MATH 210 Notes

Vladislav Taranchuk

December 8, 2021

Contents

1 Lecture - 09/01/2021

1.1 Mathematical Logic

We begin our course with the study of the basic concepts of mathematical logic.

Definition. A **proposition** is a definitive statement of fact, that is either *true* or *false*. If the statement is inconclusive, or it is relative, or dependent on something or someone, then it is NOT a proposition.

Examples: Here are some examples of propositions, and their corresponding truth values.

- $7 > 3$ - *True*
- "Today is September 1st" - *True*
- "Tomorrow is September 1st" - *False*
- $5 + 35 = 1$ - *False*
- $x^2 - 3x + 2 = (x - 2)(x - 1)$ - *True*
- "The Earth is flat" - *False*?

Non-Examples: Here are some statements that do no qualify as propositions. Why?

- $x + 3 > 5$ - This statement is unverifiable, unless we know what x is.
- "The weather outside is nice" - This is an opinion, not a fact.
- "They are attractive" - Again, this is an opinion, not a fact.
- Line ℓ is parallel to line k - We do not know what lines ℓ and m are
- $x^2 + 5 = 0$ - This statement is unverifiable, unless we know what x is.

There are many ways we can turn equations or inequalities into mathematical propositions. While the statement $x+3 > 5$ does not itself carry a truth value, it is still a statement that *can become* true or false depending on x. One way to turn $x + 3 > 5$ into a proposition, is to assign a truth value to it. For example, if we say "Let $x + 3 > 5$" or "Suppose $x + 3 > 5$", then we are *assigning a truth value of true* to the statement, thereby turning it into a proposition. The same is true for any other mathematical statements with variables or unknowns.

Another way statements with unknowns or variables can be turned into propositions, is if the statement is preceded by a *quantifier* for each variable in the statement. We will discuss quantifiers in detail in Lecture 2.

Often times, mathematical propositions can have a truth value that is not easy to determine, and will require a serious rigorous argument to *prove* whether the proposition is true or false. One of the primary goals of this course will be to teach us to make mathematically rigorous arguments.

Let p and q be propositions. We introduce the following mathematical notation:

- $\neg$ is called the **not (negation)** symbol. We read $\neg p$ as "not p".
- $\wedge$ is called the **and (conjunction)** symbol. We read $p \wedge q$ as "p and q".
- $\vee$ is called the **or (disjunction)** symbol. We read $p \vee q$ as "p or q"
- $\rightarrow$ is called the **implies (implication)** symbol. We read $p \rightarrow q$ as "p implies q"
- $\leftrightarrow$ is called the **if and only if (double implication)**. We read $p \leftrightarrow q$ as "p if and only if q".

The implies symbol $\rightarrow$, can often be read in several different ways. Here are the most common, " p implies q", "if p, then q", "p is sufficient for q ", " q is necessary for p ".

Likewise, the if and only if symbol $\leftrightarrow$ can be read in several different ways. $p \leftrightarrow q$, " p if and only if q", "p is necessary and sufficient for q". The language of this last quote gives away the fact that $p \leftrightarrow q$ means that p implies q and q implies p.

Using this symbol it is possible to build more complicated mathematical propositions. We will now build what is called a *Truth Table* to determine the truth values of each above mentioned symbols. Make certain to understand and memorize the following truth table. The symbols above alongside the propositions form the building blocks of building more complex mathematical propositions.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Let us comment on the truth table for a moment. Most of the truth values are fairly intuitive, except for perhaps the implication. Let p and q be propositions.

- If p is true then $\neg p$ is false, and vice versa.
- $p \wedge q$ is only true when both p is true AND q is true simultaneously.
- $p \vee q$ is true any time that either p is true OR q is true.
- $p \leftrightarrow$ is only true when p has the same truth value as q.

Let's do a few examples using these rules to determine the truth values of some more complicated propositions.

Example 1: Suppose that p, q, r are propositions. Build the truth table of $(p \wedge q) \to \neg r$.

