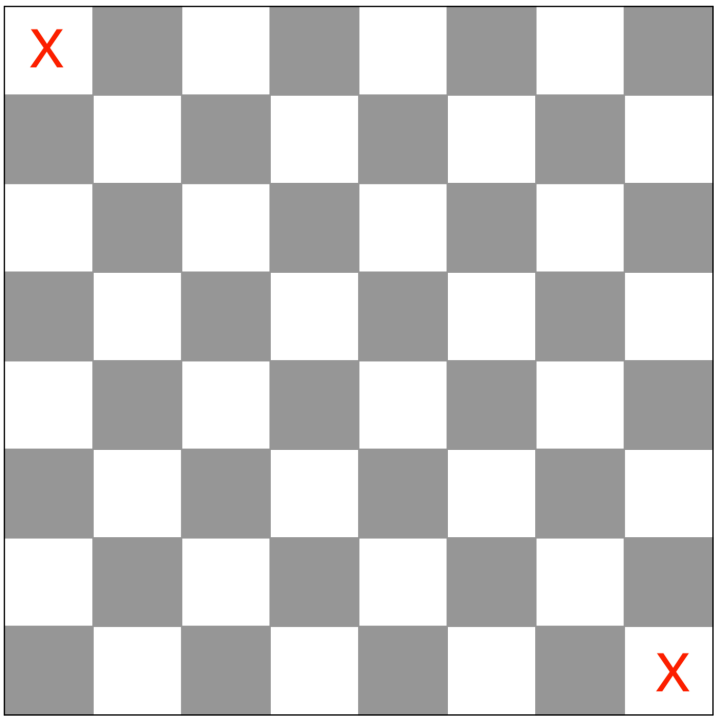





X
X


X
X


X
X


X
X

1 Sets, subsets, and cardinality

Definition: A set A is a **subset** of a set C is EVERY element of A is also an element of C. We denote this $A \subseteq C$.

Definition: We say two sets are **equal** if they have the same elements.

For example:

- The set of people who live in San Diego is a subset of the set of people who live in California.
- The set of integers divisible by 6 is a subset of the set of all integers.
- The set $\{e, f, v\}$ is a subset of the set $\{f, a, v, e\}$.

1. We say that two sets are equal if they have the same elements. For each of the following, determine if they are equal. If they are not equal, is either a subset of the other? In the space between the sets, put one of the symbols: $=$, $\subseteq$, or $\supseteq$, or write NC if the sets are not comparable.

$\{3, 1, 4, 5\}$ $\{5, 4, 1, 3\}$

$\{x \in \mathbf{Z} : x^2 = 4\}$ $\{2, -2\}$

$\{x \in \mathbb{N} : x^2 = 4\}$ $\{2, -2\}$

$\{x \in \mathbb{N} : x \text{ is a multiple of } 10\}$ $\{x \in \mathbb{N} : x \text{ is a multiple of } 5\}$

$\{x \in \mathbb{N} : x \text{ is a multiple of } 10\}$ $\{x \in \mathbb{N} : x \text{ is a multiple of } 12\}$

STOP

2. Consider the set

$$A = \{1, 2, \{3\}, \varnothing, \{2, 3\}\}$$

1. What is the cardinality of A? $|A| =$
2. Is $3 \in A$?
3. How about $\{3\}$?
4. Is $\{1, 2\} \subseteq A$?
5. Is $\{2, 3\} \subseteq A$?
6. Is $\{2, 3\} \in A$?
7. Is $\{2, \{3\}\} \subseteq A$?

STOP

Practice Problems (we won't have time to look at all of these)

1. Let's get some practice with set notation. First let's practice reading. These sets are all finite. Work out what elements are in each set and write down.

   $S = \{n : n \in \mathbb{Z} \text{ and } n^2 < 12.4\}$

   $A = \{n^2 : n \in \{1, 2, 3, 4, 5, 6\}\}$.

   $T = \{n^2 : n \in \mathbb{Z} \text{ and } 2n \in \{1, 2, 3, 4, 5, 6\}\}$.

   $B = \{n \in \mathbb{Z} \ : \ n^2 \in \{1, 2, 3, 4, 5, 6\}\}$

2. Now let's do things in reverse. Here's a description and you try to write this in "bar" notation. Please work with your teammates to make sure you understand the pieces and components and how they fit together.

   X: The set of all integers between 1937 and 2022 inclusive.

   A: The set of all integers that are multiples of 10.

   B: The set of all integers that are 3 more than a multiple of 12.

   C: The set of all positive integers that are one less than a perfect square.

3. A) Why is it not possible for two sets A and B to satisfy both $A \cap B = \{f, o, u, r\}$ and $A \cup B = \{f, o, r, t, y, s, i, x\}$.

   B) Suppose that A and B satisfy: $|A| = 101, |B| = 88, |B - A| = 31$. Using a Venn diagram, calculate $|A - B|$.

4. The following are all finite sets with fewer than 10 elements. Write out the elements.

   $A = \{x \mid x = 3k \text{ for } k \in \mathbf{Z} \text{ with } 0 \leq k \leq 4\}$

   $B = \{x^2 \mid x \in \{1, -1, 2, -2\}\}$

   $S = \{x \in \mathbf{Z} \mid x^2 \in A\}$

   $C = \{x^2 \mid x \in \mathbb{R} \text{ and } 2x \in \{3, 4, 5, 6\}\}$

   $D = \{x^2 \mid x \in \mathbf{Z} \text{ and } 2x \in \{3, 4, 5, 6\}\}$

   What is the cardinality of $\mathcal{P}(A \cup D)$?

2 Powersets

1. Let X be the set $\{1, 2, 3\}$. How many subsets of X are there? Write them down. Now do the same with $\{1, 2, 3, 4\}$. The **set of all subsets of X is called the power set** of X and is denoted $\mathcal{P}(X)$.

If a set X has n elements, it has _____ subsets.

2. We say that two sets X and Y are **disjoint** if they have nothing in common. In other words, if $X \cap Y = \{\}$ (the empty set. How many subsets of $\{b, r, i, d, g, e\}$ are disjoint from the set $\{s, t, r, e, a, m\}$?

3. Let

$$A = \{a, b, c, d, e\}.$$

For each integer $k \in \{0, 1, 2, 3, 4, 5\}$ define $B_k = \{C \in \mathcal{P}(A) : |C| = k\}$ (this is probably very confusing; that's okay). First, pick a specific value for k, say $k = 1$. Now write out the definition of B_1 (just copy the definition above replacing k's with 1's. Then list all the elements in B_1. Next, write out B_2 in roster notation. Can you write an english sentence describing the set B_3?

STOP

3 Union, Intersection, Difference & Complement

Let's go back to the set of all integers between 1937 and 2022 inclusive. What is the cardinality of this set?

Take the universal set as the natural numbers. Define

$$E = \{x : \exists k \in \mathbb{N}(x = 2k)\} \text{ and } P = \{x : x \text{ is prime}\}$$

Describe each set using an english sentence.

1. $\overline{E}$.
2. $E \cap P$.
3. $P - E$.
4. $\overline{P \cap E}$.

Now have each member of your group describe an interesting subset of the real numbers using an English sentence. Then try to write a definition of this set using set builder notation.

A survey was done asking 270 seniors what type of music they listen to. Please draw a Venn diagram and use notation to show how you arrive at your answer. I'm looking for you to identify a set (as a union, complement, or intersection, and write it carefully.)

100	Classical
50	Opera
110	Rock
86	Classical and Rock
30	Classical and Opera
20	Opera and Rock
18	Listen to all three

a) How many listen to classical music and nothing else?

b) How many seniors don't listen to any of these three genres?

STOP

1 Warmup

Let

$$A = \{1937, 1938, \ldots, 2021, 2022\}.$$

In this exercise you will calculate $|A|$.

- With people around you, discuss how you might calculate $|A|$
- The goal isn't so much to get the correct answer, but to come up with a **reason** so that you are confident that you have the correct answer.

2 Union and Intersection, Complement, and Cartesian Product

Let $A = \{1, 2, 3\}$ and let $B = \{2, 3, 4\}$. Suppose that the universal set is $U = \{1, 2, 3, 4, 5\}$. Determine the following.

1. $A \cup B$

2. $A \cap B$

3. $\overline{A} \cap B$

4. $\overline{A} \cap \overline{B}$

5. $\overline{A} \cap \{x \in U \mid x \text{ is prime.}\}$

6. $A \times B$

7. $(A \times B) - (B \times A)$

Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the universal set for this problem and let $A = \{2, 3, 7\}$ and $B = \{2, 5, 6, 9\}$.

(a) What is $|A \times B|$?

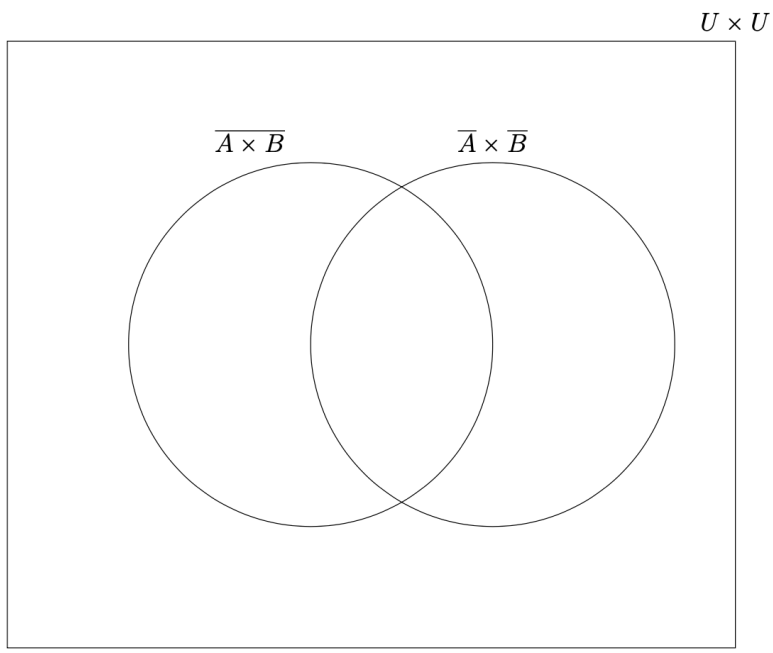
(b) How many elements does $\overline{A \times B}$ have?

(c) How many elements does $\overline{A} \times \overline{B}$ have?

(d) Below is a Venn diagram for the two sets in the previous parts. Insert the elements

$$(1, 4), \quad (2, 2), \quad (1, 2)$$

into the appropriate regions in the diagram. Hint: Of the four regions - these three numbers should occupy 3 different regions.

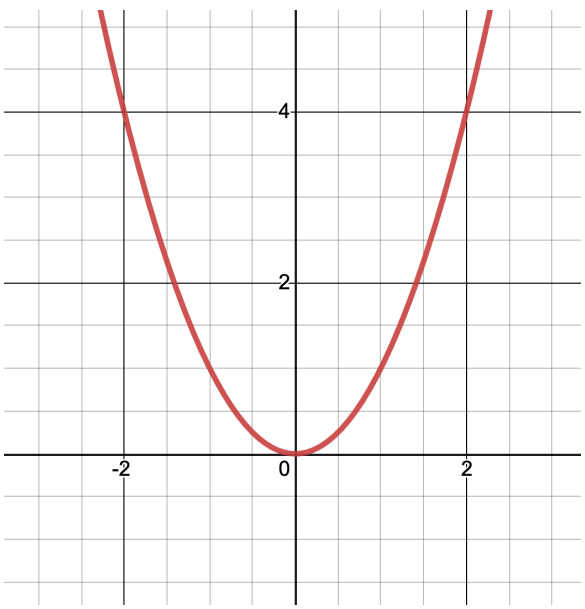


3 Looking forward to functions

How would we visualize the set $\mathbb{R} \times \mathbb{R}$?

What about the set $\mathbb{R} \times [0, \infty)$.

What about the set $\mathbf{Z} \times \mathbf{Z}$?



True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbb{R} \times \mathbb{R}$?

True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbb{R} \times [0, \infty)$?

True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbf{Z} \times \mathbf{Z}$.

Let G denote the graph of $y = x^2$ pictured above, as a subset of the set $\mathbb{R} \times \mathbb{R}$.

Let $Y = \{(u, u) \ : \ u \in \mathbb{R}\}$.

What is $G \cap Y$?

What is $G \cup Y$?

4 More Challenging Questions about Sets

Recall that the **powerset** of a set X consists of all subsets of X. Let's think about the following questions. For each of these, do you think this result is sometimes/always/never true?

Hypotheses: A and B are nonempty finite sets.

Question 1:

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)?$$

Question 2:

$$\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)?$$

Question 3:

$$\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)?$$

Question 4:

$$\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)?$$

Chapter 5 Homework Problems

Due: Wednesday March 2nd

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Book Problems:

5.1.1,5.1.3,5.1.4,5.1.5,5.1.6,

5.3.1,5.3.4,

5.4.1,5.4.3,5.4.4,

5.6.1,5.6.3

5.7.1

Additional Problems:

1. A poll of 100 students is taken about whether they like apples, bananas, or chocolate. Students selected all that applied. You are given the following information:
   - 10 students liked all three of apples, bananas and chocolate
   - everyone who likes apples also likes bananas
   - 35 students like apples
   - 70 students like bananas
   - 6 students like only chocolate

   Filling in a Venn diagram, use this to determine how many students liked none of apples, bananas, or chocolate.

2. The following are all finite sets with fewer than 10 elements (except for the last one). Write out the elements.

   $A = \{x \mid x = 3k \text{ for } k \in \mathbf{Z} \text{ with } 0 \leq k \leq 4\}$

   $B = \{x^2 \mid x \in \{1, -1, 2, -2\}\}$

   $S = \{x \in \mathbf{Z} \mid x^2 \in A\}$

   $C = \{x^2 \mid x \in \mathbb{R} \text{ and } 2x \in \{3, 4, 5, 6\}\}$

   $D = \{x^2 \mid x \in \mathbf{Z} \text{ and } 2x \in \{3, 4, 5, 6\}\}$

   $P(A \cup D)$ (The power set of $A \cup D$) (This one has a lot of elements, so you don't need to write them all down, but try writing a few.) How many elements are in this set through? (Answer in footnote[†])

3. Draw a picture that illustrates the following true fact about sets, and explain in your own words why it is true:

   "If A and B are finite sets then $|A \cup B| = |A| + |B| - |A \cap B|$."

[†] 64

4.

Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the universal set for this problem and let $A = \{2, 3, 7\}$ and $B = \{2, 5, 6, 9\}$.

(a) What is $|A \times B|$?

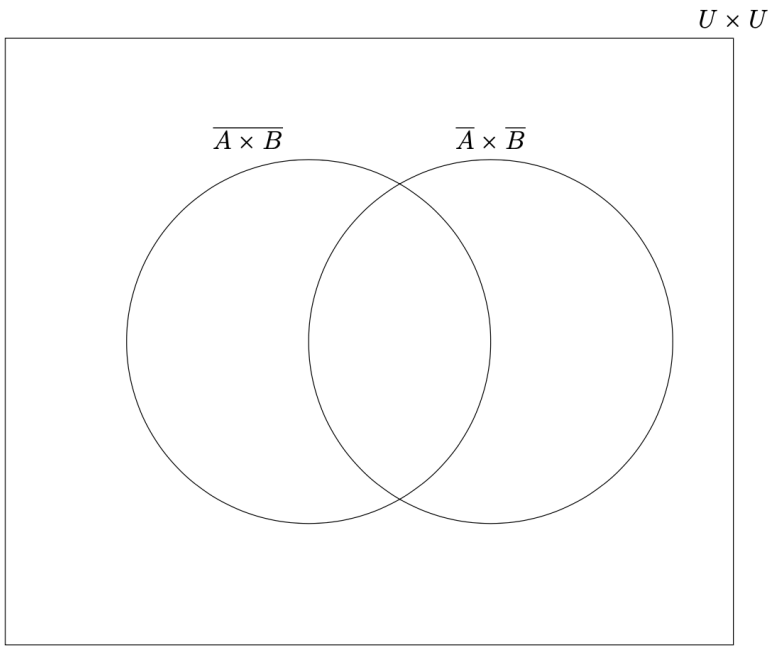
(b) How many elements does $\overline{A \times B}$ have?

(c) How many elements does $\overline{A} \times \overline{B}$ have?

(d) Below is a Venn diagram for the two sets in the previous parts. Insert the elements

$$(1, 4), \quad (2, 2), \quad (1, 2)$$

into the appropriate regions in the diagram. Hint: Of the four regions - these three numbers should occupy 3 different regions.



Quiz 5

Name: _____

1. Let $X = \{b, e, a, c, h\}$.

Write down a subset of X.

There are many choices here, e.g. $\{b, a, c\}$

Write down an element of $X \times (\mathbb{Z} - \mathbb{N})$.

This is saying that we want an ordered pair, where the first element is in X, (so a letter) and the second element is in $\mathbb{Z} - \mathbb{N}$ which means it is an integer that is NOT a natural number. So something like $(b, -7)$ would be correct.

How many proper, nonempty, subsets does X have?

Since X has 5 elements it has 2^5 or 32 total subsets. But one is the empty set, and one is the whole set X, so if we want proper, nonempty, we need to exclude those, so the answer to this question is 30. Partial credit for writing 32 or 31.

2. Consider the universal set $U = \{k \in \mathbf{Z} : -10 \leq k \leq 10\}$.

Let

$$A = \{n \in U \ : \ n^2 > 50\}, \quad B = \{n \in U \ : \ 5|n\}$$

a. True or false: $A \cup B = U$. Explain your answer briefly. This might be a good place to write down what A and B are for you to refer to it later.

So $A = \{\pm 10, \pm 9, \pm 8\}$ and $B = \{\pm 10, \pm 5, 0\}$. Thus $A \cup B$ will not contain all the elements from U, for instance, 3 is in neither A nor B.

b. What is $A \cap B$? Write your answer as a list of numbers.

$A \cap B = \{\pm 10\}$

c. Which is correct? (Circle all that apply)

$$\{6, 8\} \in \mathcal{P}(U) \qquad \{6, 8\} \subseteq \mathcal{P}(U).$$

$P(U)$ has *elements* that are subsets of U. So $\{6, 8\}$ is an element (one of thousands of elements of $P(U)$). It is not a subset. However, it would be correct to say that $\{\{6\}, \{8\}\} \subseteq P(U)$.

THERE IS A PROBLEM ON THE OTHER SIDE

3. This one is more challenging, but you can do it!

Let $A = \{1, 2, 3\}$. A student finds two subsets X and Y of the set $\mathcal{P}(A)$ and notices that $|X \times Y| = 24$. There are multiple possibilities for the cardinalities $|X|$ and $|Y|$. List all the possibilities and explain why your list is correct. You will not need all of the blank spaces below.

"One possibility is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Another is that $|X| =$ _____ and $|Y| =$ _____.

Justification:

The idea here is that $|X \times Y| = |X| \cdot |Y|$ so we know that $|X|$ and $|Y|$ are two numbers that multiply to 24. There are lots of possibilities. But we also know that X and Y are subsets of $P(\{1, 2, 3\})$ which has 8 elements. This means that $|X|$ and $|Y|$ must be ≤ 8. Thus the only combinations for $|X|, |Y|$ are $(4, 6), (6, 4), (3, 8), (8, 3)$.

1 Introduction to Functions

Warmup: Can you think of some examples of functions

$$F : \{\text{students at USD}\} \longrightarrow \mathbb{Z}$$

For each of the functions above what is their **domain**? What is their **target (or co-domain)**. What is their **range**? Would these still be functions if we changed the co-domain to $\mathbb{R}$? What new functions could we include then?

In general:

The domain is [sometimes/always/never] the set to the left of the $\longrightarrow$

The target or co-domain is [sometimes/always/never] the set to the right of the $\longrightarrow$

The range is [sometimes/always/never] the set to the right of the $\longrightarrow$

and it is [sometimes/always/never] a subset of the set to the right of the $\longrightarrow$.

Example: Which of the following are **well-defined** functions. (Meaning that that every input has some output determined by the rule.) Remember that $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

$r : \mathbb{R} \to \mathbf{Z}$ with the rule $r(x) = x^2$

$f : \mathbf{Z} \to \mathbb{N}$ with the rule $f(x) = x^2$

$g : \mathbf{Z} \to \mathbf{Z}$ with the rule $g(x) = x^2$

$h : \mathbf{Z} \to \mathbb{R}$ with the rule $h(x) = x^2$

$i : \{\text{people on Earth}\} \to \mathbf{Z}$ with the rule $i(x) =$ x's age in years

$j : \{\text{people on Earth}\} \to \{0, 1, 2, 3, 4, \ldots, 50\}$ with the rule $j(x) =$ x's age in years

$k : \{\text{people in our class}\} \to \{0, 1, 2, 3, 4, \ldots, 50\}$ with the rule $k(x) =$ x's age in years

$\ell : \{\text{Joe Biden, Justin } \overline{B} \text{ (Biebs), Ariana Grande}\} \to \{0, 1, 2, 3, 4, \ldots, 50\}$ with the rule

$$\ell(x) = \begin{cases} \text{x's age in years} & \text{if x is 50 or younger} \\ 7 & \text{otherwise} \end{cases}$$

Example: Let X be the set $\{a, b, c, d\}$ Consider the function

$$F : \mathcal{P}(X) \to \mathbf{Z}, \quad \text{given by } F(S) = |S|.$$

What is $F(\{a, c, e\})$?

What is $F(\{\})$?

What is the range of F?

What is the cardinality of the domain of F?

What is $\{x \in X \mid F(x) \geq 3\}$?

Example: Let $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $p(x, y) = xy$. Why do you think I used the letter p for the name of this function?

What is the range of p? Why? Do some examples to better understand! What if $p(2, 3)$ what about $p(11, 1)$?

Let $A = \{z \in \mathbb{N} \times \mathbb{N} \mid p(z) = 20\}$. Describe A.

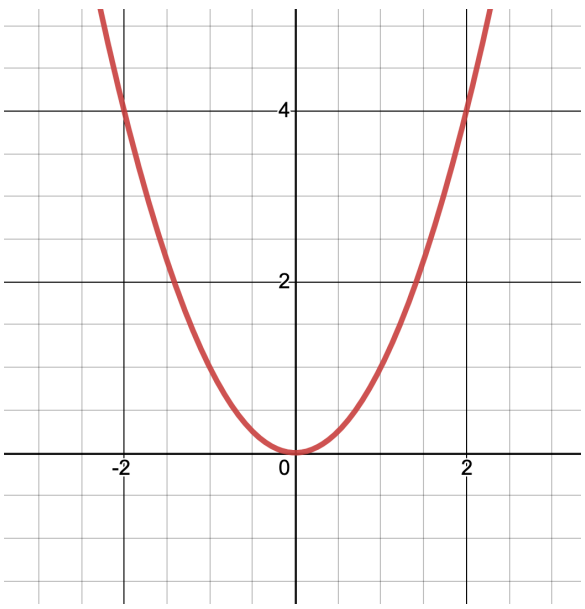
More generally, let $A_b = \{z \in \mathbb{N} \times \mathbb{N} \mid p(z) = b\}$. Describe A_b. (Hint: don't panic - see if you can connect this problem to the one we just did. The previous problem was A_{20}. What would A_6 be? In general what is A_b communicating?

Now let $Y = \{n \in \mathbb{N} \mid |A_n| = 2\}$. Describe Y.

How would we visualize the set $\mathbb{R} \times \mathbb{R}$?

What about the set $\mathbb{R} \times [0, \infty)$.

What about the set $\mathbf{Z} \times \mathbf{Z}$?



True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbb{R} \times \mathbb{R}$?

True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbb{R} \times [0, \infty)$?

True or False, the set of points on the graph of $y = x^2$ is a subset of $\mathbf{Z} \times \mathbf{Z}$.

Let G denote the graph of $y = x^2$ pictured above, as a subset of the set $\mathbb{R} \times \mathbb{R}$.

Let $Y = \{(u, u) \ : \ u \in \mathbb{R}\}$.

What is $G \cap Y$?

What is $G \cup Y$?

1 One to One, Onto, and Composition of Functions

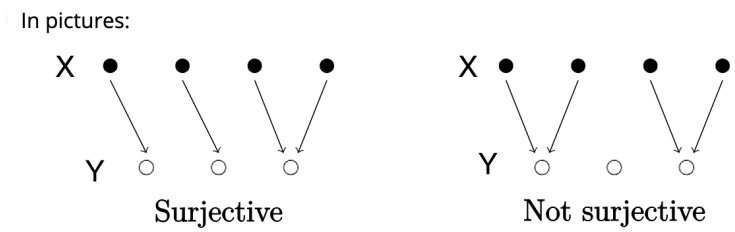
On this worksheet you will learn the following concepts:

- What it means for a function to be **surjective** or **onto** (these are synonyms).
- What it means for a function to be **injective** or **1-1** (these are synonyms).