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \to \neg r$
T	T	T	T	F	T
T	T	F	T	T	F
T	F	T	F	F	T
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	T
F	F	F	F	T	T

Example 2: Suppose that p, q, r are propositions. Determine the truth table for

$$[(p \to q) \wedge (q \to r)] \to (p \to r)$$

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Examples 2 above as it turns out is also an example of a proposition that is a *tautology*.

Definition. There are two special types of propositions to which we give special names.

- A **tautology** is a proposition that is always true. Denote a tautology by **1**.
- A **contradiction** is a proposition that is always false. Denote a contradiction by **0**.

Let us try to understand Example 2 using plain English and by defining p, q, r to be specific statements.

- $p =$ It is raining outside.
- $q =$ I am bringing my umbrella.
- $r =$ I won't get wet.

We can then attempt to translate into English the following propositions.

- $p \to q$ = If it is raining outside, then I am bringing my umbrella.
- $q \to r$ = If I am bringing my umbrella, then I won't get wet.
- $(p \to q) \wedge (q \to r)$ = If it is raining outside, then I am bringing my umbrella *and* If I am bringing my umbrella, then I won't get wet.
- $p \to r$ = If it is raining outside, then I won't get wet.

Using this now, we can see how in plain English the statement "If it is raining outside, then I am bringing my umbrella *and* If I am bringing my umbrella, then I won't get wet." *implies* the statement "If it is raining outside, then I won't get wet."

However, it is important to understand that the statement $(p \to q) \wedge (q \to r)$ is NOT logically equivalent to $p \to r$, meaning, these two statments are not quite saying exactly the same thing.

Definition. Let A and B be two propositions(they could be complex or simple). We say A is **logically equivalent** to B and denote it by $A \iff B$ if A and B always take on the same truth values.

The easiest way to check if two statements are logically equivalent is by building a truth table for both and observing if they both statements always have the same truth values.

Definition. Let p and q be propositions. We say that the **contrapositive** of the proposition "$p \to q$" is "$\neg q \to \neg p$".

Let us prove our first theorem, demonstrating that an implication and its contrapositive are logically equivalent. Before we begin, it is worth mentioning that there are many ways to prove statements. We will proceed in the fashion of a *direct proof* for the following theorem. A direct proof is the most straightforward way to prove something, you may have heard this type of argument called by another name, *modus ponens*. You will probably never hear the term "*modus ponens*" used in this class ever again. :)

Theorem 1.1.1. *Suppose p and q be propositions. Then*

$$p \to q \iff \neg q \to \neg p.$$

Proof. The following table shows that $p \to q$ and $\neg q \to \neg p$ take on the same truth values.

p	q	$\neg q$	$\neg p$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

□

When a proof is finished, mathematicians draw a little box to denote the end. Alternatively, one can also write Q.E.D. to denote end of a proof.

2 Lecture - 09/03/2021

2.1 The Algebra of Logic

Just like there are laws that govern how to properly evaluate algebraic equations and how to add, subtract, multiply and divide numbers, there are laws that govern how to evaluate complex logical propositions correctly. All these laws can be proven using truth tables, an exercise I would recommend you all try in order to convince yourselves.

Theorem 2.1.1. *Let p, q, r be propositions. Then the following laws are true:*

1. ***Idempotence Law**: $p \vee p \iff p \wedge p \iff p$.*
2. ***Double Negation Law**: $\neg(\neg p) \iff p$.*
3. ***Law of Contrapositive** $p \to q \iff \neg q \to \neg p$.*
4. ***Associativity**:*
   - $((p \wedge q) \wedge r) \iff (p \wedge (q \wedge r))$.
   - $((p \vee q) \vee r) \iff (p \vee (q \vee r))$.
5. ***Distributive Laws**:*
   - $((p \vee q) \wedge r) \iff (p \wedge r) \vee (q \wedge r)$.
   - $((p \wedge q) \vee r) \iff (p \vee r) \wedge (q \vee r)$
6. ***De Morgan's Laws**:*
   - $\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$.
   - $\neg(p \wedge q) \iff (\neg p) \vee (\neg q)$.

Two more laws that demonstrate that one can re-write any proposition containing the symbols $\to$ and $\leftrightarrow$ into one only containing the symbols $\neg, \vee, \wedge$.

- $p \to q \iff (\neg p \vee q)$.
- $p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$.

Example: Let p and q be propositions. Simplify the proposition:

$$[\neg(p \vee q)] \vee [(\neg p) \wedge q].$$

Solution.

$$\begin{aligned}
[\neg(p \vee q)] \vee [(\neg p) \wedge q] &\iff \underline{[(\neg p) \wedge (\neg q)]} \vee [(\neg p) \wedge q] \quad \text{By } \textit{De Morgan's Law} \\
&\iff (\neg p) \wedge [(\neg q) \vee q] \quad \text{By the } \textit{Distributive Law} \\
&\iff (\neg p) \wedge \mathbf{1} \quad \text{Since } [(\neg q) \vee q] \text{ is a } \textit{tautology} \text{ (Why?)} \\
&\iff \neg p.
\end{aligned}$$

Finally, introduce two notations that slightly extend the notions of $\wedge$ and $\vee$. Suppose that $a_1, a_2, a_3, \ldots, a_n$ are all propositions. Then:

$$\bigwedge_{i=1}^{n} a_i = a_1 \wedge a_2 \wedge \cdots \wedge a_n \quad \text{and} \quad \bigvee_{i=1}^{n} a_i = a_1 \vee a_2 \vee \cdots \vee a_n$$

2.2 Quantifiers

Recall the several examples we had of statements that were not propositions:

- $x + 3 > 5$
- Line ℓ is parallel to line k
- $x^2 + 5 = 0$

The issue was that x was unknown and we could not verify whether or not the statement was true or false. This can be fixed, if to each unknown variable in the statement we attach a *quantifier*.

Definition. A **quantifier** in mathematical logic is a phrase that can be attached to a statement that gives information about an unknown variable. There are two different quantifiers in mathematical logic, "For all" and "there exists":

- "For all" is denoted by the symbol $\forall$. Often times, we say "For every" or "For each" instead of "For all".
- "There exists" is denoted by the symbol $\exists$. Often time, we "For some", instead of "There exists".

Example: Consider the following propositions:

(i) There exists a real number x such that $x + 3 > 5$.

(ii) For all real numbers x, $x + 3 > 5$.

(iii) Given a line ℓ whose equation is $y = 3x + 2$ there exists a line k (distinct from ℓ) that is parallel to ℓ.

All of these statements now have an explicit truth value, and we can verify each one.

(i) Can we find just one real number x that satisfies the inequality $x + 3 > 5$? If so, then (i) is true. How about $x = 10$? Well, then $x + 3 = 10 + 3 = 13 > 5$, and so $x = 10$ is a real number that satisfies the inequality. Thus proposition (i) is *True*.

(ii) Is it true that EVERY real number satisfies the inequality $x + 3 > 5$. Well we can subtract 3 from both sides to see that $x + 3 > 5 \iff x > 2$. Is it true that EVERY real number is greater than 2? Definitely not! So proposition (ii) is *False*.

(iii) Consider the line $y = 3x + 2$, can you find just one other line that is parallel to $y = 3x + 2$? We know that two lines are parallel if they have the same slope. So $y = 3x$ is a line different from $y = 3x + 2$ but is parallel to it. So then proposition (iii) is *True*.

Let us now consider quantifiers when we have a proposition with multiple unknown variable floating around.

To avoid rewriting the same statements over and over, we can give names to various statements. Let $P(x)$ denote the statement $x + 3 > 5$. Then instead of writing "There exists a real number x such that $x + 3 > 5$", we may write "$\exists x$, x a real number, $P(x)$". Soon we will be able to shorten this statement even more once we introduce the notion of sets.