What it means to be surjective or onto

Definition: We say that a function $f : X \to Y$ is **surjective** or **onto** if the range of f is equal to the target.

Here is a picture. With your group talk about why these are surjective or not. Give your reason using the definition you just wrote. Why is the second one not surjective?



1. Explain why the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not surjective.
2. Explain why the function $f : \mathbb{R} \to [0, \infty)$ given by $f(x) = x^2$ is surjective.
3. Is the function $f : \mathbf{Z} \to \mathbf{Z}$ given by $f(x) = 3x$ surjective?
4. Suppose that X is a group of musicians (who all either a drummer, guitarist, bassist, or singer), and consider the function
$$f : X \to \{\text{guitar, bass, vocals, drums}\}$$
that assigns each person their instrument. What does it mean in words to say that the function X is onto?
5. Consider the function
$$m : \{\text{people born in 2022}\} \to \{January, February, \ldots, December\}$$
$$m(x) = \text{the birth month of } x.$$
Is m surjective? Why or why not?
6. With your group talk about the following statements and see which you think are true: (Hint: 2 are true, one is false)

   A.) f is surjective means that every element $y \in Y$ is equal to $f(x)$ for some x in X.

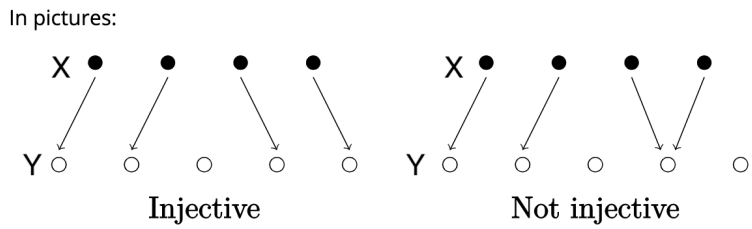
   B.) f is surjective means that $\forall x \in X \ \exists y \in Y : f(x) = y$.

   C.) f is surjective means that $\forall y \in Y, \ \exists x \in X : f(x) = y$.

Injective Functions

Definition: We say that a function $f : X \to Y$ is **injective** or **1-1** if no two elements in X are sent to the same element in Y.

Here is a picture. With your group talk about why these are injective or not. Give your reason using the definition.



1. Consider the function $m : \{\text{people on Earth}\} \to \{January, February, \ldots, December\}$ given by $m(x) =$ the birth month of X. Is m injective? Why or why not?

2. Is the function $f : \mathbf{Z} \to \mathbf{Z}$ given by $f(x) = 3x$ injective?

3. Suppose that X is a group of musicians (who all either a drummer, guitarist, bassist, or singer), and consider the function
$$f : X \to \{\text{guitar, bass, vocals, drums}\}$$
that assigns each person their instrument. What does it mean in words to say that the function X is 1-1?

4. Which of the following functions are **injective**?
$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$$
$$g : \mathbb{R} \to [0, \infty), \quad g(x) = x^2$$
$$h : [0, \infty) \to \mathbb{R}, \quad h(x) = x^2$$
$$p : [0, \infty) \to [0, \infty) \quad p(x) = x^2.$$

5. (You may want to skip this problem to make sure you get to all 4 parts today) With your group talk about the following statements and see which you think are true: (Hint: 2 are true, 1 is false, since it is a property of general functions, not just 1-1 functions.)

   A.) f is injective means that every input has an output.

   B.) f is injective means that if a and b in X are different inputs then $f(a)$ and $f(b)$ are different outputs in Y.

   C.) f is injective means that if $a, b \in X$ and $a \neq b$ then $f(a) \neq f(b)$.

Here is a restatement of the properties you have learned so far:

Injective vs Surjective.

A function is ***injective*** provided every element of the codomain is the image of *at most* one element from the domain.

A function is ***surjective*** provided every element of the codomain is the image of *at least* one element from the domain.

What do you think about this? Does it make sense? Now is your chance to ask questions!

Sometimes functions can be injective AND surjective. These functions are called bijective. What would it mean for our band example for the function f to be bijective?

With your groups, consider the following functions. Are they injective, surjective, both, neither?

1. $f: \mathbb{N} \to \mathbb{N}, f(k) = 2k + 1$
2. $g: \mathbb{Q} \to \mathbb{Q}, g(x) = 2x + 1$
3. $h: \mathbb{R} \to \mathbb{Z}, h(x) = \lfloor x \rfloor$
4. $h: \mathbb{Z} \to \mathbb{Z}, h(x) = \lfloor x \rfloor$
5. $j: \mathbb{Z} \times \mathbb{Z}^+ \to \mathbb{Q}, j(p, q) = \frac{p}{q}$
6. $f_2: \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f_2(m, n) = m^n$. *(The convention is that $0^0 = 1$.)*

Composition of Functions

Can you think of two functions f and g with the property that $g \circ f$ is surjective, but f is not?

It's important to study how properties of compositions of functions behave.

Let's explore the following statements:

1. If $f : X \to Y$ and $g : Y \to Z$ are injective functions then $g \circ f : X \to Z$ is injective.

2. If $f : X \to Y$ and $g : Y \to Z$ are surjective functions then $g \circ f : X \to Z$ is surjective

3. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Suppose that $g \circ f$ is surjective. Then prove that g is surjective.

4. Let $f : X \to Y$ and $g : Y \to Z$ and $h : Z \to W$ be injective functions. Prove that $h \circ g \circ f$ is injective. Do this by APPLYING the result from 1.

5. Let f_1, f_2, f_3, f_4, f_5 be functions (all from $\mathbb{R}$ to $\mathbb{R}$.) Prove that if all five functions are injective then so is their composition $f_5 \circ f_4 \circ f_3 \circ f_2 \circ f_1$.

How Many Functions? On the homework you were asked how many functions there were from from a set X to a set Y in two cases.

- On the homework I had you write down all the functions from $\{1, 2, 3\}$ to $\{a, b\}$ (there were 8)
- And from $\{1, 2\}$ to $\{a, b, c\}$ (there were 9)

Question: How does this generalize? What if $|X| = n$ and $|Y| = m$. How many functions are there from $X \to Y$?

Question: Suppose you knew that there was an injective function $f : X \to Y$ and $|X| = 10$. What could you say about $|Y|$?

Chapter 6 Homework Problems

Due: Friday March 18th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Book Problems:

6.1: 1, 2a, 3, 4, 5agkl, 6ac

6.2: 2, 4ce

6.3: 1abcd, 2abc, 5

6.5: 1, 2, 5

The quiz will cover definition of functions, 1-1 onto, bijections, as well as compositions of functions.

1. Being able to write down examples is a super important skill as well. In the problems below I ask you to write down some examples of functions that have desired properties. As you are going through these, you might need to work in pencil, go back and erase your thoughts and then continue again.

   For all of these problems, just draw your functions with arrows. Work very slowly and think about what properties you want.

   (a) Write down an example of a function $f : \{1, 2, 3\} \to \{a, b, c, d, e\}$ that is NOT injective. (Remember that injective is another word for 1-1) Please do this by drawing arrows. If this is not possible, explain why.

   (b) Write down an example of a function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ that NOT surjective. (Remember surjective is another word for onto) Please do this by drawing arrows. If this is not possible, explain why.

   We will now define two operations that we can do combining sets and functions:
   Suppose that $f : X \to Y$ is a function, and that A is a subset of the domain. Then define

   $$f(A) = \{f(x) \ : \ x \in A\}.$$

   In other words, $f(A)$ is the set of all outputs $f(x)$ where we take x in the set A.

   Now take a subset B of the co-domain. Then we define

   $$f^{-1}(B) = \{x \in X \ : \ f(x) \in B\}$$

   (c) Get some practice. Let $f : \mathbb{R} \to \mathbb{R}$ be the function $f(x) = x^2$. Check that $f(\{-1, 1, 4\}) = \{1, 16\}$, and that $f^{-1}(\{16, 25\}) = \{4, -4, 5, -5\}$, and that $f^{-1}(\{-9\}) = \{\}$.

   (d) Write down an example of a function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ (by drawing arrows) so that

   $$f^{-1}(\{2, 3, 4\}) = \{1, 5\}.$$

   (e) Write down an example of a function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ (by drawing arrows) so that

   $$f(\{2, 3, 4\}) = \{1, 5\}.$$

   (f) Write down an example of a function $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ (by drawing arrows) so that

   $$|\{n \ : \ f(n) = n\}| = 2.$$

(g) Write down an example of a function $f : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ so that

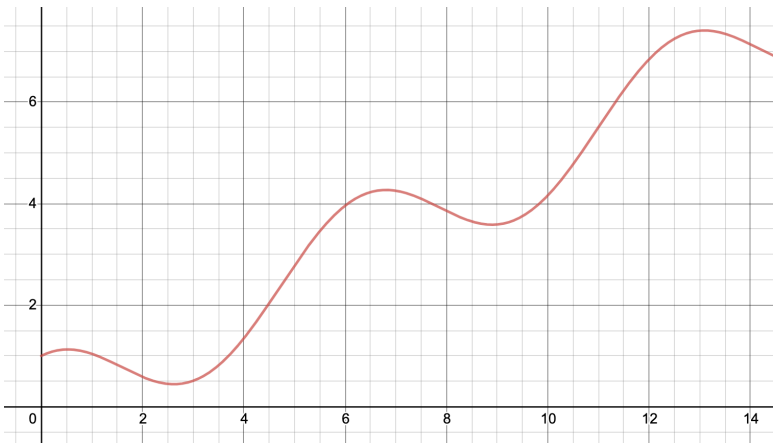
$$f^{-1}(f(\{2,3\})) = \{2,3,5\}$$

2. How many functions are there with domain $\{1,2,3\}$ and codomain $\{a,b\}$. How many are surjective? How many are injective? (You may want to write these out and draw a picture)

3. How many functions are there with domain $\{1,2\}$ and codomain $\{a,b,c\}$. How many are surjective? How many are injective? (You may want to write these out and draw a picture)

4. (Optional) Below is the graph of the function $f : [0,\infty) \to \mathbb{R}$ given by $f(x) = \frac{1}{2}x + \cos x$.

   - Notice that according to the graph there are TWO inputs x such that $f(x) = 1$. Find approximations for these two points using Desmos.com and explain why this means the function is NOT injective.
   - Using the methods of calculus (and the graph) determine the range of f. (I do not want an approximation here, I want an exact answer.)
   - Is the function f surjective?



Quiz 6 Name: _____

1. Let $f : \mathbf{Z} \to \mathbb{N}$ be defined by $f(x) = x^2 + 5$.

The domain of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The target of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The range of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The function f is [onto/not onto]

The function f is [1-1/not 1-1]

Let $A = \{-2, 1\}$ and $B = \{1, 2\}$.

Write down the sets indicated below, using the same function defined above. These are like the ones you practiced on the HW.

$f(A) =$

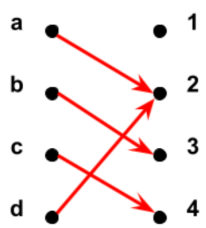
$f(B) =$

$f(A) \cap f(B) =$

$A \cap B =$

$f(A \cap B) =$

2. The picture below represents a function $f : A \to X$ where $A = \{a, b, c, d\}$ and $X = \{1, 2, 3, 4\}$.



What is $f^{-1}(\{3, 1, 4\})$?

If $g : X \to \{0, 1\}$ given by $g(x) = \lfloor \frac{x}{3} \rfloor$. Draw in the arrows for g in the picture above.

$g \circ f(a) =$

$g \circ f(b) =$

f is [onto / not onto]

$g \circ f$ is [onto /not onto]

3. If you are starting a proof that $f : R \to S$ is onto, which of these could be the first sentence? (Circle the best choice)

1. Let $r \in R$. We will show $\exists s \in S$ with $f(s) = r$
2. Let $r \in R$. We will show $\exists s \in S$ with $f(r) = s$
3. Let $s \in S$. We will show $\exists r \in R$ with $f(s) = r$
4. Let $s \in S$. We will show $\exists r \in R$ with $f(r) = s$

A function $f : \mathcal{P}(\{1, 2, 3\}) \to \mathcal{P}(\{1, 2, 3, 4\})$ is defined by

$$f(S) = S \cup \{4\}.$$

Write down TWO example input and output pairs:

$f($_____$) =$ _____

$f($_____$) =$ _____

A student wants to define a function using the formula $f(n) = n - 1$. For each of the choices for possible domain and target below, I want you to:

- Place an x over the choice if the formula $f(n) = n - 1$ would NOT give a well-defined function.

a.) $f : \{1, 2, 3, \ldots\} \to \{1, 2, 3, \ldots\}$

b.) $f : \{1, 2, 3, \ldots\} \to \mathbb{R}$

c.) $f : \{\text{positive even integers}\} \to \{\text{positive even integers}\}$

d.) $f : \{\text{positive even integers}\} \to \{\text{positive odd integers}\}$

e.) $f : \{\text{positive odd integers}\} \to \{\text{positive even integers}\}$

4. A student tries to define a function $g : \mathbf{Z} \times \mathbf{Z} \to \mathbb{R}$ with the formula:

$$g(x, y) = \frac{x - y}{x + y + 1}.$$

Explain why this is not well-defined. (Be explicit - it's better here to give specific values that give the problematic behavior.)

The student updates their function to the following $g : \mathbb{N} \times \mathbb{N} \to \mathbf{Z}$ given by

$$g(x, y) = \frac{x - y}{x + y + 1}.$$

Explain why this function is NOT injective (i.e. that it is NOT 1-1)

Explain why this function is NOT onto. (Hint: Try to decide whether or not the number 1 is in the range of f)

Quiz 6 Name: _____

1. Let $f : \mathbf{Z} \to \mathbb{N}$ be defined by $f(x) = x^2 + 5$. fd The domain of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The target of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The range of f is [$\mathbf{Z}$/$\mathbb{N}$/something else]

The function f is [onto/not onto]

The function f is [1-1/not 1-1]

Let $A = \{-2, 1\}$ and $B = \{1, 2\}$.

Write down the sets indicated below, using the same function defined above. These are like the ones you practiced on the HW.

$f(A) =$

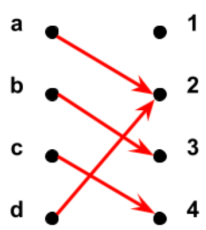
$f(B) =$

$f(A) \cap f(B) =$

$A \cap B =$

$f(A \cap B) =$

2. The picture below represents a function $f : A \to X$ where $A = \{a, b, c, d\}$ and $X = \{1, 2, 3, 4\}$.



What is $f^{-1}(\{3, 1, 4\})$?

If $g : X \to \{0, 1\}$ given by $g(x) = \lfloor \frac{x}{3} \rfloor$. Draw in the arrows for g in the picture above.

$g \circ f(a) =$

$g \circ f(b) =$

f is [onto / not onto]

$g \circ f$ is [onto /not onto]

3. If you are starting a proof that $f : R \to S$ is onto, which of these could be the first sentence? (Circle the best choice)

1. Let $r \in R$. We will show $\exists s \in S$ with $f(s) = r$
2. Let $r \in R$. We will show $\exists s \in S$ with $f(r) = s$
3. Let $s \in S$. We will show $\exists r \in R$ with $f(s) = r$
4. Let $s \in S$. We will show $\exists r \in R$ with $f(r) = s$

A function $f : \mathcal{P}(\{1, 2, 3\}) \to \mathcal{P}(\{1, 2, 3, 4\})$ is defined by

$$f(S) = S \cup \{4\}.$$

Write down TWO example input and output pairs:

$f($_____$) =$ _____

$f($_____$) =$ _____

A student wants to define a function using the formula $f(n) = n - 1$. For each of the choices for possible domain and target below, I want you to:

- Place an x over the choice if the formula $f(n) = n - 1$ would NOT give a well-defined function.

a.) $f : \{1, 2, 3, \ldots\} \to \{1, 2, 3, \ldots\}$

b.) $f : \{1, 2, 3, \ldots\} \to \mathbb{R}$

c.) $f : \{\text{positive even integers}\} \to \{\text{positive even integers}\}$

d.) $f : \{\text{positive even integers}\} \to \{\text{positive odd integers}\}$

e.) $f : \{\text{positive odd integers}\} \to \{\text{positive even integers}\}$

4. A student tries to define a function $g : \mathbf{Z} \times \mathbf{Z} \to \mathbb{R}$ with the formula:

$$g(x, y) = \frac{x - y}{x + y + 1}.$$

Explain why this is not well-defined. (Be explicit - it's better here to give specific values that give the problematic behavior.)

The student updates their function to the following $g : \mathbb{N} \times \mathbb{N} \to \mathbf{Z}$ given by

$$g(x, y) = \frac{x - y}{x + y + 1}.$$

Explain why this function is NOT injective (i.e. that it is NOT 1-1)

Explain why this function is NOT onto. (Hint: Try to decide whether or not the number 1 is in the range of f)

1 Sequences and Recursion

Consider the sequence:

$$a_n : 3, 7, 11, 15, 19, \ldots,$$

Assuming the pattern continues, and that the first term is a_0, write down an **explicit formula** for a_n. For practice, what is a_{n-3}? what is a_{n+1}?

Now write a **recursive formula** for a_n in terms of how you get to a_{n-1}.

In general we will want to understand both **explicit** and **recursive** formulas. For extra practice, **check that the explicit formula above satisfies the recursive formula**:

Question: Are there other sequences that satisfy the same **recursive formula?**

For our next class, please read section 7.3 of the zyBooks, or alternatively, read: (just google open discrete math book, it's section 2.1. This online book has a better presentation that zybooks I think. **Some of this week's HW is taken from here, so you can check that out for possible hints / solutions**
`http://discrete.openmathbooks.org/dmoi3/sec_seq_intro.html`

A recursive formula on its own doesn't always determine a **unique** sequence. You also need to include **initial conditions.** We'll see more examples of this throughout.

On the next page are three activities that are designed to help you get an idea for recursive thinking. For each of these problems:

- The answer is not important
- What IS important is thinking about how to reduce the problem to a **simpler one.**
- Look for clues / patterns.
- (Most important) A reason **why** this pattern seems to be emerging.

1) The Legend of the Towers!

Investigate!

There is a monastery in Hanoi, as the legend goes, with a great hall containing three tall pillars. Resting on the first pillar are 64 giant disks (or washers), all different sizes, stacked from largest to smallest. The monks are charged with the following task: they must move the entire stack of disks to the third pillar. However, due to the size of the disks, the monks cannot move more than one at a time. Each disk must be placed on one of the pillars before the next disk is moved. And because the disks are so heavy and fragile, the monks may never place a larger disk on top of a smaller disk. When the monks finally complete their task, the world shall come to an end. Your task: figure out how long before we need to start worrying about the end of the world.

1. First, let's find the minimum number of moves required for a smaller number of disks. Collect some data. Make a table.
2. Conjecture a formula for the minimum number of moves required to move n disks. Test your conjecture. How do you know your formula is correct?
3. If the monks were able to move one disk every second without ever stopping, how long before the world ends?

if M_n represents the number of minimum moves to move a stack with n disks, record your information below.

2) The Coffee Shop Problem!

Every day you walk from your home (labeled S for start) to your favorite coffeeshop, (labeled E for end). You must walk along the city blocks, and want to get there as fast as possible, but you discover there are still lots of ways to walk.

a) How many blocks must you walk to get the coffee shop?

b) Talk about what restrictions there are on your movements? Can you go in all directions?

c) How many different ways you can go to get from S to E? (Solve a simpler problem first!)

d) (Only do this at the end) If $W_{i,j}$ represents how many ways you can end up at grid point (i, j) starting at position $(0, 0)$ what sort of recurrence relation could you write down?

3)

Investigate!

You have a large collection of 1×1 squares and 1×2 dominoes. You want to arrange these to make a 1×15 strip. How many ways can you do this?

1. Start by collecting data. How many length 1×1 strips can you make? How many 1×2 strips? How many 1×3 strips? And so on.
2. How are the 1×3 and 1×4 strips related to the 1×5 strips?
3. How many 1×15 strips can you make?
4. What if I asked you to find the number of 1×1000 strips? Would the method you used to calculate the number fo 1×15 strips be helpful?

Let D_n represent the number of ways you can make a $1 \times n$ strip.

2 So you think you found a pattern?

In the last activities you

- Noticed a pattern AND
- Came up with a reason why this pattern continues

Both of these steps are important if we are interested in studying future values of the sequence.

Warning

Just because you notice a pattern doesn't mean the pattern is guaranteed to continue.

Let's see some examples of processes where we have patterns. Do you think the pattern continues? Do you have a reason to believe it does or doesn't?

1) Add up the first n odd numbers. What do you notice? What do you wonder?

2) If n is a positive integer than is expression $n^2 - n + 41$ always prime? Start with $n = 1$, $n = 2$.

3) The Fibonacci numbers are defined by $f_0 = 1$, $f_1 = 1$ and

$$f_n = f_{n-1} + f_{n-2} \text{ for } \underline{\hspace{3cm}}.$$

Write down the first 10 Fibonacci numbers:

Question: What happens if we look at the SUM of the first n Fibonacci numbers. What sequence do we get? What do you notice? What do you wonder?

4) Take n points (irregularly) spaced around on a circle and draw all possible lines connecting these points. How many regions does this process form with $n = 1, 2, 3, 4, 5$ points? What do you notice? What do you wonder? Do you have a reason for this pattern?

5) (Extras) How do the Fibonacci numbers grow multiplicatively? Python Experiment!

Chapter 7 Homework Problems

Due: Friday March 25th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Book Problems:

There are no book problems this week, but make sure you are comfortable with the participation and challenge activities in 7.1 and 7.2.

Additional Problems:

1. Your professor wants to get big and strong for his rock climbing, so he decides to start doing pushups. On the first day he will do 1 pushup, on the 2nd he'll do 2, etc. Let p_n represent the number of pushups he will do on day n.
   (a) Write down an **explicit** and **recursive** formula for p_n.
   (b) Now let a_n represent the total accumulated number of pushups he has done after n days. For instance, $a_3 = 6$. Write down a **recursive** formula for a_n.
   (c) Write an explicit formula for a_n using "+⋯+" notation.
   (d) Write an explicit formula for a_n using $\sum$ notation.
   (e) After you solve the problem about triangular numbers below, come back and write in an explicit formula for a_n that doesn't have dot dot dot or sum notation.
2. Sometimes you have to figure out what terms will come next or before in a sequence. For instance, let
$$f_n = 3n + 7.$$
   What 2 terms would come before and after f_n? I am asking you write down expressions for $f_{n-1}, f_{n-2}, f_{n+1}$ and f_{n+2}.
3. What is the 40th term of the arithmetic sequence that starts with $7, 11, 15, \ldots$.
4. Find a_6 in the sequence defined by $a_n = 2a_{n-1} - a_{n-2}$ with $a_0 = 3$ and $a_1 = 4$.
5. If the 11th term of an arithmetic sequence is 20 and the 13th term is 30 what is the 1st term? What is the 100th term? What is the nth term? I recommend not looking for formulas for how to solve problems like this. Just write down what you know and think about how the numbers are changing and what you can do. Test some cases with smaller numbers and look for patterns. It's much more important to be able to think these through rather than to just get the right answer.
6. Use summation ($\sum$) or product ($\prod$) notation to rewrite the following.
   (a) $2 + 4 + 6 + 8 + \cdots + 2n$.
   (b) $1 + 5 + 9 + 13 + \cdots + 425$
   (c) $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{50}$
   (d) $2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2n$
   (e) $\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{100}{101}$

7. Expand the following sums and products, that is, write them out the "long way":

a. $\sum_{k=1}^{100}(3+4k)$.

b. $\sum_{k=0}^{n} 2^k$.

c. $\sum_{k=2}^{50} \frac{1}{(k^2-1)}$.

d. $\prod_{k=2}^{100} \frac{k^2}{(k^2-1)}$.

e. $\prod_{k=0}^{n}(2+3k)$.

8. A **triangular number** is a number of the form

$$T_n = 1+2+3+4+\cdots+n.$$

(a) What are T_1, T_2, T_3, T_4?

(b) Draw a picture that illustrates why these are called 'triangular' numbers. (Hint: bowling pins)

(c) We are going to prove that $T_n = \frac{n(n+1)}{2}$ in a bunch of different ways.

1) Using your picture, extend your "triangle" to a "rectangle" to get a "picture proof" that

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

2) Look at the two lines below: Explain why these are both the same.

$$\begin{array}{ccccccccccccc} T_n & = & 1 & + & 2 & + & 3 & + & \cdots & + & (n-1) & + & n \\ T_n & = & n & + & (n-1) & + & (n-2) & + & \cdots & + & 2 & + & 1 \end{array}$$

Now add the two lines together to get that

$$2T_n = (n+1)+(n+1)+\cdots+(n+1)+(n+1).$$

How many times does $(n+1)$ appear on the right hand side? Use this to complete the proof that $T_n = \frac{n(n+1)}{2}$.

3) In class next week we will use something called Mathematical Induction to complete this proof.

9. In the popular song "The 12 days of Christmas" there are gifts given on each of 12 days. Using the Google, familiarize yourself with the lyrics and answer the following questions.

(a) Using your formula from the previous problem, how many gifts are given on the 12th day? Check your answer by manually adding up the numbers.

(b) How many gifts are given on each of the first 5 days? You should write down 5 numbers.

(c) Now write down how many **total** gifts have been sent after each of the first 5 days. So for instance, after the second day, they've received $1+(1+2)=4$ gifts, so the second number on your list should be 4. Your sequence you is called the **sequence of partial sums.** And should be bigger than the numbers you got in part a).

(d) Google OEIS and go to the website for the Online Encyclopedia for Integer Sequences and type in your 5 numbers from part b). You should see something about "pyramidal" numbers. Can you draw a picture representing why you think these might be called that? Go back to your work with triangular numbers above if you are stuck.

(e) Now using the formula given on the OEIS, calculate how many total gifts will be given after the 12th day.

10. Show that $a_n = 3 \cdot 2^n + 7 \cdot 5^n$ is a solution to the recurrence relation $a_n = 7a_{n-1} - 10a_{n-2}$. What would the initial conditions need to be for this to be the closed formula for the sequence? (This problem is asking you to CHECK that the formula for a_n will satisfy the given equation. I recommend you start with:

$$7a_{n-1} - 10a_{n-2} =$$

and simplify. At the end you should get a_n. You will need some algebra and some exponent rules. x and check carefully that

Quiz 7 Name: _____

(Review) 1. Let $S = \{2, 4\}$. What is $S \cup \{5, 2\}$?

Write down an element of $\mathbf{Z} \times (\mathbb{Q} - \mathbf{Z})$.

What is $\mathcal{P}(\{5, 6, 7\})$? (I want you to write this down as a set.)

$\mathcal{P}(\{5, 6, 7\}) =$ _____

Circle all of the following that are true:

$5 \in \{5, 6, 7\}$ $\{5\} \in \{5, 6, 7\}$

$5 \subseteq \{5, 6, 7\}$ $\{5\} \subseteq \{5, 6, 7\}$

2. (Hint: You might want to write down the first few terms of these sequences to help you)

Let a_n be the sequence defined by $a_n = 2n + 3$. Which of the following is the recurrence relation satisfied by a_n?

a) $a_n = a_{n-1} + 3$

b) $a_n = a_{n-1} + 2$

c) $a_n = a_{n-1} + 2n + 3$

d) $a_n = a_{n-1} + a_{n-2}$

This is an example of a [geometric sequence /arithmetic sequence /neither].

Define a new sequence as

$$s_n = a_0 + a_1 + \cdots + a_n = \sum_{k=0}^{n} a_i$$

Which of the following is a correct statement:

a) $s_n = s_{n-1} + n$

b) $s_n = s_{n-1} + s_n$

c) $s_n = s_{n-1} + a_n$

d) $s_n = s_{n-1} + s_{n-2}$

3. Consider the sequence defined by $b_k = k^2$ for $k \geq 2$. Fill in the blanks below to complete the sigma notation that would represent the sum of the first 10 terms of b_k.

$$\sum_{\square}^{\square} \square$$

4.

Write out the summation the "long way" by filling in the blanks. Note, I am asking you to fill in the first and second terms as well as that last two terms.

$$\sum_{k=1}^{20}(4k-3) = \underline{\qquad\qquad} + \underline{\qquad\qquad} + \cdots + \underline{\qquad\qquad\qquad} + \underline{\qquad\qquad\qquad}$$

Now do the same with:

$$\sum_{k=1}^{N}(4k-3) = \underline{\qquad\qquad} + \underline{\qquad\qquad} + \cdots + \underline{\qquad\qquad\qquad} + \underline{\qquad\qquad\qquad}$$

5. You are studying a problem that involves playing a game with n coins. In this game, you work out how many moves it takes to win if there are n coins and you come up with a sequence s_n that represents this. You discover that each time you add one more coin, the number of moves it takes to win will "double and then increase by 3". Write this down as a recurrence relation.

If it takes 2 moves to win the game with 1 coin, fill in the answers below:

It will take _____ moves to win with 2 coins.

It will take _____ moves to win with 3 coins.

Mathematical Induction

A Story: You find yourself facing an endless list of tasks that you must complete:

Task(1)

Task(2)

Task(3)

...

Task(100)

Task(101)

...

Task(1000000)

...

Not liking to have a todo list (let alone one with an endless list!) your goal is

GOAL: Complete ALL of these tasks

How will you cope? You decide to go to town and see if there is anyone who can help you. In the first shop you enter, you see that they sell the following services.

A) Complete Task(1) $50.00

B) Complete Task(5) $1.00

C) Complete Tasks (1) through (100) $10.00

D) Complete Tasks (20) through (10000) $15.00

E) Complete all even numbered tasks $1000.00

F) Complete all odd numbered tasks $7000.00

Question 1: Could you enlist the services of this shop to meet your **GOAL**? What would you buy?

You decide to shop around just to be sure you're not missing anything, and in the second shop you see that the have the following services:

X) IF Task(n) is completed for some n THEN Task(2n) will also be completed. $5.00

Y) IF Task(n) is completed for some n THEN Task(n+1) will also be completed. $100.00

Question 2: What happens if you buy items B and X? What tasks get completed?

Question 3: What happens if you buy items B and Y? What tasks get completed?

Question 4: What services could you buy to meet your GOAL?

This technique is called the Principle of Mathematical Induction and we will be using it a lot in the rest of the course. In a nutshell, the PMI says:

If you have a list of statements S(1), S(2), S(3), S(4) etc. and your GOAL is to prove them all then one strategy that will work is to

- Prove the first statement S(1)
- And show that for any k, IF $S(k)$ is true THEN $S(k+1)$ is true.

Sometimes induction is phrased in terms of dominoes. Imagine you want to knock over a row of dominoes all lined up. You can accomplish this by

- Making sure that any time **any** domino falls, it knocks over the next one.
- Make sure the 1st domino falls over.

Here are some problems that can be tackled by mathematical induction. For each of these we will ask:

- What is the list of statements?
- For example, what is $S(n)$, $S(1)$, $S(6)$, $S(k)$ and $S(k+1)$?

1. Statement: For all $n \in \mathbb{N}$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

$S(n)$ is the statement $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$

$S(n)$ is NOT the left hand side or the right hand side. It is the mathematical sentence saying that these are equal.

$S(1)$ is

$S(6)$ is

$S(k)$ is

$S(k+1)$ is

2. Statement: If $n \geq 1$ then $6^n - 1$ is divisible by 5.

$S(n)$: $6^n - 1$ is divisible by 5."

$S(1)$ is

$S(6)$ is

$S(k)$ is

$S(k+1)$ is

3. Statement: For all integers $n \geq 5$ $n^2 < 2^n$.

$S(n)$ is the statement "$n^2 < 2^n$"

$S(1)$ is

$S(6)$ is

$S(k)$ is

$S(k+1)$ is

Here are 4 statements that we can prove by Mathematical Induction

- As we work through these, think about the dominoes that we are setting up at each step.

1) Let n be a positive integer. Then

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

2) Suppose that f_n represents the nth Fibonacci number. Prove that for all $n \geq 0$,

$$f_0 + f_1 + f_2 + \ldots + f_n = f_{n+2} - 1.$$

Proof: Let $S(n)$ be the statement:

$$f_0 + f_1 + f_2 + \ldots + f_n = f_{n+2} - 1.$$

We will use induction on n starting with $n = 0$. The statement $S(0)$ says that $f_0 = f_2 - 1$ which is true since both sides are 0. Now as our induction hypothesis suppose that the statement $S(k)$ is true. That is, that

$$f_0 + f_1 + f_2 + \ldots + f_k = f_{k+2} - 1.$$

We want to show that $S(k+1)$ is true, so we need to study the sum $f_0 + f_1 + f_2 + \ldots + f_{k+1}$ and we hope to prove this is equal to $f_{k+3} - 1$.

Now,

$$\begin{aligned} f_0 + f_1 + f_2 + \ldots + f_{k+1} &= f_0 + f_1 + f_2 + \cdots + f_k + f_{k+1} \\ &= (f_0 + f_1 + f_2 + \cdots + f_k) + f_{k+1} \\ &= (f_{k+2} - 1) + f_{k+1} \\ &= f_{k+2} + f_{k+1} - 1 \\ &= f_{k+3} - 1 \end{aligned} \qquad \square$$

3) Prove that if $n \geq 4$ then $n! \geq 2^n$

4) Prove that if n is a positive integer then

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

Proof: We will prove this statement by induction on n. The base case says that $1 \leq 2 - 1$ which is true. So now assume as our induction hypothesis that

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$$

We want to prove that

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq$$

So let's analyze the left hand side:

$$\begin{aligned} \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} &= \left(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{k^2}\right) + \frac{1}{(k+1)^2} \\ &\leq \qquad\qquad\qquad\qquad + \frac{1}{(k+1)^2} \end{aligned}$$

Prove that if n people attend a party then there will be $\frac{n^2-n}{2}$ handshakes (if everyone shakes everyone else's hand).

Proof: We will use induction on n. The base case says that if

As our induction hypothesis suppose that if k people attend a party then there will be $\frac{k^2-k}{2}$ handshakes. We want to show that if $k+1$ attend the party that there will be handshakes.

Strong Induction

You have a 5 cent and 8 cent postage stamps and you can use any combination of these to mail a letter. Let $S(n)$ be the statement: "You can make n cents postage with 5 and 8 cent stamps." When do you think $S(n)$ is true? Prove your result.

This proof was an example of something called **strong induction** which works as follows:

- Prove some base cases (you might need more than one)
- Show that IF $S(1), S(2), \ldots, S(k)$ are true THEN $S(k+1)$ is true.

This is like saying "Show that IF dominoes $1, 2, 3, \ldots k$ have fallen over then so will domino $k+1$."

You have a candy bar with n squares of chocolate ($n \geq 1$) arranged in a rectangular grid. Prove that no matter how you break up the candy bar, one break at a time, it will take a total of $n-1$ breaks to break up the bar.

Proof. Let $P(n)$ be the statement, "it takes $n-1$ breaks to reduce a n-square chocolate bar to single squares."

Base case: Consider $P(2)$. The squares must be arranged into a 1×2 rectangle, and we require $2-1=1$ breaks to reduce this to single squares.

Inductive case: Fix an arbitrary $n \geq 2$ and assume $P(k)$ is true for all $k < n$. Consider a n-square rectangular chocolate bar. Break the bar once along any row or column. This results in two chocolate bars, say of sizes a and b. That is, we have an a-square rectangular chocolate bar, a b-square rectangular chocolate bar, and $a+b=n$.

We also know that $a < n$ and $b < n$, so by our inductive hypothesis, $P(a)$ and $P(b)$ are true. To reduce the a-square bar to single squares takes $a-1$ breaks; to reduce the b-square bar to single squares takes $b-1$ breaks. Doing this results in our original bar being reduced to single squares. All together it took the initial break, plus the $a-1$ and $b-1$ breaks, for a total of $1+a-1+b-1=a+b-1=n-1$ breaks. Thus $P(n)$ is true.

Therefore, by strong induction, $P(n)$ is true for all $n \geq 2$.

QED

Theorem: Let $n > 1$ be an integer. Then n is either prime or it can be written as a product of primes.

First, the idea: if we take some number n, maybe it is prime. If so, we are done. If not, then it is composite, so it is the product of two smaller numbers. Each of these factors is smaller than n (but at least 2), so we can repeat the argument with these numbers. We have reduced to a smaller case.

Now the formal proof:

Proof. Let $P(n)$ be the statement, "n is either prime or can be written as the product of primes." We will prove $P(n)$ is true for all $n \geq 2$.

Base case: $P(2)$ is true because 2 is indeed prime.

Inductive case: assume $P(k)$ is true for all $k < n$. We want to show that $P(n)$ is true. That is, we want to show that n is either prime or is the product of primes. If n is prime, we are done. If not, then n has more than 2 divisors, so we can write $n = m_1 \cdot m_2$, with m_1 and m_2 less than n (and greater than 1). By the inductive hypothesis, m_1 and m_2 are each either prime or can be written as the product of primes. In either case, we have that n is written as the product of primes.

Thus by the strong induction, $P(n)$ is true for all $n \geq 2$.

QED

Homework 8 Part 1 - Due NEXT CLASS ON WEDNESDAY

Homework this week will be a little bit different. We will be working on problems each day in class and you will complete some exercises at home. These will be due each day. These will be graded more carefully than usual and will count as your quiz score. You will get completion credit for HW8 as a bonus for turning everything in on time.

1. All of the following are statements that we might prove by induction. For each of these statements please
   - Write what statements $S(k), S(1), S(5)$, and $S(k+1)$ are. These should all be statements (i.e. a sentence or an equation, or an inequality, not a number.)
   - Determine whether $S(1)$ and $S(5)$ are true or false. I will want to see that you checked these.
   - Note - I'm not asking you to prove these - please read the instructions so you don't do more work than necessary.

   (a) $1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$

   Sample Solution:
   $S(n)$ says $1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$.
   $S(1)$ says $1 = \frac{1(2)}{2}$. This is true since $1 = 1$.
   $S(5)$ says $1+2+3+4+5 = \frac{5(6)}{2}$ this is true since $15 = 15$.
   $S(n+1)$ says $1+2+3+4+\cdots+n+1 = \frac{(n+1)(n+2)}{2}$

   (b) $1+2^n \leq 3^n$

   (c) If n people are at a party then there are $\frac{n^2-n}{2}$ handshakes between them.

   (d) Let x be a positive real number. Then $(1+x)^n \geq 1+nx$.

   (e) $\displaystyle\sum_{k=1}^{n} k(k+2) = \frac{n(n+1)(2n+7)}{6}$

2. You have a 3 cent and 5 cent postage stamps and you can use any combination of these to mail a letter. For instance you could make 11 cents by using two 3-cent and one 5-cent stamp. Let $S(n)$ be the statement: "You can make n cents postage with 3 and 5 cent stamps." Determine whether $S(1), S(2), S(3), \ldots, S(12)$ are true or false. I expect you to list all 12 answers and support the "true" statements by indicating how to get that postage.

3. You have already read the Zybooks for induction, and now to get extra review I want you to read the section here: `http://discrete.openmathbooks.org/dmoi3/sec_seq-induction.html`. Choose one of the examples 2.5.1, 2.5.2, 2.5.3 and copy down the proof into your notes slowly and carefully. Your goal is to understand what you are reading and writing. Then do the same with Exercise 3 (the one about $7^n - 1$). Again, the solutions are posted. I want you to look at the explanations on the right hand side and make sure you see how they connect with the equals signs. In general proofs might not have all these reasons spelled out and you'll have to turn up your brain to think how the statements are related. Now is your time to practice reading and understanding through writing.

Homework 8 Part 2 - Due NEXT CLASS ON FRIDAY

1. The key to induction is thinking about how to build from simpler cases to more complicated one. For practice, I want you to consider the following problem:

   Suppose that there is some mysterious property X that some numbers have and others don't. You study this property and learn the following

   Lemma: If a and b are two numbers that have property X then $a+b$ also has property X.

   Now I want you to write a proof explaining how you could USE this Lemma to prove the following:

   Theorem 1: Suppose that c, d, n, m are numbers that each have property X. Show that

   $$c+d+n+m$$

   has property X. (Hint: your proof should use the Lemma at least 3 different times)

   Now consider

   Theorem 2: Suppose that $x_1, \ldots, x_5$ are numbers that each have property X. Show that

   $$x_1 + x_2 + x_3 + x_4 + x_5$$

   has property X.

   - Prove Theorem 2 in two different ways. First use Lemma 1 repeatedly. You should use the lemma multiple times.
   - Prove Theorem 2 USING Theorem 1 AND the Lemma. I want to see you use Theorem 1 here.

   I hope you feel like a pro using this Lemma. The idea is that you can USE it as a tool to help simplify bigger problems. Induction is like this - our induction hypothesis becomes a tool that we can use.

2. Using induction, prove that if $n \geq 1$ then $n^3 - n$ is a multiple of 3. I have made a video of me proving a similar statement here. Watch this video for advice on how to structure your proofs: `https://drive.google.com/open?id=1aK4G1X_ZL92PrgVcuPf5C8j7059nqb4H`

3. Now it's your turn to write your own proof by mathematical induction. Prove that for all $n \geq 1$:

   $$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdot + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}.$$

   (Hint: After you write the induction hypothesis $S(k)$ I recommend you write something like: "I will now examine $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + ???$" [and then simplify this using the IH as a tool]")

Homework 8 Part 3 - Due NEXT CLASS ON WEDNESDAY

1. The notation $\binom{n}{k}$ is defined when $n \geq k$ as follows

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

   (a) Using this formula calculate $\binom{5}{2}$ and $\binom{10}{2}$. You should get 10 and 45.

   (b) For more practice, work out all the numbers $\binom{4}{k}$ where $0 \leq k \leq 4$.

   (c) Read the (very short section) entitled Pascal's Triangle here: `http://discrete.openmathbooks.org/dmoi3/sec_counting-binom.html`. Make sure your numbers match the ones in Pascal's Triangle.

   (d) One of the most important properties of Pascal's Triangle is **Binomial Theorem**, which says that

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

   This is a generalization of the formulas you know like

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

   Using Pascal's Triangles to help you get the numbers, I want you to write down what the binomial theorem would say that $(x+y)^6$ would equal. I want you to get practice with notation. There will be a total of 7 terms, $k = 0, 1, \ldots, 6$. What are the **exponents of** x, y and what are the **coefficients**.

   (e) In the previous step you should have gotten a formula that looks like:

$$(x+y)^6 = \text{ sum of a bunch of terms.}$$

   This formula is true for ALL values of x and y. Go ahead and try it by checking what happens when you set $x = 1, y = 1$. Check that both sides are the same. What happen when you set $x = 1, y = -1$? Again, check that both sides are the same.

   (f) Using what you noticed above, write a proof that **uses** the Binomial Theorem to prove that if n is a positive integer then

$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

   (Hint: Your proof should only be about 1 or 2 lines long. You don't want to prove the binomial theorem but you want to use it to prove the equation above.)

   (g) (Bonus for fun) Trying to calculate big factorials like 1000! is hard if you don't have lots of room in memory. However, there are wonderful approximations, like Stirling's Approximation:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

   Yes, it really involves both e and π.

2. Let's write some induction proofs:

   (a) Prove that for all positive integers n

$$1 \cdot 3 + 2 \cdot 4 + \cdots + n \cdot (n+2) = \frac{n(n+1)(2n+7)}{6}$$

   (this was on our first part of the homework from this unit).

(b) Recall the Fibonacci numbers start with $f_0 = 0, f_1 = 1$ and then $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. Prove that for all $n \geq 1$

$$f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}.$$

(c) (Bonus - Optional) Prove that for all $n \geq 0$

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

This proof isn't so enlightening, but if you want to grind through some algebra, you might enjoy it.

3. Let's write a few proofs by strong induction as well. Solve the postage stamp problem with postage amounts of 3 cents and 7 cents. I am asking you to determine for what amounts n of postage it is possible to make exactly that much using 3 and 7 cent stamps. You should find that from some point onwards you can always make n postage. Prove this claim using induction like we did in class.

4. This will require a bit of strong induction as well. You can do it! Prove that for all $n \geq 1$,

$$f_{n+6} = 4f_{n+3} + f_n,$$

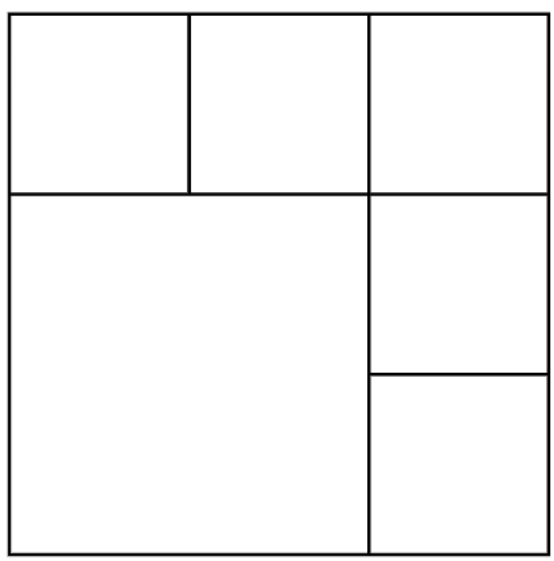
where these are the Fibonacci numbers. For your induction hypothesis you will want to assume that not only does

$$f_{k+6} = 4f_{k+3} + f_k,$$

but also all smaller values as well, so for instance another tool in your toolkit might be

$$f_{k+5} = 4f_{k+2} + f_{k-1}.$$

5. How many squares can you cut a square into? You are allowed to cut the square into smaller squares by cutting along lines parallel to the sides of the original square (these lines do not need to travel the entire side length of the original square). For example, by cutting along the lines below, you will divide a square into 6 smaller squares:



You could also just divide it evenly along the sides to get 4 squares. So far we have found a way to cut our square into 4 pieces, 6 squares. Can you find a way to cut it into exactly two squares? (you answer should be no!) what about 5 squares? 7 squares? 8 squares? Prove by (strong) induction that it is always possible to cut a square into n smaller squares if $n \geq 6$.

Theorem: If $n \geq 1$ then $n^2 - n$ is even.

Proof: Let $S(n)$ be the statement that $n^2 - n$ is even. I will prove that this is true for all $n \geq 1$ by mathematical induction.

Base Case: If $n = 1$, then the statement says that $1^2 - 1$ is even, which is true.

Inductive Step: Suppose that $S(k)$ is true for some k. That is, that

$$k^2 - k = 2j \text{ for some integer } j.$$

We want to show that $S(k+1)$ is true, that is, that $(k+1)^2 - (k+1)$ is even. So let's simplify $(k+1)^2 - (k+1)$:

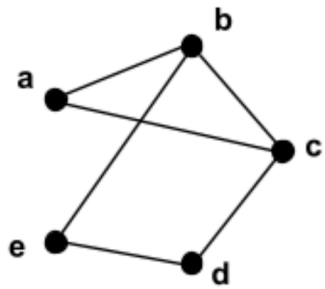
$$\begin{aligned}(k+1)^2 - (k+1) &= k^2 + 2k + 1 - (k+1) \\ &= k^2 + 2k - k \\ &= k^2 + k\end{aligned}$$

By our induction hypothesis, we know that $k^2 = k + 2j$, so if we substitute this in:

$$\begin{aligned}(k+1)^2 - (k+1) &= (k + 2j) + k \\ &= 2k + 2j = 2(k + j)\end{aligned}$$

1 Introduction to Graph Theory

This chapter is all about **graphs**. It might be helpful to think about a graph as a _____.



What are some of the key words you read about in the reading this week. Jot them down next to the graph above.

What are some examples of graphs that occur in the real world. Write down 3 different examples. If you are stuck - think about any system where there are nodes or vertices, and edges that connect them.

Throughout this week and next we will be exploring some interesting questions and applications about graph theory. I strongly recommend you make a sheet with vocabulary about graphs and keep this nearby when doing the readings and homework.

1) Alice, Bob, Cameron, Dani, and Euler are all members of the social networking website Facebook. The site allows members to be friends with each other. It turns out that Alice and Cameron are friends, as are Bob and Dani. Euler is friends with everyone. Represent this situation with a graph. After you have drawn your graph, talk with your group about what the degree of each vertex is. Is this graph regular? What is its total degree? What does the degree of a given vertex represent in this application? Explain how the total degree is related to the number of connections.

Theorem: If we add up the degrees of all the vertices in a graph G with vertices V and edges E the sum will always equal twice the number of edges.

$$\sum_{v \in V} \deg(v) = 2 \cdot |E|.$$

2) If the degrees of a graph G are: $\{4, 4, 3, 3, 3, 2, 1\}$. How many vertices does G have? how many edges does it have? Can you draw a picture of a graph G with these degrees? Compare your graph with your neighbor's - are the graphs equal?