Example: Let x, y be real numbers. Let $Q(x, y)$ denote the statement "$x^2 + y = 10$". Let us consider a few different propositions and translate them into plain English. After which we will determine the truth value of each proposition.

(i) $\exists x \exists y Q(x, y)$.
This means: There exists an x and a y satisfying $x^2 + y = 10$. - *True*
Consider $x = 3$ and $y = 1$, then $x^2 + y = 3^2 + 1 = 9 + 1 = 10$.

(ii) $\exists x \forall y Q(x, y)$.
This means: There exists an x for which every y will satisfy $x^2 + y = 10$. - *False*
This is impossible! If we pick an x, then there is only one y that will satisfy $x^2 + y = 10$, namely $y = 10 - x^2$. So it is not true that that any real number y would work.

(iii) $\forall x \exists y Q(x, y)$.
This means: For every x, there exists a y that satisfies $x^2 + y = 10$. - *True*
This is true, by the same argument we made in (*ii*). Pick any real number x, and then choose $y = 10 - x^2$ (so y depends on x). Then substituting for y, we have

$$x^2 + y = x^2 + (10 - x^2) = 10.$$

So then it is true that for all x, we can find a y satisfying $x^2 + y = 10$.

(iv) $\forall y \exists x Q(x, y)$.
This means: For every y, there exists an x that satisfies $x^2 + y = 10$. - *False*
This one is similar to the (*iii*), then why is it false? Let us find a counter-example. Suppose that $y = 11$, then for this y, we need to find an x satisfying $x^2 + 11 = 10$. Now, if $x^2 + 11 = 10$, then $x^2 = -1$ so $x = \pm\sqrt{-1}$. But $\sqrt{-1}$ is NOT a real number. So then the proposition cannot be true, because it is not true for all real numbers y.

Example: Let s be a student at UD, c be a class taught at UD in Spring 2021, and g be a grade. Let $Q(s, c, g)$ represent the statement "Student s took class c and earned grade g." Let us interpret and determine the truth value of the following.

- $\forall s \exists c \exists g Q(s, c, g)$.
  This means: Every student took a class and earned some grade for it. - *True*
- $\forall c \exists s Q(s, c, \mathrm{F})$.
  This means: In every class, there was a student who received a failing grade, F. - *False*
- $\exists s Q(s, \text{Math 210, B})$.
  This means: There exists a student in Math 210 who earned a B. - *True*

3 Lecture - 09/08/2021

3.1 Sets

We begin this section by defining the notion of a set. It is a rather ambiguous notion, yet mathematics is fundamentally built from the ground up using sets. There is a whole branch of mathematics called Set Theory which studies this exact idea. Set Theory aims to formalize the language of mathematics in order to ensure that there are no logical contradictions lurking within the foundation of mathematics.

Definition. A **set** is just a collection of *distinct* things that we wish to group together. The "things" themselves are referred to as *elements* of the set. To denote a set we, enclose the elements of the set with {}, curly braces.

Examples of Sets:

- { apple, dog, 6, car, John } has elements: 'apple', 'dog', '6', 'car', 'John'.
- $\{0, 1, \{1, 2, 3\}\}$ has elements: '0', '1', '$\{1, 2, 3\}$'. Both 2 and 3 are NOT elements of the set.
- $\{\{\{x\}\}\}$ has element: $\{\{x\}\}$.

Notice that the second set still meets the definition even though visually, we observe that 1 appears twice. This is because 1 is only an element of the set once. The other 1 is inside $\{1, 2, 3\}$, which is entirely separate.

Non-Examples of Sets:

- $\{2, 3, 5, 5, 6\}$
- $\{\{0\}, \{0\}\}$

To denote that a element belongs to a set, we use the symbol $\in$, and $\notin$ if an element is *not* in a set.

Example: Let $A = \{2, 3, 7, 11, \{12\}\}$. Determine if the following propositions are true or false:

(i) $3 \in A$ - *True*

(ii) $4 \in A$ - *False*

(iii) $12 \notin A$ - *True*

(iv) $\{12\} \in A$ - *True*

We now introduce some common notation for sets that will be frequently used.