3) Each of three houses must be connected to each of three utilities. Draw a graph that represents this situation. Is it possible to arrange the houses and utilities somehow so that none of the utility lines cross? What is the degree of each vertex? Is this a **regular** graph? Is it a **bipartite** graph? Is it a **complete** graph?

.

Property $\star$: A graph has property $\star$ if either one of the following conditions (or both) is true:

- There are three vertices such that there is an edge between all three pairs of them. (This is called a 3-"clique". It's like a friend group where everyone knows everyone.)
- There are three vertices where there are NO edges between any of the 3. (This is like where there are 3 people, none of whom are friends.)

4)

a.) There is a party with 4 people there. Using a graph, with edges representing friendship of people of a graph that does NOT have Property $\star$.

b.) After you complete part a), can you draw a graph with 5 people that doesn't have property $\star$?

c.) What about for 6 people? Why or why not?

How many people do you need at a party so that no matter what, you can guarantee that either there is a set of k mutual friends, or a set of k mutual strangers?

If $k = 3$: _____

If $k = 4$: _____

If $k = 5$: _____

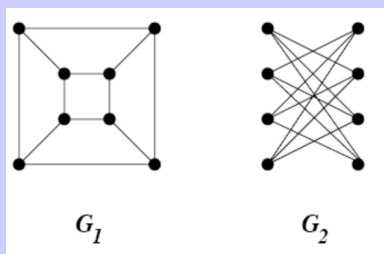
If $k = 6$: _____

2 Graph Isomorphisms

Warmup: Explain why the two graphs below are **isomorphic**:

Two graphs are isomorphic if their vertices can be relabeled so that the graphs are EQUAL.

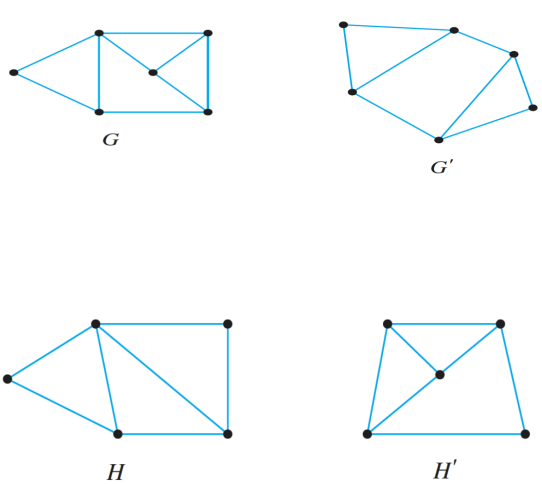
In general it is quite hard to tell if two graphs are isomorphic. For instance, the two graphs below are isomorphic, but I'd hardly say it's easy to see!

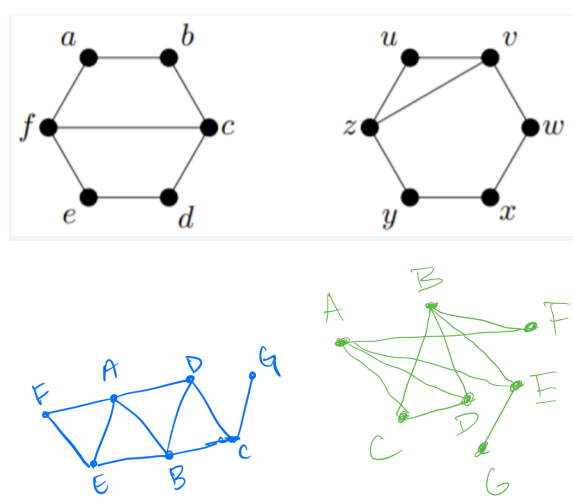


- There is no known "efficient"[a] algorithm to determine if two graphs are isomorphic.
- Even if you know they are isomorphic, there's no efficient way to find the labeling of the vertices that gives the isomorphism.
- This has applications to "zero-knowledge" proofs.[b]
- There are some strategies, but at the end of the day you might need to just try every possible labeling of the vertices and see if the graphs line up. Yuck!

[a] polynomial time
[b] See `https://jeremykun.com/tag/graph-isomorphism/`

Sometimes it can be **easier** to tell if two graphs are not isomorphic, by looking at **properties** or **invariants** of the graph and seeing if they are match. Look at the examples below, can you explain why the pair of graphs are not isomorphic?





True or False:

(T/F) If two graphs are isomorphic then they have the same number of vertices.

(T/F) If two graphs are isomorphic then they have the same number of edges.

(T/F) If two graphs are isomorphic then they have the same degree sequence.

(T/F) If two graphs are isomorphic then both graphs have the same "number of triangles".

All of the above are examples of **invariants of the graph.** These are describing properties of the network and don't depend on the names of the nodes.

Now carefully think about the statements below:

(T/F) If two graphs have the same number of edges they are isomorphic.

(T/F) If two graphs have the same degree sequence they are isomorphic.

(T/F) If you check a lot of properties and both graphs agree, then the graphs are isomorphic.

(T/F) If two graphs with 4 vertices have the same degree sequence then they are isomorphic.

(T/F) If two graphs with 5 vertices have the same degree sequence then they are isomorphic.

Questions on Size:
What is the maximum number of edges for a graph with n vertices (hint: think about the handshake problem)

To give a graph is the same as choosing a _____ of the set of all possible edges. So what is the total number of possible graphs? (not yet accounting for isomorphism)

How many non-isomorphic graphs are there with n vertices? Starting with $n = 1$ vertex the sequence is:

Check out `https://oeis.org/A000088`

Chapter 9 Homework Problems

Due: Friday March April 8th

Homework is always due on Quiz days. I'll tentatively put a due date on each homework, but this might get pushed back depending on how much we cover in class.

Zybooks Problems: (These are recommended for practice with the quiz - you do not need to write these down)

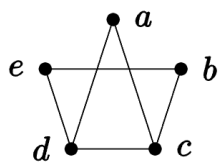
9.1.1, 9.1.3, 9.1.4, 9.2.3, 9.3.1, 9.3.2

Additional Problems These are taken from Open Discrete Math. I highly recommend reading this section of that book and checking the site for hints and solutions to some of these problems.

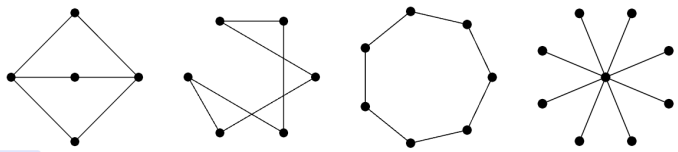
1. Among a group of 5 people is it possible for everyone to be friends with exactly 3 people? Why or why not?
2. It is possible for two graphs to be different (non-isomorphic) but yet they still have the same number of vertices AND the same number of edges. Draw a picture of two graphs that illustrates this. Explain why your graphs are not isomorphic.
3. It is possible for two graphs to be different (non-isomorphic) but yet they still have the same number of vertices AND the same number of edges AND the degrees of the vertices in the two graphs are the same (so both graphs have vertices with degrees 1, 2, 2, 3, and 4, for example) Draw a picture of two graphs that illustrates this. Explain why your graphs are not isomorphic.
4. Are the two graphs below equal? Are they isomorphic? Why or why not?

   Graph 1: $V = \{a, b, c, d, e\}$, $E = \{\{a, b\}, \{a, c\}, \{a, e\}, \{b, d\}, \{b, e\}, \{c, d\}\}$

   Graph 2:



5. Which of the graphs below are **bipartite**?

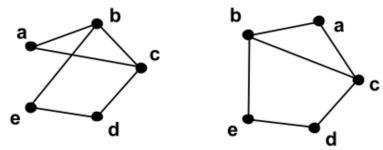


6. Is it possible to have two different (non-isomorphic) graphs with 5 vertices with total degree 20? Why or why not?
7. Consider graphs with n vertices. Remember, graphs do NOT need to be connected.
   (a) How many edges must the graph have to guarantee at least one vertex has degree two or more? Prove your answer.
   (b) How many edges must the graph have to guarantee all vertices have degree two or more? Prove your answer.

   (Hint: You might want to answer the questions for some specific values of n to get a feel for them, but your final answers should be in terms of n.)
8. Suppose G is a connected graph with $(n > 1)$ vertices and $n - 1$ edges. Prove that G has a vertex of degree 1. Hint: Use the Handshake Theorem. What would happen if every vertex had degree ≥ 2?

1 Applications of Graph Theory

A planar graph is a graph that can be drawn in the plane without any edges crossing. Below are two embeddings of the same graph. Which is a planar embedding?



Does every graph have a planar embedding? [Yes / No]

The graph $K_{3,3}$ is not a planar graph. Let's see why:

In the argument above we appealed to the fact that a planar graph will have **regions or faces** formed by the edges. On Monday's class we will prove **Euler's Formula** which gives a relationship between the number of vertices, edges, and regions in a connected planar graph:

$$v - e + f = 2.$$

Important Point: In Euler's Formula for graphs we always count the "outside" region as a face.

Let's get some practice **using** Euler's Formula.

1) Is it possible for a connected graph with 7 vertices and 10 edges to be drawn so that no edges cross and create 4 faces? Explain your answer.

2) Is it possible for a connected graph with 6 vertices to have degree sequence: 2,2,3,4,4,5? If so, how many faces would it have? If not, explain.

3) Is it possible for a connected graph with 5 vertices to have 12 edges and 9 faces?

For now, we're going to get some practice drawing graphs. The graphs below are all planar. Draw pictures to illustrate this.

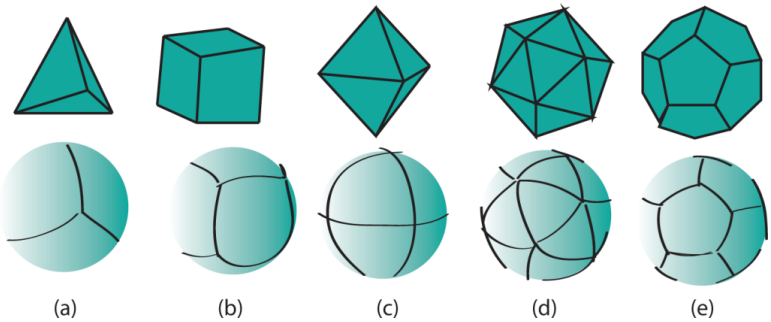
$K_4, \quad K_{2,2}, \quad K_{2,3}, \quad K_5$

Next we will look at the **polyhedra** you have around the room. These are 3D shapes that have vertices, edges, and faces. If you just look at the edges and the vertices you will get a graph. Which of these graphs are planar? Draw the ones that have a planar embedding. If you finish early - which are bipartite?

Tetrahedron(4 vertices), Octahedron (6 vertices), Cube (8 vertices),

Dodecahedron (12 vertices), Icosahedron (20 vertices)

All of these shapes have planar embeddings - (as do all 3D convex polyhedra) for the following reason: We can project these shapes onto a sphere, and then cut the sphere open, stretch and flatten it to a graph.



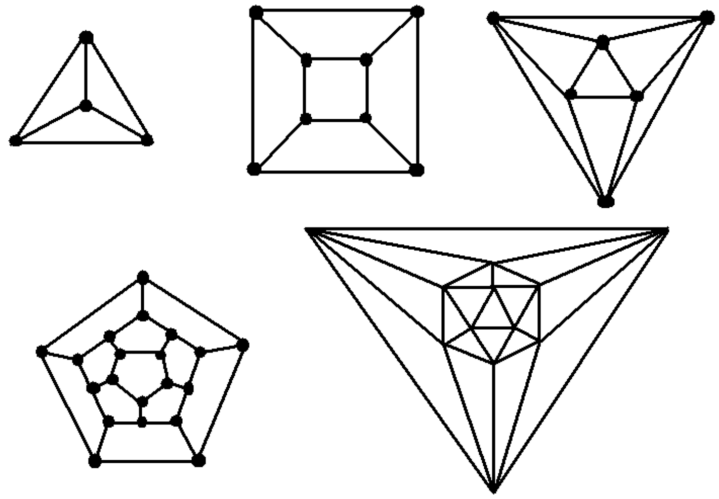
This proves that even for 3D polyhedra, Euler's Formula is still true. (Why?)

Is there a convex polyhedron consisting of three triangles and six pentagons?

What about three triangles, six pentagons and five heptagons (7-sided polygons)?

(Homework problem for after Easter Break:) Is there a connected planar graph with an odd number of faces where every vertex has degree 6? Prove your answer.

I'm thinking of a polyhedron containing 12 faces. Seven are triangles and four are quadralaterals. The polyhedron has 11 vertices including those around the mystery face. How many sides does the last face have?



2 Why is Euler's Formula True?

Recap from last time:

- Planar graphs are ones that can be drawn in the **plane, without** any edges crossing.
- Not every graph is planar
- **IF** a graph is planar **THEN** Euler's formula relates the number of vertices, edges and faces of the graph.

Warmup:

A few weeks ago we proved the handshake theorem, that if there are n people at a party then if everyone shakes hands there will be $\frac{n^2 - n}{2}$ handshakes. Chat with your neighbor about how the inductive step worked.

I'd like everyone to draw a **connected, planar** graph below with somewhere between 5 and 10 edges, and plenty of edges. Once you have your graph, label the number of vertices, edges and faces for your graph. Don't forget that the "outside region" counts as a face.

Theorem: Euler's Formula says that in any **connected, planar** graph with v vertices, e edges, and f faces, we have

$$v - e + f = 2.$$

- Does your graph satisfy this formula?
- If you were going to try and prove that this formula was true for ANY connected planar graph, what would you try?
- If I were to suggest induction could we induct on the number of vertices? number of edges? faces?
- What would a "base case" be?

Write down three ideas or questions you have.

We are going to prove Euler's Formula by induction on _____.

The base case says that:

Induction Step:

Applications of Euler's Formula

Last time we saw that Euler's formula is still true for 3D (convex) polyhedra. We are going to focus on studying Platonic Solids.

Definition: A platonic solid is a 3D solid (fancy word: convex polyhedron) whose faces are all identical, regular polygons meeting at the same three-dimensional angles. The same number of polygons must come together at each vertex. Let's call this the "Meeting Number" M.

In our classroom we have examples of 5 different platonic solids. What are the meeting numbers for these shapes?

Name	v	e	f	M
Tetrahedron (4 triangles)	4	6	4	
Cube (6 squares)	8	12	6	
Octahedron (8 triangles)	6	12	8	
Dodecahedron (12 pentagons)	20	30	12	
Icosahedron (20 triangles)	12	30	20	

We can physically inspect these shapes and see that they all match our **definition**. But how do we know there aren't any more? Maybe there's another way to put a bunch of triangles together? Or maybe some way to put together a bunch of 10-sided shapes? Let's use Euler's formula to help us.

We'll do the case with triangles, and you will do the remaining cases on your **homework.**

Warmup: You're wondering if you you could build a 3D solid shape with 40 triangles, how many edges would it have? You think that each triangle has 3 edges, so that's a total of 120 edges in the 3D shape, right? **Critique and correct this argument**.

So if we have f triangles, how many edges do we have?

What about the number of vertices?

What does Euler's formula say?

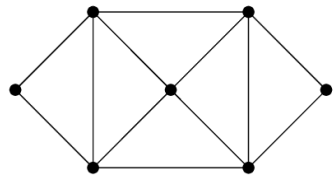
(These questions will appear on the homework this week)

- Is there a convex polyhedron consisting of three triangles and six pentagons?
- What about three triangles, six pentagons and five heptagons (7-sided polygons)?
- Is there a connected planar graph with an odd number of faces where every vertex has degree 6? Prove your answer.
- I'm thinking of a polyhedron containing 12 faces. Seven are triangles and four are quadralaterals. The polyhedron has 11 vertices including those around the mystery face. How many sides does the last face have?

3 Trees

A **cycle** is a path that starts and stops at the same vertex, but contains no other repeated vertices.

Find 3 examples of **cycles** in the graph below.



Suppose you wanted to draw a subgraph that **touched** every vertex and **had the smallest number of edges possible.** Draw in some possibilities. What do you notice? How many edges did you use each time? Did your subgraphs have any cycles?

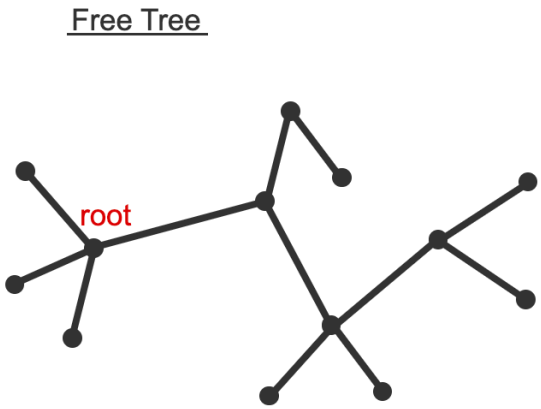
A **tree** is a graph with _____. The examples you drew in above were all examples of trees.

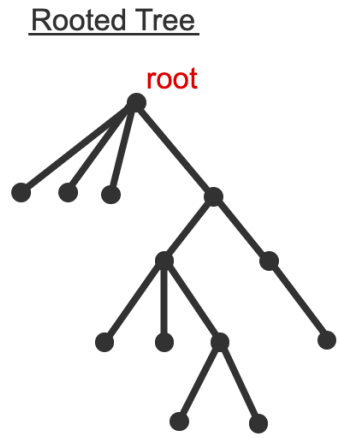
Draw some examples of trees. How many (non-isomorphic) trees with 5 vertices can you find?

True / False: Every tree is a bi-partite graph.

Remember that graphs are just about the connections - the way we draw them in the plane doesn't matter.

In applications, trees often encode relations between vertices. For instance, think of family trees, or file systems (with folders and subfolders). These are all trees, but for these the arrangement is important.





We'll go through and identify some key words: **ancestors, descendants, leaves, siblings**

Important Properties of Trees:

1) Between any two vertices there is a **unique** path between them.

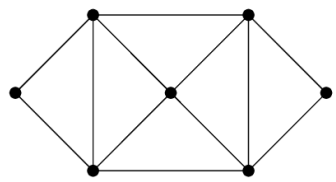
2) If a tree has n vertices then it has $n-1$ edges.

(In class we'll work through some of the proofs)

Application - Spanning Trees

Definition Let G be a simple graph. A spanning tree of G is a subgraph of G that is a tree containing every vertex of G.

Problem: How many spanning trees can you find in the graph below? Are they all isomorphic?



Problem: Do all spanning trees of a graph have to have the same number of edges?

Application of Trees: (Backtracking) On a chessboard find a way to place 4 queens on a 4x4 chess board so that none can attack the other. (Using the rules of chess, this means that no two are in the same row, column, or diagonal.)

HW Problem: For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Remember, a degree sequence lists out the degrees (number of edges incident to the vertex) of all the vertices in a graph in non-increasing order.

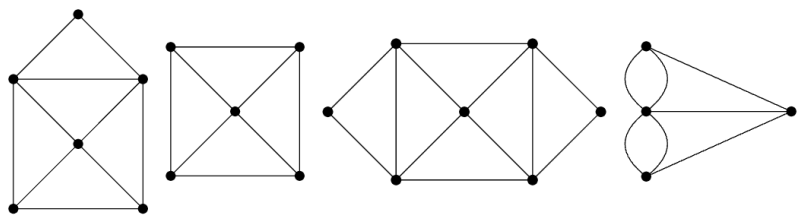
1. (4 , 1 , 1 , 1 , 1)
2. (3 , 3 , 2 , 1 , 1)
3. (2 , 2 , 2 , 1 , 1)
4. (4 , 4 , 3 , 3 , 3 , 2 , 2 , 1 , 1 , 1 , 1 , 1 , 1 , 1)

4 (Euler and Hamiltonian) Circuits and Paths

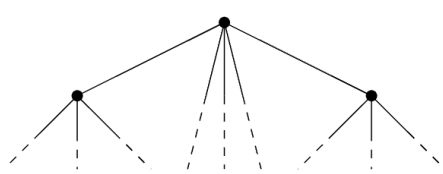
Investigate!

An ***Euler path***, in a graph or multigraph, is a walk through the graph which uses every edge exactly once. An ***Euler circuit*** is an Euler path which starts and stops at the same vertex. Our goal is to find a quick way to check whether a graph (or multigraph) has an Euler path or circuit.

1. Which of the graphs below have Euler paths? Which have Euler circuits?



2. List the degrees of each vertex of the graphs above. Is there a connection between degrees and the existence of Euler paths and circuits?
3. Is it possible for a graph with a degree 1 vertex to have an Euler circuit? If so, draw one. If not, explain why not. What about an Euler path?
4. What if every vertex of the graph has degree 2. Is there an Euler path? An Euler circuit? Draw some graphs.
5. Below is *part* of a graph. Even though you can only see some of the vertices, can you deduce whether the graph will have an Euler path or circuit?



A story about the bridges of Königsberg:

In the city of Königsberg (in Prussia) there are 7 bridges as depicted below. Is is possible to take a walk in such a way that starts somewhere, crosses every bridge exactly once, and returns where you started?

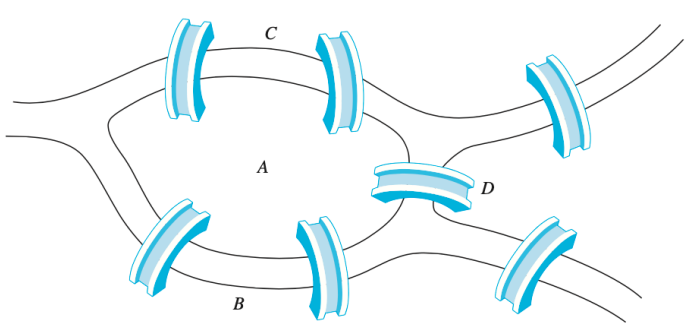
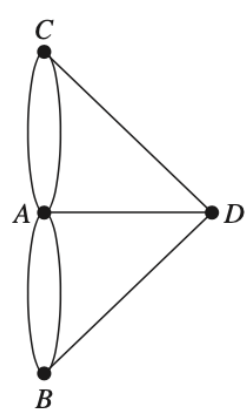


FIGURE 1 **The Seven Bridges of Königsberg.**



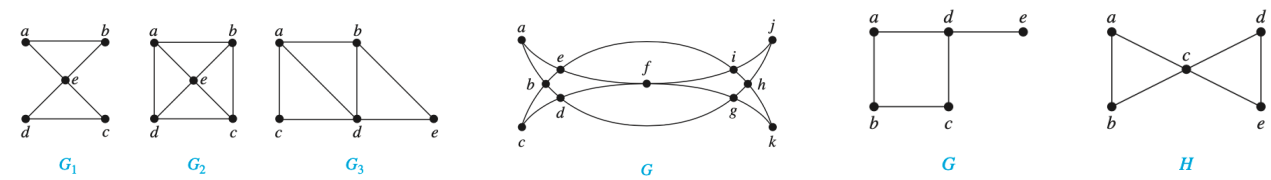
Theorem:
A graph has an Eulerian circuit <u>if and only if</u>

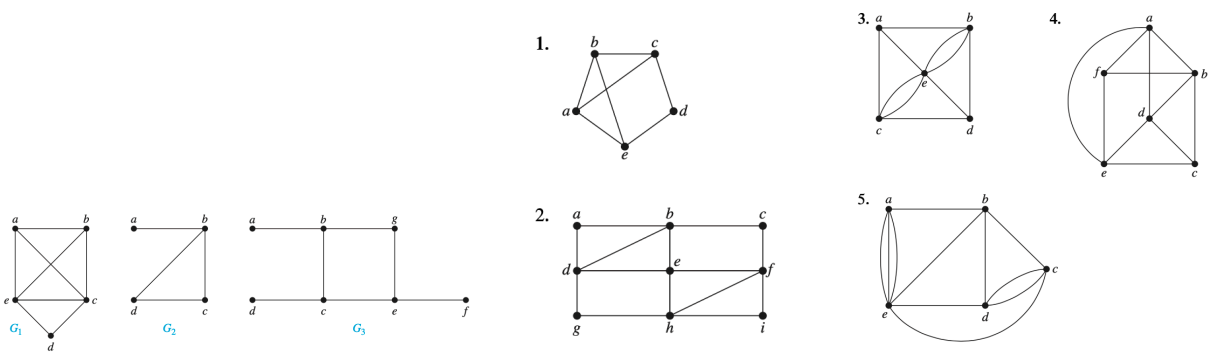
A graph has an Eulerian path <u>if and only if</u>

Let's talk about the "only if" and the "if" separately. They are saying different things:
If a graph HAS an Eulerian circuit, why does every vertex have even degree?

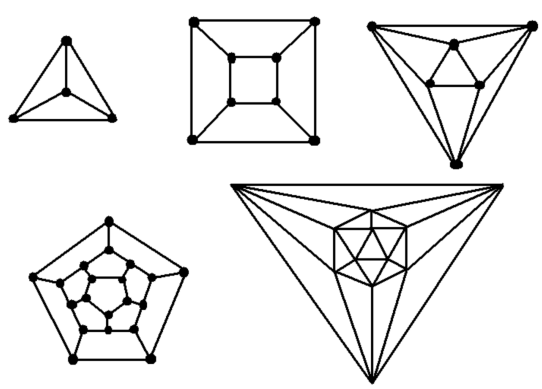
If every vertex HAS even degree, why is there an Eulerian circuit?

Here are a bunch of graphs below: Which of these have Eulerian circuits





Recall that the edges of the Platonic solids form (planar) graphs. Which of the following have Eulerian paths / Eulerian Circuits. Later we'll ask about Hamiltonian circuits.



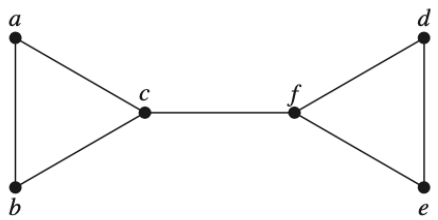
Hamiltonian Circuits and Paths

A Hamilton (or Hamiltonian) path is a walk that visits every **vertex** exactly once.

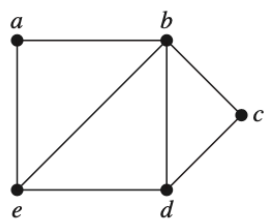
- In general there is no known way to determine if a graph has a Hamiltonian circuit. (Life is hard sometimes)
- The best approach for looking for Hamilton paths is to just try and draw one.

In Exercises 30–36 determine whether the given graph has a Hamilton circuit. If it does, find such a circuit. If it does not, give an argument to show why no such circuit exists.

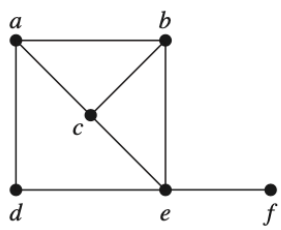
30.



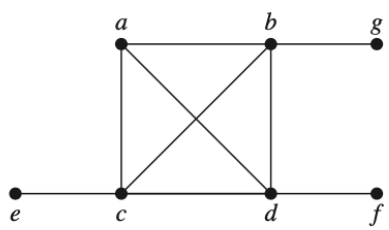
31.

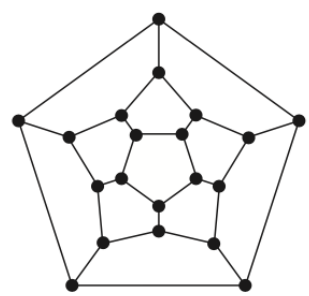


32.



33.





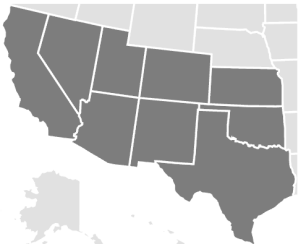
(b)

There are SOME positive results that we can say about Hamilton paths. For instance, there is Dirac's Theorem, which says:

Dirac's Theorem If G is a simple graph with n vertices, $n \geq 3$ such that the degree of every vertex in G is at least $n/2$ then G has a Hamilton circuit.

Additional Practice Problems

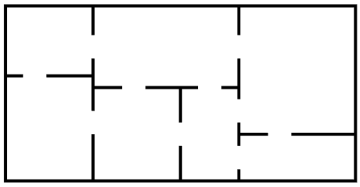
1. You and your friends want to tour the southwest by car. You will visit the nine states below, with the following rather odd rule: you must cross each border between neighboring states exactly once (so, for example, you must cross the Colorado-Utah border exactly once). Can you do it? If so, does it matter where you start your road trip? What fact about graph theory solves this problem?



2. Which of the following graphs contain an Euler path? Which contain an Euler circuit?

a. K_4 b. K_5. c. $K_{5,7}$ d. $K_{2,7}$ e. C_7

3. Edward A. Mouse has just finished his brand new house. The floor plan is shown below:



a. Edward wants to give a tour of his new pad to a lady-mouse-friend. Is it possible for them to walk through every doorway exactly once? If so, in which rooms must they begin and end the tour? Explain.

b. Is it possible to tour the house visiting each room exactly once (not necessarily using every doorway)? Explain.

c. After a few mouse-years, Edward decides to remodel. He would like to add some new doors between the rooms he has. Of course, he cannot add any doors to the exterior of the house. Is it possible for each room to have an odd number of doors? Explain.

4. For which n does the graph K_n contain an Euler circuit? Explain.

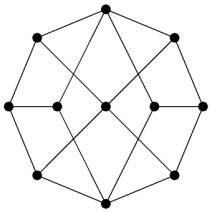
5. For which m and n does the graph $K_{m,n}$ contain an Euler path? An Euler circuit? Explain.

6. For which n does K_n contain a Hamilton path? A Hamilton cycle? Explain.

7. For which m and n does the graph $K_{m,n}$ contain a Hamilton path? A Hamilton cycle? Explain.

8. A bridge builder has come to Königsberg and would like to add bridges so that it *is* possible to travel over every bridge exactly once. How many bridges must be built?

12. Consider the following graph:



a. Find a Hamilton path. Can your path be extended to a Hamilton cycle?

b. Is the graph bipartite? If so, how many vertices are in each "part"?

c. Use your answer to part (b) to prove that the graph has no Hamilton cycle.

d. Suppose you have a bipartite graph G in which one part has at least two more vertices than the other. Prove that G does not have a Hamilton path.

Chapter 10 Homework Problems

Due: Monday April 25th

Many of the problems on this homework assignment are taken from Discrete Math an Open Introduction. `http://discrete.openmathbooks.org/dmoi3/ch_graphtheory.html` Check out the site for hints and solutions.

1. (Questions on Planar Graphs) A) Is there a convex polyhedron consisting of three triangles and six pentagons? Why or why not?

   B) What about three triangles, six pentagons and five heptagons (7-sided polygons)?

   C) Is there a connected planar graph with an odd number of faces where every vertex has degree 6? Prove your answer.

   D) I'm thinking of a polyhedron containing 12 faces. Seven are triangles and four are quadralaterals. The polyhedron has 11 vertices including those around the mystery face. How many sides does the last face have?

2. Extend our calculations that we did in class to complete the proof that there are only 5 Platonic solids. Recall that we showed that if we wanted to use f triangles then we needed a meeting number of 3,4, or 5, and that these resulted in the tetrahedron, octahedron, and icosahedron, respectively.

   (a) Do similar calculations for the square and pentagon and show that each gives a new Platonic Solid.

   (b) (Optional Challenge) Can you use Euler's formula to show that you cannot use a shape with more than five sides to build a platonic solid?

3. For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Remember, a degree sequence lists out the degrees (number of edges incident to the vertex) of all the vertices in a graph in non-increasing order.

   (a) (4 , 1 , 1 , 1 , 1)

   (b) (3 , 3 , 2 , 1 , 1)

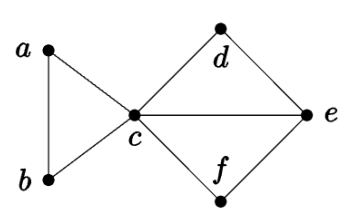
   (c) (2 , 2 , 2 , 1 , 1)

   (d) (4 , 4 , 3 , 3 , 3 , 2 , 2 , 1 , 1 , 1 , 1 , 1 , 1 , 1)

4. Suppose you have a graph with v vertices and e edges that satisfies $v = e + 1$. Must the graph be a tree? Prove your answer.

5. Unless it is already a tree, a given graph G will have multiple spanning trees. How similar or different must these be? Must all spanning trees of a given graph be isomorphic to each other? Explain why or give a counterexample. Must all spanning trees of a given graph have the same number of edges? Explain why or give a counterexample. Must all spanning trees of a graph have the same number of leaves (vertices of degree 1)? Explain why or give a counterexample.

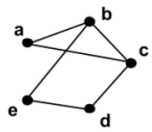
6. Find all spanning trees of the graph below. How many different spanning trees are there? How many different spanning trees are there up to isomorphism (that is, if you grouped all the spanning trees by which are isomorphic, how many groups would you have)?



7. Finally, check out some of the Euler Path problems here: `http://discrete.openmathbooks.org/dmoi3/sec_paths.html`
   - Homework is always for practice, so you can choose those that you like.
   - I highly recommend 1, 2, 9, 10.

Quiz 10 Name: _____

A) Let G be the graph below:



Is G a planar graph? [Yes / No]

Is this picture a planar embedding of G? [Yes / No]

Is G a connected graph? [Yes / No]

Does G have an Euler circuit [Yes / No]

B) Which of the following graphs are trees? (Circle all that are)

$$K_2, \quad K_3, \quad K_4, \quad K_{1,5}, \quad K_{2,4}, \quad K_{3,3}$$

Which of the following graphs have an Euler path?

$$K_2, K_{10}, \quad K_{11}, \quad K_{12}, \quad K_{1,5}, \quad K_{2,4}, \quad K_{3,3}$$

C) Let G be the graph $K_{4,7}$. How many vertices and edges does G have?

How many edges would a spanning tree for $K_{4,7}$ have?

D) In a connected planar graph with 7 edges and three faces, how many vertices must there be?

What is the degree sequence for the cube graph? (The graph of edges of the platonic solid - the cube)

How many spanning trees does K_3 have?

Does K_{12} have an Euler path? Why or why not?

A polyhedron is made that has 12 vertices and 24 edges. How many faces does it have?

E) Is there a connected planar graph with an odd number of faces such that every vertex has degree 10. Why or why not?

F) A 3D polyhedron can be made with 6 squares and 8 hexagons. How many edges and how many vertices does it have? Show your work.

1 Number Theory: Introduction

In this last section of the class we will be studying properties of the **integers**. We will see that many seemingly simple questions about whole numbers can be devilishly challenging, but that this difficulty can lead to some powerful encryption methods.

To start we will begin by talking about integer division and the division algorithm.

Warmup: Imagine you had 16 cookies to distribute to 5 children. This is an example of an **integer division**. How many cookies would you have left over?

Which of the equations below are true? Which of them represents that answer you talked about with your group above.

$$16 = 3 \cdot 5 + 1$$

$$16 = 2 \cdot 5 + 6$$

$$16 = 0 \cdot 5 + 16$$

When we want to divide one integer n by another integer d, sometimes d goes into n a whole number of times. Other times we are left with a remainder. **We want to be specific about what we mean by remainder.**

Theorem: The division algorithm
If n is an integer and d is a **positive** integer, then there are **unique** integers q and r with

$$n = qd + r, \text{ and } 0 \leq r < d.$$

The number r is called the remainder, and the number q is called the quotient.

WARNING:

Note, this last condition is extremely important - we never allow remainders that are $\geq d$.

Practice: Use the division algorithm to divide:

101 by 11

-12 by 5.

Let a be an integer and let $x = 4a - 1$. Divide x by 4.

This division algorithm is so important that it generates a whole new number system, the method of modular arithmetic:

> The symbol $n \bmod d$ will always mean "the remainder when n is divided by d"
>
> In Python, this is calculated by using the notation `n%d`

Our goal today is to just get familiar with this new notation.

Let's look at the number line and think about what "mod 5" means.

1. How many possibilities are there for $x \bmod 7$? What are they?

2. What does it mean if I say that $x \bmod 7 = 0$?

3. What does it mean if I say that $x \bmod 2 = 1$?

4. Can you think of two different integers a and b so that $a \bmod 10 = b \bmod 10$? This is what it means to be **congruent** mod 10.

5. Can you name 3 numbers that are congruent mod 4?

6. Can you name a composite number that is congruent to 1 mod 6?

7. Write down what it means for $n \bmod 7 = 3$. (Your answer should use the phrase "for some integer k".)

8. What is $-1 \bmod 7$? What is $-1 \bmod d$

On Friday I will give us a brief 5-10 minute quiz about modular arithmetic. I just want you to be able to perform basic calculations (without a calculator). I highly recommend checking the exercises on the zybooks, including 11.1 #1, 2, 3, 4, 6, and 11.2 #1,2,5. There will also be a worksheet on Wednesday with more example problems.

2 Modular Arithmetic Practice

- We typically work mod$n$ for some number n. (Usually it's the same n for the whole problem or application. Only rarely do we mix and match)
- When we work mod$n$ we are talking about the possible remainders when we divide a number by n.

  Example: If we are working mod 4 then there are 4 possible remainders when we divide an integer by 4. These are $0, 1, 2, 3$.
- Lots of different integers are **equivalent**, of **congruent** (denoted $\equiv$) mod n. We say that two numbers are equivalent if they have the same remainder when divided by n.

  Example: $17 \equiv 9 \bmod 8$ since they both have remainder 1 when you divide by 8.

  Example: $17 \equiv 1 \bmod 8$ as well.

  Example: if n is even then $n \equiv 0 \bmod 2$ (since n will leave a remainder of 0 when divided by 2.)

1. Let's just get practice seeing which numbers are equivalent mod n. Let's work mod 7 on this problem. The table below has some numbers filled in. Place the remaining numbers in the appropriate place based on what they are equivalent to.

Mod 7	
0, 21	
1, 22	
2,	
3,	
4,	
5, −2, −9	
6, −1	

7 8
9 10
−3 14
37 45
7·4

x
y
z

Where $x = 7a + 4$ for some $a \in \mathbf{Z}$

$y = 7b - 2$ for some $b \in \mathbf{Z}$

$z = x + y$.

Some questions to ponder:

- After you've filled in these numbers, how could you add more numbers to a given row?
- How far apart are the numbers in each row?

Takeaway: If two numbers are equivalent,

$$a \equiv b \bmod m \iff (a - b) \text{ is a multiple of m.}$$

2. One of the coolest things about modular arithmetic is that we can do arithmetic with numbers and it has this awesome property that if you just care about the answer $\bmod n$ then it **doesn't matter which equivalent numbers you use.**

$$x \cdot y \bmod n \equiv (x \bmod n) \cdot (y \bmod n)$$

$$(x + y) \bmod n \equiv (x \bmod n) + (y \bmod n)$$

Example: Let's check an easy case: $11 \cdot 9 \bmod 7$.

Now it's your turn:

(a) What is 687364182736487126384726 mod 10? (hint: don't reach for a calculator - think about what is left over after you divide by 10.)

(b) What is 687364182736487126384726 mod 100?

(c) What is $(2526) \cdot (423237) \mod 10$. Talk with your group and make sure everyone can do this mentally.

(d) What is $(37)(17) \bmod 7$?

(e) Describe an efficient means of reducing 7654321 mod 35 using a calculator.

(f) Use the technique developed in the previous exercise to reduce 2468 mod 11, 314159 mod 123, 106 mod 17, and 55555 mod 88. You are allowed to use a pocket calculator for this.

(g) Match the statements on the left with statements on the right:

$x \equiv 0 \mod 2$	x is odd
$x \equiv 1 \mod 2$	x is even
$0 \times 0 \equiv 0 \mod 2$	An even number times an even number is an even number
$0 \times 1 \equiv 0 \mod 2$	An even number times an odd number is an even number
$1 \times 1 \equiv 1 \mod 2$	An odd number times an odd number is an odd number
$1 + 1 \equiv 0 \mod 2$	The sum of two odd numbers is even
	The sum of two even numbers is even

(h) Draw in two different "clocks" for arithmetic modulo 7. One one, use the numbers $\{0, 1, 2, 3, 4, 5, 6\}$. On the other, use the numbers $\{0, \pm 1, \pm 2, \pm 3\}$. Do you see any pros or cons to either clock? Find the number 41 on each clock. Which clock would help you calculate $41^{2022} \bmod 7$? What is it? What is $41^{41} \bmod 7$?

3. Extra practice:

(a) Just using trial and error, and the fact that there are only finitely many possibilities, check whether the following equations have solutions. If they have solutions, say how many they have:

$$x^2 = 3 \bmod 13$$

$$2x = 1 \bmod 9$$

$$2x = 4 \bmod 10$$

$$2x = 1 \bmod 10$$

$$7x = 2 \bmod 10$$

$$7x = 1 \bmod 32$$

(b) Here is a sample of how an encryption scheme might work.

Hear Ye, Hear Ye! I am now accepting encrypted messages. Please pick your favorite three digit number N and now calculate

$$N^7 \mod 26563$$

and announce your number loudly. I have a magical way of decrypting your number. Gee, I hope no one else can figure it out!

i. Using this online calculator:

`https://planetcalc.com/8326/`

determine what the encrypted message of $N = 123$ would be.

ii. Suppose you overhear someone transmit the encrypted message of "7034". How could you figure out their original number? Could you write a short program to figure out what the original number was? How long would this process take? [‡]

iii. Do you think your approach would work if the encryption process were doing

$N^7 \mod 35794234179725868774991807832568455403003778024228226193532908190484670252364677411513516111204504060317568667$?

and N is a number in between 0 and 35794234179725868774991807832568455403003778024228226193532908190484670252364677411513516111204504060317568667?

[‡]Later we will learn how to "undo exponents" in problems like this. In this example, we'll see that to "undo" this 7 power, we can take a 3743rd power.

Homework 11

For our last homework assignment, I am going to split up the problems into different sections. These homeworks are all optional to complete, but you may want to solve them so that you can use them on our upcoming quizzes.

Problems about the basics of Modular Arithmetic

1. Consider the sequence of letters below where the first term is t:

   t, o, m, a, t, o, m, a, t, o, ...

   If I say that the nth letter is o, then write down what you know about n. (Your answer should be of the form "n = blah blah something involving mod.")

2. Determine whether the following statements are true or false.

   (a) $321 \equiv 123 \bmod 101$
   (b) $-10 \equiv 10 \bmod 6$
   (c) $3 \cdot 16 \equiv 3 \cdot 2 \bmod 7$
   (d) $91 \equiv 0 \bmod 13$
   (e) $16^2 \equiv 2^2 \bmod 7$.

3. For which positive integers $m \geq 2$ is it true that $1^4 \equiv 2^4 \bmod m$?

4. Show with an example that it is possible for $a \not\equiv b \bmod 6$ but $2a \equiv 2b \bmod 6$.

5. Prove that if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$.

6. We know that mod 2, there are only two numbers. Use this to explain why $n^3 + 3n + 5$ is always odd. (Hint: what do we need to check mod 2?)

7. What can you say about $n^5 - n + 2 \bmod 5$?

8. Evaluate these quantities.

   a) -17 **mod** 2 **b)** 144 **mod** 7
   c) -101 **mod** 13 **d)** 199 **mod** 19

   Evaluate these quantities.

   a) 13 **mod** 3 **b)** -97 **mod** 11
   c) 155 **mod** 19 **d)** -221 **mod** 23

9. Remember that modulo 4 there are only four numbers. $\{0, 1, 2, 3\}$. By checking all four possibilities, verify the statement: "If x is any integer, then x^2 must be congruent to 0 or 1 mod 4. Check your answer when $x = 7$ and $x = 10$.

10. (Use the previous exercise for this) Suppose that x and y are integers and $n = x^2 + y^2$. What are the possibilities for $n \bmod 4$? Use this to give a proof that a number of the form $4k + 3$ (for an integer k) can NEVER be the sum of two squares.

11. Write down a multiplication table for arithmetic modulo 4. Use your table to answer the following questions. Explain your answers.

    (a) True / False If x and y are two integers and $xy \bmod 4 = 3$ then either $x \bmod 4 = 3$ or $y \bmod 4 = 3$.

    (b) True / False If x and y are two integers and $xy \bmod 4 = 1$ then either $x \bmod 4 = 1$ or $y \bmod 4 = 1$.

12. (a) True or False: If x is an integer and x is congruent to 3 modulo 8 then x must be odd.

    (b) True or False: If x is an integer and x is congruent to 3 modulo 7 then x must be odd.

13. While in class we saw that lots of arithmetic works just fine when we go "mod" a number, there are two important exceptions. Find numbers n, a, b so that

    $$2a \equiv 2b \mod n$$

    but $a \not\equiv b \mod n$. This shows that we cannot "divide by 2" mod n. **In general we need to be careful with division, modulo n.**

14. Another special thing to be wary of is that exponents **cannot** be reduced mod n. Let's just convince ourselves of that: Check that $2^9 \mod 8$ is NOT the same as $2^1 \mod 8$. **We will later learn a different technique for simplifying exponents that is called Fermat's Little Theorem.**

Quick Quiz on Modular Arithmetic

1. Which is congruent to 35 mod 8?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8$$

2. Which is congruent to $(10)(-2)$ mod 6?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5$$

3. Which is congruent to $(37)(15) \mod 7$

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6$$

4. Which is congruent to $(12)^9(14)^9$ mod 13?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad 10, \quad 11, \quad 12$$

5. What is 5742991423 modulo 100?

6. A student is working mod 8 and needs to simplify the expression:

$$37x + 2 \text{ where } x \text{ is an integer}$$

which of the following would be a correct simplification mod 8?

(a) $3x + 2$

(b) $4x + 2$

(c) $5x + 2$

(d) $6x + 2$

Quick Quiz Makeup on Modular Arithmetic

1. Which of the following is 0 mod 9?

$$34, 35, 36, 37, 38, 39$$

2. Which of the following is -3 mod 8?

$$79, 80, 81, 82, 83, 84, 85, 86, 87, 88$$

3. Write down three positive numbers that are congruent to -8 mod 20.

1 Primes!

An integer n is called prime if $n > 1$ and n has no factors other than n and 1. The primes are the **building blocks of the natural numbers**. Let's see why:

The Fundamental Theorem of Arithmetic:

Any natural number $n > 1$ can be written as a product of primes. This expression is unique, up to a reordering of the prime factors.

Example: Find the prime factorizations of 100, 13, 999, 1111, 7007, 26563

You may have noticed that as the numbers get bigger it can be harder to find the prime factors.

Question: Given a (large) number N how can we find its factors? How could we test if it is prime?

With your neighbors talk about some ideas - if you had a calculator, how could you test if a number was prime: For instance, how could you test if the number 13290059 was prime? What would you try?

The method of trial division.
Given: A natural number n. Goal: Find a proper factor of n or determine if n is prime.

Algorithm: Try dividing n by 2, 3, 4, 5, 6, 7, 8, $\ldots \underline{n-1}$. If you find a factor, great - otherwise conclude that n is prime.

Questions: How high do we have to go before we conclude that n is prime?
Do we really have to check **every** number?

Better Algorithm: Try dividing n by

Cool example: The Sieve of Eratosthenes Would you like to generate all the prime numbers up to a certain point? Well here's an ancient method that will do it!

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

1.1 How many Primes are there?

Open Questions

1. How many primes are there of the form $2^n - 1$? These are called Mersenne primes. (`https://www.mersenne.org/primes/`)
2. How many primes are there of the form $2^{2^n} + 1$? These are called Fermat numbers. Fermat studied these numbers and in 1640 conjectured that all numbers of this form are prime. He verified his conjecture for $n = 1, 2, 3, 4$. (`https://en.wikipedia.org/wiki/Fermat_number`)
3. (Goldbach's Conjecture) Worth \$1,000,000) Every **even** number $n \geq 4$ is the sum of two prime numbers.
4. (Twin Prime Conjecture) There are infinitely many primes that differ by 2. Such pairs are called twin primes. For example, 17 and 19 are twin primes. So are 5 and 7.

   There was a big breakthrough on this problem in 2013, when Yitang Zhang proved that there are infinitely many primes that are within $70,000,000$ of each other. This was a fantastic achievement, and then many experts around the world worked together to improve this statement to show that there are infinitely many primes that are within 246 of each other.

Prime numbers have lots of applications - especially in computer science. We will focus on one in this class.

It is **easy-ish** to produce large prime numbers. (There are very fast algorithms[§]) but **very very very hard** to factor a large number. `https://en.wikipedia.org/wiki/RSA_Factoring_Challenge`.

- In fact, roughly $1/\ln(n)$ of the first n natural numbers are prime. So for example, if you pick a number less than $1,000,000$ there is a 7% chance the number is prime.
- There is still about a 1% chance that a random 25 digit number is prime.
- We will see that there is a very strong encryption protocol that roughly works like this:
  1. Alice wants to sell something to Bob and Bob wants to securely send his credit card number to Alice.
  2. Alice picks two large primes, p, q say with a few hundred digits each. (This is very fast)
  3. Alices keeps these numbers secret and does not share them with anyone.
  4. She multiplies them together to get a number N.
  5. Alice is **VERY** confident that no one will be able to factor N, and thus no one will be able to figure out her secret prime factors.
  6. Alice sends the number N to Bob along with some encryption instructions to Bob. People probably are overhearing / hacking etc. But that's ok. It doesn't matter who hears her number N, or the instructions.
  7. Bob will encrypt his credit card number privately on his computer using the instructions and send some encrypted number back to Alice. People probably hear this message, but Bob and Alice don't care because...
  8. Even though everyone hears Alice's **instructions,** and Bob's message, only Alice will be able to decode the message and get Bob's credit card number.
  9. This is because to decode the message, someone would **need to find the factors of** N which is **EXTREMELY HARD.** Luckily Alice has the factors safe and secure.
  10. We will learn the details of this encryption / decryption method in the next two weeks.

[§]That work "probabilistically" but in practice the chance of error is smaller than the chance of cosmic rays affecting your physical computer resulting in an error in using a deterministic algorithm

Remember: Factoring large numbers is hard!

1.2 The greatest common divisor

The greatest common divisor (gcd) of two integers a and b is

One way to find the gcd of two integers is to find their prime factorization:

Example: Find $\gcd(24, 50)$, and $\gcd(17, 22)$, and $\gcd(120, 500)$

This might be _____ if the integers are large because _____.

Good news: There is an algorithm that is very fast that can calculate the gcd of any two integers. (It could find the gcd of two 500 digits numbers in an instant!) We'll learn about this algorithm in our next class.

Definition: Two numbers are called **relatively prime** if

Problem: Find all the numbers n such that n is relatively prime to 24. How many did you find?

Definition: Let n be a positive integer. We define Euler's ϕ function as follows:

$$\phi(n) =$$

Using your work from the previous page, what is $\phi(24)$? What is $\phi(13)$? What is $\phi(p)$ if p is prime?

Theorem Let n be a positive integer, and suppose that the prime factorization of n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

Examples:

1. Check that this formula agrees with what you got for $\phi(24)$.

2. What is $\phi(216)$?

3. If p and q are primes, then what is $\phi(pq)$?

4. Is $\phi(n)$ ever prime?

2 GCD and the Euclidean Algorithm

Today we are going to learn

- That factoring **large** numbers is tough in general. Here's a fast implementation: `https://www.alpertron.com.ar/ECM.HTM`
- A fast algorithm for finding the GCD of two numbers.

Warmup: What steps would you tell the computer to factor the following two numbers?

$$a = 837829, b = 217243.$$

Answer: Use trial division, dividing a up to the number _____ and b up to the number _____.

Once you have the factors, find $\gcd(a, b)$:

Question: Do you think we would be successful if the numbers were instead

$$a = 752231879761809129364981812929139257455269462486862533619421,$$

$$b = 608009768017215266111386856381266921132657276037504362206413?$$

A modern computer can factor these in about _____

Or what about:

$$a=1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139$$

$$b=9287334039176488892156458800859628239613304861313547027375740877487841484497827475498936986056251 51$$

A modern computer can factor these in about _____.

`https://en.wikipedia.org/wiki/RSA_numbers` Has a history of some breakthroughs in factoring numbers and `https://www.mersenne.org/primes/` for history on Mersenne Primes.

Moral: Factoring numbers is feasible if the numbers are small, but once the numbers have 100 digits or more, then even the best algorithms will take a LOT of time.
Surprise: There is a way to find the GCD of two numbers (even gigantic numbers) that is EXTREMELY fast. And this was discovered over 2000 years ago! For example, even this simple applet here can find the GCD of those HUGE numbers above: `https://planetcalc.com/3298/`

The Euclidean Algorithm:

Lemma Let $a = bq + r$ where a, b, q, r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Summary of Algorithm:

To find the gcd of a and b, start with the bigger number on the left, say a:

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Example: Use the algorithm to calculate $\gcd(91, 287)$

Moral: The Euclidean Algorithm (discovered around 300 BC is extremely fast.) E.g. we can find the gcd of those giant numbers on the front page in less than a second! (Factoring them would likely take hours or days.)

This presents an interesting **scheme**. Since factoring is **hard and slow** but Euclidean algorithm is **easy and fast**, can we use this to our advantage when we encrypt and decrypt data? More on this next week!

Example: Find the gcd of 1529 and 14039 without factoring. (You'll need a pocket calculator to calculate remainders.)

Bézout's Theorem If a and b are positive integers then there exist integers s and t such that

$$as + bt = \gcd(a, b).$$

In other words, the gcd of a and b can be expressed as a **linear combination** of the original numbers a and b.

Example: The gcd of 21 and 44 is 1, (you can see this quickly by just factoring). Use the Euclidean algorithm to write 1 as a **linear combination** of the numbers 21 and 44.

Problems about Primality, GCD, LCM, and the Euclidean Algorithm

1.

Determine whether each of these integers is prime.

a) 21 **b)** 29
c) 71 **d)** 97
e) 111 **f)** 143

Determine whether each of these integers is prime.

a) 19 **b)** 27
c) 93 **d)** 101
e) 107 **f)** 113

2. Find the prime factorization of 10!
3. How many zeros are there at the end of 100!?
4. There are five numbers less than 100 that have exactly twelve divisors. Find them.
5. To help appreciate that factoring numbers is hard, try to factor 46903 just using a pocket calculator.
6. What can be said about a number if it has exactly three divisors?
7. Prove that n has an odd number of divisors precisely when n is a perfect square.
8. Prove or disprove. There are three consecutive odd positive integers that are all prime.
9.

What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$
b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
c) $23^{31}, 23^{17}$
d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
f) $1111, 0$

10.

Use the Euclidean algorithm to find

a) gcd(12, 18). **b)** gcd(111, 201).
c) gcd(1001, 1331). **d)** gcd(12345, 54321).
e) gcd(1000, 5040). **f)** gcd(9888, 6060).

11. Express the gcd of each of the following pairs of numbers by using the "reverse" Euclidean algorithm.

a) 10, 11 **b)** 21, 44 **c)** 36, 48
d) 34, 55 **e)** 117, 213 **f)** 0, 223

12. (a) Explain why the expression $n^2 - 79n + 1601$ is NOT always prime. (Hint: what value of n could you plug in and be certain that this is not prime?)

    (b) Which integers $1 \le n < 12$ are relatively prime to 12

    (c) Which integers $1 \le n < 20$ are relatively prime to 20

    (d) If p is prime, which integers $1 \le n < p$ are relatively prime to p.

13. We call a positive integer **perfect** if it is equal to the sum of its proper divisors. Show that 6 and 28 are perfect.

14. (Optional - More Challenging) Suppose that p and $2^p - 1$ are both prime. Let $n = 2^{p-1}(2^p - 1)$. Work out all the proper divisors of n and use this to show that n is perfect. (It is true that every **even** perfect number must be of this form. It is **unknown** whether there are any **odd** perfect numbers.

15. Find the following values of Euler's ϕ function.

$$\phi(6), \quad \phi(12), \quad \phi(20), \quad \phi(28), \quad \phi(p) \text{ if } p \text{ is prime.}$$

16. What is $\phi(p^k)$ is p is prime and k is a positive integer. (For instance, how many numbers are relatively prime to p^3?

17. Here is a factorization rule you might have seen before.

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

   (a) Use this to factor $x^2 - 1$, $x^3 - 1$ and $x^4 - 1$. Write out all the terms.

   (b) In each of your factorizations (which are equations that are true for ANY input x), plug $x = 3$ into both sides. Explain why this shows that $3^n - 1$ is never prime if $n \geq 2$.

   (c) Explain why this factorization shows that $x^n - 1$ is never prime if $x \geq 3$ and $n \geq 2$.

   (d) Explain why this doesn't work when $x = 2$. Where does the argument break down. For example $2^3 - 1$ IS prime, and so is $2^5 - 1$.

18. In this problem we are going to dive a little deeper into factorizations. Imagine you wanted to factor $x^8 - 1$, with the goal of understanding what $2^8 - 1$ was. If you used the formula in the previous problem you would get:

$$x^8 - 1 = (x-1)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1).$$

And if you let $x = 2$ then this would give you a boring factorization because the first factor is 1. So this doesn't help us see if $2^8 - 1$ factors.

However, take a look at this factorization, where we use the factorization of $(blah)^4 - 1$:

$$x^8 - 1 = (x^2)^4 - 1 = (x^2 - 1)((x^2)^3 + (x^2)^2 + (x^2)^1 + 1).$$

This is a really clever idea!

- Use this idea to factor $x^{15} - 1$ into two factors. Figure out what your blah could be.
- Now use your factorization to find a factor of $2^{15} - 1$ without using a calculator. Then check your result with a calculator.
- Use this idea to find a factor of $2^{77} - 1$ (which is a huge number - 151115727451828646838271), again without using a calculator.
- Find a factor of $2^{14977} - 1$ using the method of this problem. Note - this number is so huge that finding a factor by brute force would be very infeasible. But using a factorization can easily give us the answer.

Why is Bézout's Theorem so important? It helps us solve modular equations. For example, suppose you want to solve the equation:

$$101x = 1 \bmod 4620.$$

What are some methods we could try? Remember we are looking for an answer mod 4620 so there are only 4620 possibilities.

An Application: Solving Equations Modulo n: Here's a typical problem that comes up in encryption theory. You are asked to solve any equation like this:

$$7x = 1 \mod 11.$$

One simple approach is to just try all the numbers:

- mod 11 there are only 11 possible numbers, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
- Let's just try them all and see which ones are solutions.
- This might be annoying to do by hand, but it's very quick for a computer.

DO: Check that $x = 8$ is a solution, by mentally doing $7x$ and checking that it is 1 mod11.

Now imagine solving the following equations using this method:

- $7x = 1 \mod 111$
- $7x = 1 \mod 1111$
- $7x = 1 \mod 11111$
- $7x = 1 \mod 111111$
- $7x = 1 \mod 1111111$
- $7x = 1 \mod 11111111$
- $7x = 1 \mod 111111111$
- $7x = 1 \mod 1111111111$
- ...
- $7x = 1 \mod 11111111111111111111$

How much time do you think it would take to solve each of these using the naive "guess and check" algorithm?

Luckily there is a very efficient way to solve these equations, which is what we're going to learn today.

Simplifying Life Modulo n

Today we are going to learn
- How to solve the equation $ax \equiv b \mod n$ when a and n are relatively prime.
- This is like **dividing both sides by** a
- Hence we are learning how to **divide** and simplify mod n.
- Then we will learn how to simplify big exponents mod n if n is prime.

Big Question:

Suppose you want to solve an equation like[¶]:

$$101x = 1 \bmod 4620.$$

Warning: Remember that modular arithmetic is a new system, so your intuition might lead you astray. For example,

$$3 \cdot 2 = 1 \bmod 5;$$

$$4 \cdot 4 = 1 \bmod 5;$$

$$1 \cdot 1 = 1 \bmod 5;$$

There might be LOTS of solutions to "what two numbers multiplied together give you 1 if you work modulo 5."

Warmup:

1. What is $-3 \bmod 17$? (Your answer should be in the range $\{0, 1, 2, \ldots, 16\}$.
2. Which equation below represents the statement: $4x \equiv 7 \bmod 11$:
   (a) The number $4x$ leaves a reminder of 11 when we divide by 7.
   (b) The number $4x$ is 7 more than a multiple of 11.
   (c) The number $4x$ is 11 more than a multiple of 7.
3. Which equation below represents the statement: $4x \equiv 7 \bmod 11$:
   (a) $4x = 11k + 7$ for some integer k
   (b) $4x = 7k + 11$ for some integer k
   (c) $11 = 4x + 7k$ for some integer k
4. Consider the equation:
   $$(-35)(4620) + 1601(101) = 1.$$
   If we look at this equation mod 4620, which term is zero?
   (a) The first term on the left hand side
   (b) The second term on the left side
   (c) The term on the right hand side
   (d) None of the terms becomes zero, because they are all nonzero integers.

[¶] the answer is 1601

Example: Consider the equation $2x = 4 \bmod 6$. Draw the "mod 6" clock and check to see which numbers are solutions to this equation.

Use your answer above to find 5 more solutions in $\mathbf{Z}$ by finding equivalent numbers on the clock.

Example: Explain why the equation $7x = 4 \bmod 63$ has no solutions. Hint: Compare this with Warmup 3 above.

Equations of the Form

$$ax \equiv b \bmod n$$

are called **linear congruences.** They can have

- A Unique Solution (on the clock) and thus infinitely many solutions in $\mathbf{Z}$;
- No Solution;
- Multiple Solutions (on the clock) and thus infinitely many solutions in $\mathbf{Z}$.

Theorem: The equation

$$ax \equiv b \bmod n$$

has solutions if and only if $\gcd(a, n)$ divides b.

Proof: (That if there are solutions then $\gcd(a, n)$ MUST divide b.)

Suppose that $ax \equiv b \bmod n$ is true for some integer x. Then this means that

$ax =$ _____ for some integer k. Solving for b we get:

Now since $\gcd(a, n)$ divides all the terms on the _____, it must also divide _____.

When a unique solution exists: If a and n are **relatively prime** then there is

- Always a solution to $ax \equiv b \bmod n$
- That solution (on the clock) is unique.

Which of the following will have unique solutions? Which will have no solutions?

a) $3x \equiv 7 \bmod 14$

b) $12x \equiv 6 \bmod 16$

c) $32x \equiv 77 \bmod 100$

d) $34x \equiv 9 \bmod 47$

What is the inverse of a number mod n**?** If a and n are relatively prime, then the equation $ax \equiv 1 \bmod n$ always has a unique solution in $\{0, 1, 2, \ldots, n-1\}$. We call this the **inverse** of a modulo n. If a and n are not relatively prime, then a does **not** have an inverse modulo n.

Moral: A number a has an inverse modulo n if and only if a and n are relatively prime.

Example: Does 9 have an inverse modulo 6?

Example: Which numbers are invertible mod 15? What are their inverses? (Here we will be working "on the clock."

How can we find the inverse if the numbers are bigger?

Example: Find the inverse of 34 modulo 49. Using the Euclidean Algorithm / Bezout's Theorem, we get:

$$13 \cdot 34 - 9 \cdot 49 = 1$$

How does this help us solve $34x = 1 \bmod 49$?

How does this help us solve $34x = 5 \bmod 49$?

In general: To solve $ax \equiv b \mod n$ (in the case a and n are relatively prime.
Step 1: Use Euclidean Algorithm to find an inverse of $a \bmod n$.

Step 2: This number will be a solution to $ax \equiv 1 \bmod n$.

Step 3: Take your solution and multiply by b to get a solution to $ax \equiv b \bmod n$.

Example: Imagine you are trying to solve

$$26x = 3 \bmod 41.$$

You use the Euclidean algorithm on what numbers?

And work out that:

$$(41)(7) - (11)(26) = 1$$

What is the inverse of 26 mod 41?

What is the solution to the original equation?

Moral: Be careful with negatives. (But don't be afraid of negatives - sometimes they make things easier)

Example: What is the inverse of 443 modulo 444?

Practice questions about inverses:

1. To solve the equation $7x \equiv 3 \bmod 41$ we would
   (a) multiply both sides by the inverse of 3 (mod 41)
   (b) multiply both sides by the inverse of 7 (mod 41)
   (c) multiply both sides by the inverse of 41 (mod 41)

2. A number times its inverse is always equal to _____.

3. You are given that $76 \cdot 4 \equiv 1 \bmod 101$. Use this information to solve the equation:

$$76x \equiv 5 \bmod 101.$$

4. You are given that $(1213)(-5) + (2022)(3) = 1$. Use this information to solve the equation:

$$1213x \equiv 2 \bmod 2022.$$

   Write your answer as a number in the range from 0 to 2021.

The numbers below represent all the "nonzero" numbers mod 13. Let's explore what happens when we take these numbers and

Remember: We're working mod 13

multiply them all by 2.

1

2

3

4

5

6

7

8

9

10

11

12

multiply them all by 4

1

2

3

4

5

6

7

8

9

10

11

12

multiply them all by 3

1

2

3

4

5

6

7

8

9

10

11

12

multiply them all by _____

1

2

3

4

5

6

7

8

9

10

11

12

A discussion on Exponents: Consider the following equations mod 5. Which are correct simplifications using modular arithmetic?

$12 + 21 \equiv 2 + 1 \bmod 5$ (when working mod 5 we can simplify the numbers we are adding mod 5)

$12 \cdot 21 \equiv 2 \cdot 1 \bmod 5$ (when working mod 5 we can simplify the numbers we are multiplying mod 5)

$12^{1000} \equiv 2^{1000} \bmod 5$ (when working mod 5 we can simplify the base of an exponential mod 5)

$2^{12} \equiv 2^2 \bmod 5$ (when working mod 5 we can simplify the base of an exponential mod 5)

We need to be careful when simplifying exponents. Luckily - there's a great little theorem that comes to the rescue

Fermat's Little Theorem:
Let p be a prime number and suppose that a is any integer that is not divisible by p. Then

$$a^{p-1} \equiv 1 \bmod p.$$

Moral: This helps us simplify exponents if we are working mod p (for a prime number p)

Examples:

Simplify $7^{222} \bmod 11$

Find $23^{1002} \bmod 41$

Euler's Theorem Let n be a positive integer, and suppose that a is an integer with $\gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \bmod 1.$$

We will not prove Euler's Theorem, but let's verify what it says when n is prime.

Examples

Explain why we CANNOT apply Euler's Thoerem to calculate: $3^{103} \bmod 15$.

Use Euler's Theorem to simplify $3^{2022} \bmod 35$.

What is $4^{98} \bmod 27$?

Problems about Modular Inverses, Fermat's Little Theorem and Euler's Theorem

Tools: I recommend this website for doing modular arithmetic. Make sure you change the calculator from Standard to Modular.
`https://www.boxentriq.com/code-breaking/big-number-calculator`
You can use this tool to double check most of this homework.
Another helpful tool is `https://www.dcode.fr/bezout-identity` which will give you Bezout coefficients.

1. Using the Euclidean algorithm, a student discovers that

$$(5)(37) - (8)(23) = 1$$

   Use this information to find:

   (a) the inverse of 23 mod 37. Check your answer by multiplying 23 by your inverse and checking that it equals 1 mod 37.

   (b) the inverse of 37 mod 23. Check your answer as in part a.

   (c) Use your answers above to find solutions to the equations

$$23x = 7 \bmod 37$$

$$23x = 3 \bmod 37$$

$$37x = 8 \bmod 23$$

2. Which of the following equations have no solution? Explain why? For those that do have a solution, find all solution "on the clock." Then find more equivalent solutions in $\mathbf{Z}$.

$$3x = 6 \bmod 7$$

$$5x = 4 \bmod 13$$

$$-5x = 4 \bmod 10$$

$$5x = 8 \bmod 15$$

3. Suppose you are working mod n and discover that $xyz = 1$. Which of the following would be a the inverse of x? Which would be the inverse of z?

   (a) y

   (b) z

   (c) yz

   (d) xyz

   (e) xy

   (f) 1

4. Suppose you are working mod n and discover that $x^4 = 1$. Which of the following would be a the inverse of x?

   (a) x

   (b) x^2

   (c) x^3

   (d) x^4

5. You can use the online calculator here: `https://www.dcode.fr/bezout-identity`. The purpose of this exercise is to help give you practice reading from the Bezout identity to get the inverse.

   Solve the following equations:

   (a) $19x \equiv 4 \bmod 141$

   (b) $55x \equiv 34 \bmod 89$

   (c) $89x \equiv 2 \bmod 232$

6. Suppose n is some positive integer and modulo n and you discover that 8 and 10 are inverses. Use this information to answer the following questions:

   (a) What is the inverse of 10? (Hint: don't overthink this one)

   (b) What is the inverse of 5 (Hint: If you know $8 \cdot 10 = 1$, can you figure out what the inverse of 5 can be from this?

   (c) Solve the equation $8x \equiv 3 \bmod n$ by multiplying both sides by the inverse of 8.

   (d) Solve the equation $4x \equiv 6 \bmod n$ by multiplying both sides by the inverse of 4.

7. Suppose that you are given that $37a - 7b = 1$, for integers a, b. Use this information to find the inverse of b mod 37. Your answer must be in the range $\{0, 1, \ldots, 36\}$, so you may need to do some simplification first.

8. Reality check: If $b \equiv 0 \bmod n$ then this means that

   b is [a multiple of n / a factor of n] (circle the correct one)

9. Use Fermat's Little Theorem to find the following **without** using a calculator. You can check these online with a modular arithmetic calculator, e.g.

   (a) $7^{121} \bmod 13$.

   (b) $8^{1002} \bmod 41$.

   (c) $3^{302} \bmod 5$

   (d) $3^{302} \bmod 7$

   (e) $3^{302} \bmod 11$

   (f) $5^{2003} \bmod 7$

10. Use Euler's Theorem to calculate the following without using a calculator:

    (a) $7^{121} \bmod 6$.

    (b) $3^{1002} \bmod 10$.

    (c) $5^{302} \bmod 12$

    (d) $3^{302} \bmod 8$

    (e) $3^{302} \bmod 25$

11. Explain why Euler's Theorem doesn't apply when calculating $8^{2022} \bmod 12$.

Quick Quiz on Modular Arithmetic

1. Which is congruent to 35 mod 8?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8$$

2. Which is congruent to $(10)(-2)$ mod 6?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5$$

3. Which is congruent to $(37)(15) \mod 7$

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6$$

4. Which is congruent to $(12)^9(14)^9$ mod 13?

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad 10, \quad 11, \quad 12$$

5. What is 5742991423 modulo 100?

6. A student is working mod 8 and needs to simplify the expression:

$$37x + 2 \text{ where } x \text{ is an integer}$$

which of the following would be a correct simplification mod 8?

(a) $3x + 2$

(b) $4x + 2$

(c) $5x + 2$

(d) $6x + 2$

Quick Quiz Makeup on Modular Arithmetic

1. Which of the following is 0 mod 9?

$$34, 35, 36, 37, 38, 39$$

2. Which of the following is -3 mod 8?

$$79, 80, 81, 82, 83, 84, 85, 86, 87, 88$$

3. Write down three positive numbers that are congruent to -8 mod 20.

Quiz on Number Theory Name: _____

1. Without a calculator, calculate $(999)^2 \bmod 1004$. (Hint: You can do this using negative numbers on the clock)

2. Below are the prime factorizations of two numbers a and b.

$$a = 2^3 \cdot 3^6 \cdot 7^5$$

$$b = 2^4 \cdot 3^2 \cdot 5^2$$

What is the prime factorization of ab?

What is $\gcd(a, b)$? Leave your answer factored.

Are a and b relatively prime? Yes / No

What is $\phi(ab)$? (You do not need to multiply anything out - I want you to use the formula from class, which is at the bottom of this page:

Theorem Let n be a positive integer, and suppose that the prime factorization of n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

3. Write down all integers $1 \leq n \leq 15$ that are relatively prime to 15. Use your answer to say what $\phi(15)$ is.

   Numbers that are relatively prime to 15: _____

   $\phi(15) =$ _____.

4. A student uses the Extended Euclidean Algorithm / Bezout's Theorem to find $\gcd(47, 83)$ and determines that the gcd is 1, and is able to write 1 as a "linear combination" of 47 and 83:

$$(47)(-30) + (17)(83) = 1$$

   If you look at this equation "mod 17" then one of the following becomes 0. Which one?

$$(47)(-30), \qquad (17)(83), \qquad 1$$

5. Suppose that p and q are distinct primes greater than 3. Using the formula for $\phi(n)$ from the front page in class, what is $\phi(9pq^2)$? (Leave it factored. You don't need to multiply this out).

1 Encryption

Today we are going to practice encrypting and decrypting. I recommend this calculator: `https://www.boxentriq.com/code-breaking/big-number-calculator` (Remember to switch to the "modular" setting.)

For simplicity, I've made a table to help us translate from letters to numbers. Note that we'll start with 01 instead of 00 so that the counting is more natural.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
T	U	V	W	X	Y	Z	space	1	2	3	4	5	6	7	8	9	0	!

With whatever encryption method we use, we will be working modulo some number, and so it's important that we can convert back to our letters. Working with modular arithmetic will

- Speed up computations
- Allow us to have secure methods
- The downside is that we work e.g. mod 100 there are lots of equivalent numbers. E.g.

$$23 \equiv 120123 \equiv 201523$$

Which "word" do we want?

Fix: If we work modulo say a 7 digit number like $n = 1021133$ then if we agree to "reduce to a number on the clock between 0 and $n - 1$, then we would always be able to recover the message.

This means in this case we can encode words up to _____ letters long.

Example: Suppose you get a message and discover that $M \equiv 191625 \bmod n$. Since we've reduced our number into the appropriate range, we can now see the word must be:
Example: Someone sends you a message M that is broken into two pieces:

$$12716 - break - 122119$$

What is the message?

Notice: You have to be careful to encrypt / decrypt the first letter if there is a leading 0.

1. Write down what MATHS! becomes when split into two blocks of three and indicate the blocks by placing a dash between them.

2. What word would 51409-71301 become?

So far we haven't done ANY encryption or decryption - our messages are just lying there out in the open!

The idea of encryption is to take a message M (a number) and then "encrypt it" in such a way to get an encoded message C. Some properties that you'd like to have are:

- You don't want your "enemies" to be able to decrypt C if they intercept it. (Imagine someone listening to your modem as you send your encrypted credit card numbers to Amazon.com - they can intercept the encrypted number relatively easily. But hopefully it's VERY hard for them to decrypt the message and get your actual credit card number.)
- You want it to be possible and easy for your friends to decrypt your message. (Once Amazon gets your encrypted message, Amazon needs to be able to determine what your actual credit card number is.)
- (Public Key Encryption) Since often we want to share information with people who are far away, it is often necessary that the encryption instructions themselves are going to be shared over a noisy connection, something like:

  Bob: Message coming

  Alice: Oh ok, make sure you encrypt it by doing this....

  Bob: Ok I encrypted it, here's my encrypted "ciphertext" C

  Alice: Ok, I'll decode it and see what your original message M was.

Example of some messages that are easy-ish to break. Let's crack the code!

You overhear the following exchange:

Bob: Message coming

Alice: Ok, take your message M and encrypt it by doing $C = M + 12 \bmod 1021133$

Bob: Ok, I did it. Here's the encrypted message $C = 250531$.

What was Bob's original message M?

Is Alice's encryption method easy for Bob to encrypt a message? [Yes / No]

Do you think Alice's encryption method is very strong - how hard is it to decode messages sent with this scheme? What if the numbers were bigger? Would that make it any stronger?

E.g. if Alice said "do $C = M + 762375327632 \bmod 8712786237645762$.

Could you still decrypt a message you intercepted?

Example of a slightly more complicated Encryption Method

You overhear the following exchange:

Bob: Message coming

Alice: Ok, take your message M and encrypt it by doing $C = 3356M + 12 \bmod 1021133$

Bob: Ok, I did it. Here's the encrypted message $C = 1011698$.

What was Bob's original message M?

Is Alice's encryption method easy for Bob to encrypt a message? [Yes / No]

Do you think Alice's encryption method is very strong - how hard is it to decode messages sent with this scheme? What if the numbers were bigger? Would that make it any stronger? E.g

$$C = 237462837M + 2347862356723 \bmod 2389742835767132461$$

Another Encryption Method

You overhear the following exchange:

Bob: Message coming

Alice: Ok, take your message M and encrypt it by doing $C = M^{7151} \bmod 1021133$

Bob: Ok, I did it. Here's the encrypted message $C = 926124$.

What was Bob's original message M?

Do you think Alice's encryption method is very strong? What if the numbers were bigger?

Encryption Project

This project will be worth 5% of your final exam score.

Using the RSA encryption method we learned in class, I want you to practice sending and receiving messages.

- For this problem everyone has their own values of N, e, M and can be found here:

  `https://docs.google.com/spreadsheets/d/1ucWNKVT1OnibpLebco_2hb4v-pxM7prrt2twKl37VNk/edit?usp=sharing`

- Notice there are three tabs, including extra credit.
- Part 1: Decode a secret message that I have sent to you. Please email me your decoded word, including a short summary of the steps that you took. I want you to explain in words your process. So I want you to say something like "I factored .... and then I found .... using this calculator... I did this and then ...." (please don't write down any of the large numbers, I'm just looking for a brief summary of the steps you took.)
- Part 2: Encode a secret message and send it to me by email. See instructions on this tab. You will be sending me a very large number. I will confirm that it decodes correctly as a common English word.
- Please send your answers to the encryption and decryption as **separate emails, no later than May 18th at 11:59pm.**
- Some helpful links: A site for calculating with big numbers
  `https://www.boxentriq.com/code-breaking/big-number-calculator`

  Some python code I wrote to convert letters to numbers
  `https://trinket.io/python/6a71c9333d`

- (Extra Credit) There are some bonus messages in the Extra Credit tab. The numbers are huge - but maybe you can decrypt them... Hmm. I wonder. (Only attempt this if you're looking for a fun challenge!)

2 Mini Projects

Overview: Throughout the semester there will be several mini-projects that you will complete to get a deeper understanding of the material. In this project, you'll get more practice with quantifiers.

Due Dates: You will be required to complete 4 of these mini projects this semester. I will be flexible with the deadlines, but here the are rules:

- You must submit your first one before spring break (this is designed to get you started on the projects)
- You can only submit one mini-project each week of the semester. (This is designed so that you don't wait until the end of the semester, to do the projects, and also so that I will get a reasonable number of projects each week and so I can grade the projects and give them back to you with feedback.)
- Otherwise I will let you work at your own pace.
- A week starts Sunday at 12:00am and ends Saturday at 11:59pm
- Finals week is included for the mini-projects

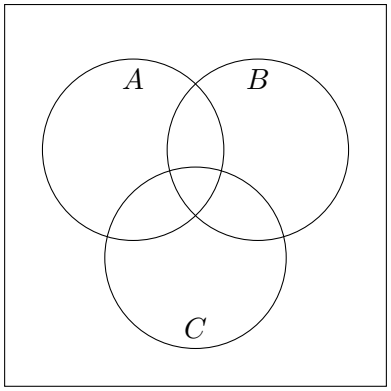
One of my big goals in this class is that we learn to struggle with challenges and push our understanding. I'm happy to help you work on this project in office hours. You are also allowed to work on this project with your peers, but I ask that you write up your solution on your own, in your own words. **You are not allowed to post any part of this project on the internet or seek help from tutors or any websites.** If you are stuck, just let me know.

Contents

1 Understanding Quantifiers

Quantifiers are important because they allow us to make precise mathematical statements. You'll get more and more comfortable with them as the semester progresses. In this mini-project you are going to explore some properties and then determine whether or not certain sets have these properties.

Instructions: Below are 3 properties that a set of real numbers can have, and then 4 sets. Your goal is to **think about which sets have which property**. To help you, you might want to think about the Venn Diagram below. Where would each set go? Does it have property A? property B?



Do I have to do all 4 sets and all 3 properties?

- No - the goal is for you to deeply understand what these properties are saying, and so I am only requiring you to pick two sets and decide whether they satisfy properties A, B, C. (Of course you can do all 4 if you like!)
- So you only have to pick 2 sets, but you need to discuss all three properties for each set.
- In your writeup I want you to explain why the sets you have chosen have or do not have each property.

I will be looking for clear writing that convinces me that you have a solid understanding of the properties and the sets. You do not have to type up your solutions, but you might find that it is easier to type than to write on paper (especially as you begin editing your work). Google drive has an equation editor (just click help and type "equation" and it will activate).

(continued on next page)

The properties:

Note: These properties use the symbol $\in$ which means "in". For instance, the sentence $x \in X$ means "x is in the set X" and $x \in \mathbb{N}$ means "x is in the set of positive integers" i.e. "x is a positive integer."

A) We say that a set X of real numbers has property A if

$$\forall x \in X \ \exists y \in X \ : \ y > x$$

B) We say that a set X of real numbers has property B if

$$\forall x \in \mathbb{N} \ \exists y \in X \ : \ y > x$$

C) We say that a set X of real numbers has property C if

$$\exists y \in \mathbb{N} \ \forall x \in X \ : \ y \leq x$$

The sets:

The open interval $(-\infty, 5)$,

The set of integers $\mathbf{Z}$,

The set of natural numbers $\mathbb{N}$ (i.e. positive integers),

The closed interval $[4, 5]$.

As an example: I will describe how I might write about a hypothetical property D) and some sample sets:

Suppose that a set has property D if:

$$\forall x \in X \ \exists y \in X \ : y > x + 7.$$

1) I will first explain why the open interval $(0, 10)$ does NOT have property D. Property D says that for any x that I choose in X, I should be able to find another y (also in my set X) but with $y > x + 7$. If I choose $x = 9$ then there's no way I can choose a y bigger than $9 + 7$ (which is 15) since my set X only goes up to 10.

A similar argument shows that the intervals $[0, 30]$ and $(-\infty, 100)$ also do NOT have property D. (Since, I could take e.g. $x = 29$ in the first example and $x = 99$ in the second).

For my last two sets, $\mathbb{N}$ and $\mathbf{Z}$ I claim that these DO have property D. Let's see why. No matter what I choose for my x, I will always be able to find a y bigger than $x + 7$ since I have infinitely large numbers to choose from. In case you want me to be more explicit, I could just take $y = x + 100$ which is definitely bigger than $x + 7$ and importantly, if x is in $\mathbb{N}$ then $x + 100$ is still in $\mathbb{N}$ as well. (Ditto for $\mathbf{Z}$).

What do you think - did I convince you?

(end of mini-project)

2 A Proof that $\sqrt{3}$ is irrational.

In this proof you will prove that the $\sqrt{3}$ is irrational. Please read the following carefully and complete the instructions inside of the boxes.

Lemma 1: If n is an integer, then there are only three possibilities for n:

Type 1: $n = 3k$ for some integer k;

Type 2: $n = 3k + 1$ for some integer k;

Type 3: $n = 3k + 2$ for some integer k;

You do NOT need to prove this statement, but it will be useful to prove Lemma 2. Instead, verify it by checking that it is true for the following values of n, and sort them into the three Types:

$$3, 17, -5, -10, 6, 7, 8$$

For each of these numbers, square them and see what Type each number would be in. For instance, 4 is of Type 2 and $4^2 = 16$ is of type 2 as well. Now write a proof of the following statement:

Statement: If n is an integer of Type 3, then n^2 will be of Type 2.

Lemma 2: Let n be an integer. If $3 \mid n^2$ then $3 \mid n$.

Prove Lemma 2 using the cases from Lemma 1.

You will likely be most successful if you use proof by contrapositive.

Think carefully about what the negation of $3|n$ would be in the context of the cases occurring in Lemma 1.

Theorem 3: The square root of 3 is irrational, that is, there is no rational solution to the equation $x^2 = 3$.

Prove Theorem 3 by proof by contradiction.

As always, please write your proofs carefully, neatly and clearly present your work. You are highly encouraged to type your projects, perhaps using Google docs, which has an equation editor.

(end of mini-project)

3 Sometimes / Always / Never

Below are some properties that might be true sometimes, always or never, depending on what the sets A and B are. Your job is to determine which is which.

- In all of these A and B are assumed to be finite nonempty sets.
- Recall that the **powerset** of a set X consists of all subsets of X including the set itself and the empty set.
- For each of the questions below I want you to say whether it is sometimes / always / never true.
- If it is always true, I want you to explain why giving a rough proof. (I will be looking for a solid explanation here).
- If it is sometimes true, then I will be looking for **two** things. First an example when it IS true, and second an example when it is not true. What do I mean by "example" well in this case an example would be a pair of sets A and B. So you might say something like:

  "Example 1: If $A = \{2, 3\}$ and $B = \{3, 4\}$ then.... and Example 2: If $A = \{...\}$ and $B = \{...\}$ then..."
- If it is never true, then you should give a reason for this. It will not be sufficient to just give one example.

Question 1:

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)?$$

Question 2:

$$\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)?$$

Question 3:

$$\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)?$$

Question 4:

$$\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)?$$

4 Explaining the Towers of Hanoi

In class you played around with the famous problem: The Towers of Hanoi. In this project, what I would like you to do is explain what you discovered about this problem by preparing a small report about the problem. I will keep things fairly open ended, but here are the main items I will be looking for.

1. I want you to first explain the setup of the problem. What is it we are measuring? In your own words explain what we are looking for. Your goal should be to define the sequence M_n clearly for the reader. You might want to include pictures you can find of this game online.

2. I want you to explain the idea of **recursion** and finding a pattern. Describe what happens in small cases, and include a table of numbers like you did in class.

3. Give your **conjectured recurrence formula**. This is something that is **suggested by the data, but not yet confirmed.**

4. Explain in words **why** this recurrence formula is true in terms of the disks and the towers. (This is the most important - I will want to see that you really understand why this recurrence holds - put this in your own words.)

   Additional Things to Include

   The above are all things I think most groups talked about in their discussions, but here are a few additional problems:

5. Please answer the question given on the Ch. 7 worksheet about "how long until the world ends."

6. In class we will prove that a closed form expression for M_n is $2^n - 1$. Show that this explicit formula satisfies your recursive formula from above.

7. The smallest disk moves a lot more than any of the others. Explore how many steps the smallest disk moves in each case. Let S_n denote how many times the smallest disk must move if there are n disks. Conjecture a recursive formula for S_n and then explain why it is correct. (Again I'm looking for a recursive explanation that relates S_n to S_{n-1} and **why.**

5 Christmas in July

This mini-project expands on the work you did in HW7. Let's start with a true story involving the USD Pool during July 2021. Your professor was swimming laps one day, a very tedious activity. To prevent boredom, he was doing what some people call "pyramids", where he would swim 1 lap, then 2, then 3, then 4, etc. In your homework you learned that the total number of laps swam after such an athletic endeavor is called a Triangular Number, and for instance in the previous sentence he would have swum $T_4 = 10$ laps. You also learned that for $n \geq 1$,

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

Your professor was pondering these equations while swimming (so much for not being bored!) and noticed that if he added T_3 and T_4 he got a perfect square (in this case 16). And this worked for any two consecutive values of T_n. For instance, $T_2 + T_3 = 9$ and $T_5 + T_4 = 25$.

1. Formulate this statement more generally and write down a statement that captures the general case. Your statement should involve two consecutive terms, and one of those terms should be T_n. The right-hand side of your equation should involve n. State for what values of n your statement is true. Is it true for $n \geq 1$? for $n \geq 0$?

2. Prove this statement in two different ways. First, use the algebraic formula for T_n above to simplify the left hand side and show it is equal to the right hand side.

3. Second prove it by drawing a picture. Your picture should use the "triangular" property of these numbers. I want to see a carefully drawn and labeled picture that shows how "triangles" combine to give a "square". (Imagine your professor's joy at thinking about this picture while swimming laps.)

Now we are going to USE this formula to solve the 12 days of Christmas problem. Remember that on the nth Day of Christmas, T_n gifts are given, and so at the end of the 12 days, there are a total of

$$T_1 + T_2 + \cdots + T_{12}$$

gifts given. Using your results from above, how can you simplify this sum of 12 terms. (Hint: it should simplify down to a sum of 6 terms). Now add up these 6 numbers with a calculator and confirm your result with what you got on HW7.

Finally, I want you to derive a formula for the total number of gifts given on the first $2n$ days of Christmas:

$$C_n = T_1 + T_2 + \cdots + T_{2n-1} + T_{2n}.$$

I want you to use the same method you used above, combining some of the triangular numbers into square numbers.

1) See if you can factor a common factor out of each term.

2) You may use one of the formulas in Project 7 "Some Sums" without proof (you'll be proving that formula there).

You should check that your formula gives the same answer you got in the case of 12 days.

6 Understanding sets and functions:

In this mini-project you will continue to practice your understanding of reading and parsing mathematical statements, but this time it will involve some functions, sets and equivalence relations.

Throughout all of these problems X will be the set consisting of the five sets below:

- The set L consisting of letters in your first name, e.g. my set would be $\{a, d, m\}$.
- The set $M = \{1, 2, 3, 4, 5\}$
- The set $X = \{9\}$
- The set $Y = \mathbb{N}$
- The set $Z = \mathbf{Z}$

You are going to draw 4 **directed graphs.** All graphs will have the same set of **vertices:** L, M, X, Y, Z. I recommend you draw these spaced apart, maybe like a pentagon.

Graph 1: Draw an arrow (directed edge) from vertex A to vertex B if $\exists f : A \to B$, f is injective.

Graph 2: Draw an arrow (directed edge) from vertex A to vertex B if $\forall f : A \to B$, f is injective.

Graph 3: Draw an arrow (directed edge) from vertex A to vertex B if $\exists f : A \to B$, f is surjective.

Graph 4: Draw an arrow (directed edge) from vertex A to vertex B if $\forall f : A \to B$, f is surjective.

For each graph, write a short explanation that captures the salient features of it. For instance, can you explain why you drew in some of the arrows (you don't have to explain everything, but as a rule of thumb, you should explain why you have drawn in some arrows and also why you haven't drawn other arrows. This question is mostly designed to help give you practice thinking about quantifiers, and functions.

7 Some Sums

One of the first proofs that we ever do with induction is the famous sum:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{7.1}$$

There are similar formulas for the sum of higher powers as well. Here are the next few:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{7.2}$$

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}. \tag{7.3}$$

Can you guess what comes next? Probably not - although there is a general pattern, it is quite complicated, but the subject of a beautiful story, [‖] In this project I want to show you a way to inductively get the next one of these formulas from the previous one: Recursion!

Part 1: Warmup

As a warmup, prove, using mathematical induction that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We are going to USE this formula along with equation 7.1 to prove equation 7.3.

Part 2: Gathering Evidence

Notice that if we multiply out the expression $(n+1)^4 - n^4$, we obtain this fairly innocuous looking expression:

$$(n+1)^4 - n^4 = 4n^3 + 6n^2 + 4n + 1.$$

To see what this is saying, I want you to write out the this equation 5 times, starting with $n = 0$ and ending with $n = 4$. Write the equations clearly in a line and line up the corresponding terms. Now, I want you to add up these 5 equations and carefully see what you get on the left hand side. You should have a very simple left hand side; your right hand side should involve sums of powers of n, including some that we have proven, like 7.1 and 7.3, and the sum of cubes that we want to study.

Part 3: Putting it all together

Now, rather than just writing the equation 5 times, what would happen if you wrote it n times. What would you get? Now use this expression and some algebra to derive the formula 7.3.

Part 4: Onwards!

Now, explain how you could extend this to the next case and derive a formula for

$$1^4 + 2^4 + 3^4 + \cdots + n^4.$$

Check your answer with the webpage listed in the footnote, and simplify your answer to match their form.

[‖] see e.g. `https://en.wikipedia.org/wiki/Faulhaber%27s_formula`.

8 So you think you can factor?

As of March 9, 2022 the largest known prime number is:

$$2^{82,589,933} - 1.$$

This is an example of what's called a Mersenne prime, which is a prime of the form $2^n - 1$. In this project you will explore some of the properties of Mersenne Primes.

Part 1: Are they all prime?

Important: Please do this part of the project before reading further. You will be making a conjecture. It's ok if it's not correct, but try your best and write your evidence down clearly.

Do some experiments with numbers of the form $2^n - 1$. Start with $n = 1$ and see if these numbers appear to be sometimes / always / never prime. What values of n (the exponent) seem to give you prime numbers. You can look online for some online prime testing websites. Hint: Make sure you look carefully at $n = 11$.

Write down a conjecture based off of your experiments. What do you think is true? You may want to have multiple parts: If n is prime, do you think $2^n - 1$ is sometimes/always prime? If n is composite?

Part 2: A Warmup with some algebra

Throughout this project you will need to use the following algebra fact:

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a^2 + a + 1). \tag{8.1}$$

As a warmup, explain what is going on in the following:

$$x^6 - 1 = ((x^2)^3 - 1) = (x^2 - 1)((x^2)^2 + (x^2) + 1).$$

I want you to explicitly explain what I have done with each equals sign, and if I used the formula (0.1) then explain what my value of n was and what my value of a was. You will need to understand this step deeply to continue so make sure you are ok with this.

Part 3: The Conclusion

Prove the following lemmas. You will need the factorization formula above:

Lemma 1: Let x, n be positive integers. If $x \geq 3$ and $n \geq 2$ then $x^n - 1$ is NEVER prime.

Now using Lemma 1, explain why can conclude Lemma 2. (In other words you should be able to prove Lemma 2 in one or two sentences by using Lemma 1)

Lemma 2: If x, n are positive integers with $n \geq 2$ and $x^n - 1$ is prime, then $x = 2$.

Lemma 3: If n is composite, say $n = \ell k$ then $2^n - 1$ is not prime.

Now explain how your work above allows you to conclude the following:

Theorem If $n \geq 2$ and $x^n - 1$ is prime then actually $x = 2$ and n must be a prime number. So the only primes of the form $x^n - 1$ are actually of the form $2^p - 1$ where p is prime.

9 A Challenging Proof by Induction: Oral Presentation

In this project I will give you a fun and challenging problem to think about. Instead of writing out your solution, for this project you will present your solution to me in office hours. To do so, please send me an email with your possible times (you may also include some times outside of office hours.) Please email me at least 4 days in advance. I will be looking for you to present your **proof by induction** clearly and carefully. If there are any gaps in your proof, you can come back the following week at "resubmit" your presentation. This oral presentation (and any resubmissions) will count as the "one per week" limit for mini-projects. Full disclaimer - this problem is very challenging, but also very rewarding. I think that once you understand how this proof works you will better appreciate mathematical induction.

The Problem:

Let $n \geq 1$ be a natural number. Let $S = \{1, 2, 3, \ldots, 2n\}$ be the set of the first $2n$ integers. Now let A be a subset of S of cardinality $n+1$. (As it turns out - there are lots of subsets of this size! For instance if $n = 10$ then there are over $160,000$ different possibilities for A) but no matter which of these subsets you choose, you are guaranteed that within the set A, there will be two elements where one divides the other. In other words, A **must** contain an element that is a multiple of another.

Step 1: Play around with this problem. Can you see why it is true for small cases of n? Start with $n = 1$ then $n = 2$. What do you think? Write down some of your early ideas - I'll ask about these during your presentation. Do you have any ideas about how to solve this more generally? Warning - this is a challenging problem!

Step 2: Here are some hints to help coach you through a proof by induction. We will be using strong induction here, including a very clever trick. In Step 1, you will have proven the base case. And so now suppose the induction hypothesis, assuming you have solved the problem for $k = 1, 3, \ldots, n$:

Induction Hypothesis:
P_k: Any subset of size $k+1$ of $\{1, 2, \ldots, 2k\}$ will have one element that divides another.
Assume $P_1, P_2, \ldots, P_n$ are true.
Goal: Show that P_{n+1} is true.

You will now start to show the inductive step by taking the set $S = \{1, 2, \ldots, 2n, 2n+1, 2n+2\}$ (why?) and a subset A consisting of $n+2$ elements. (why $n+2$?). Now you need to complete the proof.

Hints: (more available if you ask)

1. What if all of the elements of A were in $\{1, 2, \ldots, 2n\}$ What would the induction hypothesis say? Explain why you would be done.
2. What if only $n+1$ of the elements of A were in $\{1, 2, \ldots, 2n\}$? Would you be done then?
3. So if neither of these are true, what elements must be in your set A? (Hint: you should have two ...)

   continuing in this case:
4. So now how many elements do you have in $A \cap \{1, 2, \ldots, 2n\}$. Will the induction hypothesis apply to this set? (no)
5. Explain why if $n+1$ were in A you would be done.
6. Now if $n+1$ is not in A, what happens if you consider the set $A \cup \{n+1\}$? Can you apply the induction hypothesis to this set? What does this mean?
7. How does your proof finish up?

10 Sorting out the Primes

There are infinitely many primes! Let's review the proof that we saw in class (or will see, depending on when you read this!) In this proof we will use the fact that every positive integer greater than 1 has a prime factor.

Theorem: There are infinitely many primes.

Proof. We will argue by contradiction. Suppose that there were only finitely many primes. We will hope for a contradiction. Let's call them $P_1, P_2, P_3, \ldots, P_n$. In other words our list is $2, 3, 5, 7, \ldots, P_n$ and EVERY prime number is somewhere on this list. So now consider the number

$$m = P_1 \cdot P_2 \cdots P_n + 1.$$

Now, if you look at the expression for m, m is NOT divisible by P_i for any i, since if we divide m by any P_i we will always have a remainder of 1. This is a contradiction, since EVERY number greater than 1 must be divisible by some prime. We have found a contradiction, so our proof is complete. □

Ok, so there are infinitely many primes - but what can we say about them? Are they all even? all odd? Oh wait that's an easy one - the only even number that is prime is 2, and so there are infinitely many odd prime numbers.

If you think about it this way, if we made two buckets:

$$\text{even primes}, \qquad \text{odd primes}$$

Then one bucket would have 1 element, and the other would have infinitely many.

Let's keep splitting them up. Let's look at the odd primes: $\{3, 5, 7, 11, 13, \ldots\}$. Since these numbers are odd, when we divide them by 4 they will leave a remainder of 1 or 3. (Explain why remainders 0 and 2 are not possible.) In other words, all of these primes must either be of the form $4k + 1$ or $4k + 3$ for some integer k.

Let's make two buckets now for our odd primes:

$$\{\text{primes of the form } 4k + 1\}, \qquad \{\text{primes of the form } 4k + 3\}$$

Step 1: Find a list of the first 30 odd primes and one by one (in order, starting with 3) place them into these two buckets. As you do this, I want you to record how many are in each bucket at each step. For instance, at the first step, I would have 3 in bucket 2, so I would record that as $0, 1$ since nothing is in bucket 1 and there is one number in bucket 2. After putting in the first 5 odd primes, 3,5,7,11,13, I would have $2, 3$ since $5, 13$ would wind up in bucket 1 and $3, 7, 11$ in bucket 2. You may want to write up your results for this in a computer spreadsheet and link to it in your project. This part of the project should have 30 lines.

Questions: What do you notice about your list? What conjectures might you make based on your evidence? Write down a short paragraph based on what you notice and what you wonder.

Step 2: Every odd number is either of the form $4k + 1$ or $4k + 3$ for an integer k. Let's call these buckets: "Type 1" and "Type 3". For example, 15 is Type 3 and 25 is Type 1.

If we multiply odd numbers together we will obtain another odd number. Complete the multiplications below. (You don't need to prove these, as we will do this in class with modular arithmetic)

(Type 1)(Type 1) = [Type 1/Type 3]

(Type 1)(Type 3) = [Type 1/Type 3]

(Type 3)(Type 3) = [Type 1/Type 3]

Question: So if you start with a number of Type 3 (in other words looking at the right hand side), what can you say about its factors? What if you start with a Type 1 number? (These answers should be different). Your answers to this question will be very useful in Step 3. Try to write sentences like: "The only factors possible are blah." or "It is possible that the factors could be blah or blah, but we can't know for certain which one."

Step 3: You should have found a healthy supply of primes in both buckets. It turns out that there are indeed infinitely many primes in each bucket. In this step you will prove that there are infinitely many primes in the set {primes of the form $4k+3$}, the Type 3 primes. Do this by adapting the proof by contradiction above. Here are some hints:

- As a guide, I want you to consider a number $m = 4P_1 \cdots P_n + 3$. But I want you to decide what the P_i's will be. Do you want to include all the Type 3 primes? Some of them? Do you want to include the Type 1 primes as well?
- Is your number m Type 1 or Type 3?
- Is there any prime in your bucket that can divide into m? Why or why not? (Be careful - is 3 in your bucket? You might want to revise your bucket!)
- You should use your answer to the Question in Step 2 to make a conclusion. Write this step carefully.

Epilogue:

It is actually true that there are infinitely many primes of Type 1 as well. However, if you try to adapt the proof that you wrote in Step 3, you will not succeed, because unfortunately the number

$$4P_1 \cdots P_n + 1$$

will be of Type 1, and as you saw in Step 2, this number might only have factors from the other bucket. And so we won't get a contradiction. The simplest proofs I know that there are infinitely many primes of Type 1 involve some more advanced number theory (a course we are offering next year!) If you are interested, let me know - I could help design a custom mini-project about this if you want. Or we could continue reading about this after the semester ends.

Bonus Epilogue!

You know there are lots of buckets in the world. For instance, we could look at all the odd primes when we divide by 6 and we would see that every prime is gonna be of the form: $6k+1$ or $6k+3$ or $6k+5$. It turns out that all three of these buckets will have infinitely many primes. In fact, there given any "bucket" of the form $Ak+B$ where A and B are relatively prime, there will be infinitely many primes in that bucket. So e.g. there are infinitely many primes of the form: $12n+7$ and here they are:

$$\{7, 19, 31, 43, 67, 79, 103, 127, 139, 151, \ldots\}.$$

You can read more about this here:

`https://en.wikipedia.org/wiki/Dirichlet%27s_theorem_on_arithmetic_progressions`

11 Problems on Chessboards

A chessboard is an 8 by 8 grid of squares, although more generally we might want to play games on a board that is of a different size. In this project we are going to think about what we can do placing pieces on this chess board.

Part 1) The Non-Attacking Queens: In the game of chess, a queen can move in any of the 8 directions - up/down/left/right and in any of the 4 diagonal directions - and they can go any amount of distance. For instance a queen could attack a piece in the same row or same column or same diagonal on the board.

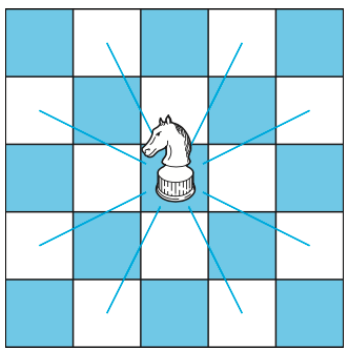
In this project I want you to consider the following question:

"Is it possible to place n queens on an $n \times n$ chessboard in such a way that no queen could attack another? If it is possible, how many different ways are there to arrange the pieces?"

Solve this question for $n = 2, 3, 4, 5$. Look at the number of ways (which is 0 if it's impossible) and now make a guess at to what you think the number will be for $n = 6$. Then work out the case for $n = 6$. Are you surprised by your answer? (Feel free to email me / chat on the discord to check your answers on these.)

For the standard 8 by 8 chessboard, there are 92 ways to put the queens on the board. On a 27 by 27 chessboard, this can be done in 234907967154122528 ways. No one has calculated how many ways there is to do it on a 28 by 28 chessboard. Maybe **you** can!

Part 2) A knight's tour: In the game of chess, a knight can move in the following way: it goes in an L shape that is 1 unit in one direction and then 2 units in a perpendicular direction. For instance the knight in the picture below to move to the indicated squares:



A **knight's tour** is a path that starts somewhere on the chessboard and moves around and visits each square exactly once. We can model this using a graph where each square on the board is a vertex and allowable moves are represented by edges.

1. Draw the graph of allowable moves for a knight on a 3 by 3 chessboard.
2. Draw the graph of allowable moves for a knight on a 3 by 4 chessboard.
3. To find a knight's tour is equivalent to what concept we learned about in class?
4. Show that there IS a knight's tour on a 3×4 chess board. For this, you just need to demonstrate one tour.
5. Show that there IS NOT a knight's tour on a 3×3 chess board. To show this, you'll need to explain why there can't be such a tour.
6. Show that there IS NOT a knight's tour on a 4×4 chess board. To show this, you'll need to explain why there can't be such a tour. (This will feel harder than the previous part, but you can do it. Hint: Think about the corners - and feel free to chat on the discord: `https://tinyurl.com/DiscordMath262Spring2022`
7. Sometimes a knight's tour can be completed in such a way that the knight could move from the end directly back to the start. Explain why such a tour is not possible if the board has an odd number of squares. If you

want to be specific, explain why you can't have such a knight's tour on a 5×11 board. (Hint: think about colors of the squares)

Some Sample Proof Problems

Here were the problems you solved on Quiz 4:

1. Suppose that b is an integer. Prove that if $9|b$ then $3|(15+2b)$.
2. Suppose that n is an integer. Prove that if n^2-2n-1 is even then n is odd.
3. Suppose x and y are real numbers. Prove that if $x+2y$ is irrational then either x is irrational or y is irrational.
4. Suppose x is a real number. If $x^5+4x^4+3x+4=100$ then $x<2$

And some similar practice problems:

1. Prove that if a and b are rational numbers then $a-3b$ is rational.
2. Suppose that $x-y$ and $x+y$ are rational numbers. Prove that x must be rational.
3. Disprove the assertion that "For positive integers m, if $m+1$ and $5m+1$ are both perfect squares, then $m=3$."
4. Find a disproof of the statement: "For real numbers x and y, if $x^2+3x=y^2+3y$ then it follows that $x=y$.
5. Prove or disprove: Let n be a positive integer. If $4 \nmid n$ then $4 \nmid n^2$.
6. Prove that if $x^3+5x=40$ then $x<3$.
7. If $x^2+y^2=z^2$ then either x or y must be even.
8. Let n be a positive integer. Prove that if n^2+4n+5 is even then n is odd.
9. Suppose that $m,n \in \mathbf{Z}$. Prove that if $m^2(n^2+5)$ is even, then m is even or n is odd.

Here are some induction problems that would be reasonable:

1. Prove by induction that for all positive integers n that $n^2 - n$ is even.
2. Prove by induction that for all positive integers n that $n^3 - n$ is a multiple of 3.
3. Prove by induction that for all positive integers n:
$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$
4. Prove by induction that for all positive integers n:
$$1 \cdot 3 + 2 \cdot 4 + \cdots + n \cdot (n+2) = \frac{n(n+1)(2n+7)}{6}.$$
5. Prove by induction that for all positive integers n:
$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2.$$
6. Prove by induction that for all positive integers n:
$$n + 2 < 4n^2.$$

In the following problems, f_n denotes the nth Fibonacci number. Recall the Fibonacci numbers start with $f_0 = 0, f_1 = 1$ and then $f_n = f_{n-1} + f_{n-2}$.

7. Prove by induction that for all positive integers n:
$$f_1 + f_2 + f_3 + \cdots + f_n = f_{n+2} - 1.$$
8. Prove by induction that for all positive integers n:
$$f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}.$$
9. Prove by induction that for all positive integers n that f_{3n} is even.

End of semester information

We made it! We've covered a lot of material this semester and I'm very proud of everyone. I know how hard you are working so let's keep up the energy for the end of the semester.

Logistical Items

- Any late homework, missing zybooks updates, modular quiz "redo"s are all DUE by 6pm on the last day of class. I will be strict about this so that going into the final I can give the most up-to-date grade information possible.
- Mini-Projects must be submitted by Wednesday May 25th at 11:59pm. This is the day of our last final. Remember, you may only turn in one project or revision each week.
- We will have a Bonus Quiz that on Friday May 13th and that will be submitted via google forms.
- 5% of your final exam score will be you encoding / decoding a secret message. See the separate file in this folder for more information.

What will be on the final?

The final will be comprehensive, but will focus mostly on the recent topics - functions, induction, graph theory and number theory. Many of the topics we learned in the beginning of the course concern mathematical language (sets, notation, quantifiers, functions, proofs, logic) are things we use all the time, and so these are also fair game, but they are likely to be applied to problems about graphs or number theory, or functions. For instance, I might ask you to decide whether this statement is true or false:

"In the graph G (some picture of a graph perhaps), let V be the set of vertices and let E be the set of edges. Is it true or false that $\forall v \in V, \exists e \in E$ such that e is incident to v." (This is very much like the "Understanding Quantifiers project that many of you did.)

Overall the final will be similar in format and structure to our quizzes. Please look over our previous quizzes and homework assignments from the class, as well as the worksheet packets. These are the best way to study. I am likely to ask very similar questions to those that I asked on the quizzes.

Note card: You may use one half sheet of paper (standard 8.5 by 11 inch paper) front and back to prepare any notes that you want. You must turn your note card in when you complete your final. If you need a half sheet of paper, let me know I can give you one. You can also use a smaller piece of paper if it's more convenient. You may not use a calculator on the exam.

Exam Rules: Your desk must be clear of all items, including cell phones. No calculators will be allowed.

How to best study: I would recommend starting with the most recent material, especially the homework that is at the end of each of the Number Theory packets 11.2, 11.4, 11.5 (and possibly 11.6 when I write it). If you can answer the questions on these homeworks you are in good shape for the number theory problems.

Here's some advice: Suppose you're working on these problems and you notice that you really struggled with the Fermat's little theorem problems, but after some effort and maybe chatting with others you can get the right answers and they match what the online calculators say. Then the next step is to take a pause, maybe come back the next day and re-solve the problems again. How much did you remember - what would happen if one of those problems shows up on the test? Can you write some notes to yourself on your note card?

Topics

Here is a list of possible topics that we have learned this semester. I know this list seems like a lot, but this list represents the questions we have had on our homework and quizzes.

Number theory: Division and remainder, the division algorithm, how to simplify mod n, using the clock arithmetic, finding congruent / equivalent numbers on the clock,

primes, the proof that there are infinitely many, factorization into primes, in trial division how many numbers do you have to test before concluding a number is prime, gcd, the Euclidean algorithm, Bezout's theorem,

using Bezout's theorem to find inverses mod n, solving congruences, what is an inverse, how to find an inverse, how to use an inverse, when is there an inverse of a mod n, when does an equation $ax \equiv b \bmod n$ have a solution, how many solutions on the clock does $ax \equiv b \bmod n$ have, can you check to see if a number is a solution to an equation,

how to simplify exponents using Fermat's Little Theorem, Euler's Theorem, how to calculate $\phi(n)$, the definition of $\phi(n)$, what it means to be relatively prime, divisibility, relating statements like $x = 4 \bmod 13$ to things like $x = 13k + 4$,

the best way to practice is to solve the homework from our number theory packets. I recommend solving some and posting your solutions to the discord server: `https://discord.gg/PjWxA8KZ` **and work together on solutions. I am happy to provide solutions here and there, but I want to encourage working together as a community to crowd source some answers.**

If you want to re-read an additional chapter from another book that focuses on some of the number theory aspects of the course, please check out this:
`https://drive.google.com/open?id=1tqaAbUl4fs2VbgzKVT3tX7CulU47jPxM`

Graph Theory: Basics of graphs - edges, vertices, when are two graphs equal, when are they isomorphic, what is a degree sequence, how can you get edges form the degrees of vertices,

what is the maximum number of edges a graph on n vertices can have (remember our graphs don't have multiple edges or "loops" allowed), what is a graph called if it has this maximum number of edges, how to tell if a graph is bipartitie, what is K_n, $K_{m,n}$, C_n,

which graphs have Euler paths, Euler circuits, Hamilton paths,

can you tell if a graph is planar, planar versus planar embedding, if it is planar then what does Euler's theorem say, what does Euler's theorem say for convex polyhedra (3D solids), what are the 5 platonic solids, are those graphs planar, can you solve problems like on the homework about building platonic solids using information and Euler's formula, what is a tree, given a small graph can you draw in a spanning trees, when are two trees isomorphic, how many edges/vertices does a spanning tree for a graph with n vertices have, what is a rooted tree,

can you draw a rooted tree, can a graph have an odd number of edges, can a graph have an odd total degree, can a graph have an odd number of vertices of odd degree, given a degree sequence, can you draw a graph with that degree sequence, must such a sequence be the graph of a tree, why or why not.

Induction: What is the basic idea of induction, can you state things like $S(k)$, $S(k+1)$ for a statement like "If $n \in \mathbb{N}$ then $n^2 - n$ is even." What about for a statement like "$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$" or a statement like "if x is a real number and $n \in \mathbb{N}$ then $(1+x)^n \geq 1 + nx$." (all of these are like homework or example problems we did in class)

What is a base case? How does strong induction work? For all of the induction problems you worked on in homework, what were the base cases, how did the induction step work? Can you write a proof of our handshake theorem, that a complete graph with n vertices has $\frac{n^2-n}{2}$ edges? Can you write an induction proof about sums? Can you solve the homework problems about the Fibonacci numbers, how would you simplify something like $f_{2n-1} + f_{2n-2}$.

Functions: What is the definition of a function, what is the domain, the target (aka codomain), what is the range of a function, when is it the same as the target, what does it mean for a function to be 1-1/injective or onto/surjective,

can you give examples of functions that have desired properties (1-1, onto, etc), how does the floor function $f(x) = \lfloor x \rfloor$ work,

is there an injective function from $\mathbf{Z}$ to $\mathbb{N}$ (yes) is there a surjective function from $\mathbb{N} \to \mathbf{Z}$ (yes), can you describe these functions? How does composition of functions work, can you draw examples of functions (with arrows) so that f is not onto but $g \circ f$ is onto, can you tell if a function is not well-defined because there's not an output for each allowable input

Earlier Material: What's most important is to be familiar with the basic proof setups, contradiction, contrapositive, direct proof, know that a statement is NOT the same as its converse, have an example of a statement that is true, but whose converse is false,

what is the union or intersection of two sets, what is the difference $A - B$ of two sets, what is a cartesian product, what is the powerset. For instance if $A = \{1, 2\}$ and $B = \{2, 4\}$ what is $P(A - B)$? What is $(A - B) \times A$, can you write down three elements of $P(A \times B)$? What is $|P(A \times B)|$?

Some random practice problems

These problems are not meant to be exhaustive - but these are meant to represent the types of questions that could combine the concepts we've been learning this semester. Further they will help you think through some complex problems.

1. If G is the graph $K_{4,7}$ with vertex set V then define the function

$$f : V \to \mathbb{N}, \quad f(v) = \deg(v).$$

   Is f 1-1? is it onto? What is the range of f? If

$$S = \{v \in V \ : f(v) \geq 5\}$$

   then what is $|S|$?

   The above problem is a good example of how a question about "graphs" is really a good way to get practice with sets and functions. For instance, here's another one:

2. Let S be the set $\{z, e, l, d, a\}$. Define the function $f : S \to P(S)$ as follows:

$$f(blah) = \{z, e, l\} \cup \{blah\}.$$

   What is $f(z)$? What is $f(a)$? Explain why f is not onto. Explain why f is not $1 - 1$.

3. Consider the set

$$S = \{a : 1 \leq a \leq 25, \quad \gcd(a, 25) = 1\}$$

   and define the function $f : S \to S$ by $f(x) = 3x \bmod 25$. Is 10 in the domain of f? What is $f(11)$? Explain why 13 is in the range of f.

4. Consider the graph G defined as follows. Let there be 6 vertices labeled $1, 2, \ldots, 6$. Connect two distinct vertices a and b if $ab \equiv \pm 2 \bmod 7$. How many edges does G have?"

5. In class we learned a formula for $\phi(n)$. What does that formula say if n is a power of a single prime? Is $\phi(n)$ sometimes, always, never odd? What if n is divisible by two or more distinct primes. Is $\phi(n)$ sometimes, always, or never odd.

6. This question is about reading a new definition and interpreting what it says: Suppose that students are attending a conference and each is given some badge number $N \in \mathbb{N}$. (Their numbers N have special properties.) Each student has a locker and inside the locker is a prize. The students are told that the password to their locker is obtained as follows. First they need to factor their number N into a product of three distinct primes: pqr with $p < q < r$. Their password is $q + r$. What is the password for student with badge number 70. What is the smallest possible password for any student?

7. This question is about reading a new definition and interpreting what it says: Let n be a natural number and let p be a prime factor of n. Suppose that p^e is the largest power of p that is a factor of n. Then the number p^e is called the **p-Torero-ness** of n. What is the 2-Torero-ness of 24? What is the 3-Torero-ness of 18? What is the 2-Torero-ness of 100?

Why am I making up these seemingly random questions? One of the biggest goals in this class is to help us improve our **reading** and **critical thinking skills.** The problems above are densely packed (just like the pages of technical/scientific/legal writings), and the only way to understand what it is saying is to get out a piece of paper and carefully work it out with examples.

Math 262 Final Exam

- The USD Honor Code is in effect for this exam.
- Please don't start the exam until told to do so.
- This exam is worth 100 points.
- You may not use a calculator on this exam.
- If you have any questions, please let me know.
- If you need extra paper, let me know - I have scratch paper.
- Please show all work and write clearly in complete sentences.

Good luck everyone!

Encryption Problem: (5 points)

You completed this problem ahead of time. Good decrypting skills!

Short answer and multiple choice (30 points)

1. (3 points) Write down a subset S of the set $\mathbf{Z} \times (\mathbb{Q} - \mathbf{Z})$ with the property that $|S| = 3$.

2. (3 points) Explain why the function

   $f : \{\text{positive even integers}\} \to \{\text{positive odd integers}\}$ given by $f(x) = x + 2$ is not well-defined.

3. (3 points) A sequence s_n is defined by the formula $s_n = 3n + 4$. A student lists a bunch of terms of the sequence below in order. Fill in the missing terms:

$$7, 10, 13, 16, \underline{\hspace{3cm}}, \ldots, \underline{\hspace{3cm}}, 3m - 5$$

4. (3 points) Which of the following is meant by: $A \subseteq X$?

   (a) A is an element of X

   (b) X is a subset of A

   (c) Every element of A is also an element of X

   (d) The ordered pair (A, X) not the empty set.

5. (3 points) A shop sells cookies in boxes of 12. If the store has made x cookies, which of the following represents the number of complete boxes it has:

   (a) $\lfloor 12x \rfloor$

   (b) $\lceil 12x \rceil$

   (c) $\lfloor x/12 \rfloor$

   (d) $\lceil x/12 \rceil$

6. (3 points) You are reading a book about math (rock on!). There is a chapter about a peculiar function called $H(x)$ and in the book you read a theorem that says that:

$$H(1) + H(4) + H(7) + \cdots + H(3n - 2) = n^2 - 3.$$

   Use this formula to calculate the following:

$$H(1) + H(4) + H(7) + \cdots + H(16)$$

7. (3 points) Write down a true statement whose converse is false.

8. (3 points) Which of the following best describes the inductive step in a proof by induction:

   (a) You prove that $S(k+1)$ is true for all k;

   (b) You prove that when $S(k)$ is true $S(k+1)$ is also true;

   (c) You assume $S(k+1)$ is true and then show that $S(k+1)$ is true;

9. (3 points) You are encrypting a message using RSA with the numbers $N = 55$ and your encryption exponent is $e = 13$. Which of the following would be a description of your decrypting exponent:

   (a) The inverse of 35 mod 60

   (b) The inverse of 13 mod 40

   (c) There is no decrypting exponent

   (d) The inverse of 13 mod 24

   (e) The inverse of 24 mod 35

   (f) The inverse of 13 mod 60

   (g) The inverse of 13 mod 35

10. (3 points) Suppose that a and b are three digit numbers and $3a + 7b = 1$ then which of the following would be a solution to

$$7x \equiv 1 \bmod a.$$

   (a) $-b$

   (b) b

   (c) a

   (d) 7

   (e) 3

   (f) $-a$

Number Theory (30 points)

Here are the primes that are less than 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

The following computations may help you during the exam:

- $70(4) - 93(3) = 1$
- $23(-16) + 41(9) = 1$
- $48(-11) + 23(23) = 1$
- $7 \cdot 29 \equiv 1 \bmod 101$
- $7 \cdot 40 \equiv 1 \bmod 93$
- $4 \cdot 37 \equiv 1 \bmod 147$
- $2623 = 43 \cdot 61$

1. (3 points) What is the inverse of 37 modulo 147?

2. (3 points) What is the inverse of 20 modulo 93?

3. (2 points) Which of the following would be a solution to $29x \equiv 4 \bmod 101$

   $x = 7$ $\qquad$ $x = 28$

   $x = 29$ $\qquad$ $x = 21$

4. (5 points) Solve the congruence by finding a solution x in the range $0 \leq x \leq 40$.

$$23x \equiv 2 \bmod 41.$$

5. (3 points) Find the gcd of a and b where

$$a = 2^3 \cdot 5^4$$
$$b = 2^5 \cdot 15^3$$

6. (4 points) How many integers x between with $1 \leq x \leq 800$ are relatively prime with 800? (Hint: You can leave your answer factored.)

7. (5 points) Simplify $3^{35} \bmod 17$ to a number in the range from 0 to 16.

8. (5 points) a) Explain why Euler's Theorem would **not** apply in the following calculation:

$$10^{100} \bmod 20.$$

b) Now simplify $10^{100} \bmod 20$ to a number in the range from 0 to 19. Explain your reasoning. (You won't be able to use Euler's theorem, but you can still calculate this another way.)

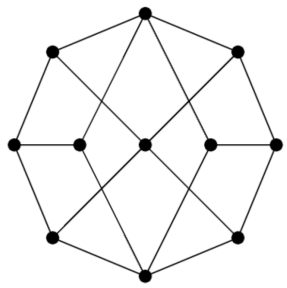
3) Some graph theory (25 points)

1. (3 points) You are given a graph G that has degree sequence $(2, 2, 3, 3, 3, 3)$. Does this graph have an Euler path? Why or why not?

2. (3 points) Draw a graph with degree sequence $(4, 1, 1, 1, 1)$. Say whether or not your graph is a tree.

3. (3 points) If a connected planar graph is drawn with total degree 22 and with 7 vertices, how many faces (or regions) must it have? (As usual, the "outside" region counts as well).

4. (6 points) Consider the graph below:



Is this graph bi-partite? If so, how many elements are in each "part". Support your answer by labeling vertices as being in part A or part B.

5. (10 points) Prove that there is not a 3D convex polyhedron that can be built with three triangles, six pentagons (5-sided polygons) and five heptagons (7-sided polygons)

A proof by induction (10 points)

Recall that the Fibonacci numbers are defined with $f_1 = 0,\ f_2 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Using induction, prove that for $n \geq 1$:

$$f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$$