- $\emptyset = \{\}$ the empty set.
- $[n] = \{1, 2, \ldots, n\}$
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of all natural numbers.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of all integers.
- $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}\}$
- $\mathbb{R}$ = the set of all real numbers.

3.2 Subsets

Now that we have defined the notion of a set, we will state what it means for one set to be a *subset* of another set.

Definition. Let A and B be sets. We say "A is a **subset** of B", and denote it by $A \subseteq B$, if and only if every element of A is also an element of B. Often times, we may also say "A is contained in B" instead of "A is a subset of B".

Example: Let $A = \{1, 2\}, B = \{1, \{2\}\}, C = \{1, 2, \{2\}\}$. Determine whether the following propositions are true.

- $\emptyset \subseteq A$ - *True*
- $\{\emptyset\} \subseteq \emptyset$ - *False*
- $A \subseteq B$ - *False*
- $A \subseteq C$ - *True*
- $(A \subseteq C) \wedge (B \subseteq C)$ - *True*
- $\{2\} \subseteq B$ - *False*
- $\{\{2\}\} \subseteq B$ - *True*
- $\{2\} \in B$ - *True*
- $A \subseteq \mathbb{N}$ - *True*
- $\mathbb{Z} \subseteq \mathbb{N}$ - *False*
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ - *True*

Definition. We say two sets A and B are **equal**, and write $A = B$, if and only $A \subseteq B$ and $B \subseteq A$. Another way of write this is $A = B$ if and only if $(x \in A \iff x \in B)$. So $x \in A$ means $x \in B$ and $x \in B$ means $x \in A$.

Exercise 3.2.1. Show that $A = \{2k + 1 : k \in \mathbb{Z}\}$ and $B = \{2k - 1 : k \in \mathbb{Z}\}$, then $A = B$ as sets.

Solution: We must show $A \subseteq B$ and $B \subseteq A$.

1. First we show $A \subseteq B$. In order to demonstrate this, we must show that if $x \in A$, then $x \in B$. Let $x \in A$, then $x = 2k + 1$ for some integer $k \in \mathbb{Z}$. Notice, we can write $2k + 1 = 2(k + 1) - 1$, where $k + 1$ is again another integer. So then $x = 2m - 1$ where $m = k + 1$, $m \in \mathbb{Z}$. Therefore, by definition, $x \in B$.

2. Now we show $B \subseteq A$. In order to demonstrate this, we must show that if $x \in B$, then $x \in A$. Let $x \in B$, then $x = 2k - 1$ for some integer $k \in \mathbb{Z}$. Notice, we can write $2k - 1 = 2(k - 1) + 1$, where $k - 1$ is again another integer. So then $x = 2m - 1$ where $m = k + 1$, and $m \in \mathbb{Z}$. Therefore, by definition, $x \in A$.

We now introduce the notion of a power set which will appear from time to time.

Definition. Let A be a set, then the **power set of** A, is defined as

$$\mathcal{P}(A) = \{B : B \subseteq A\}.$$

Example: Let $A = \{1\}$ and $B = \{1, 2\}$.

- $\mathcal{P}(\emptyset) = \{\emptyset\}$.
- $\mathcal{P}(A) = \{\emptyset, \{1\}\}$.
- $\mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

As can be seen above, for any set A, it is always the case that $\{\emptyset\} \subseteq \mathcal{P}(A)$ and $A \subseteq \mathcal{P}(A)$. It is also important to note that the individual elements of A are never elements of $\mathcal{P}(A)$.

Finally, we introduce a couple of notations that may come up every once in a while, but in general are not in common use. Let A and B be sets.

- If we wish to distinguish a subset from a **proper subset**, we write $A \subset B$ or $A \subsetneq B$. By a proper subset, we mean $A \subseteq B$ but $A \neq B$, where the usual notation $\subseteq$ has no such restriction.
- We say A is a **superset** of B, and write $A \supseteq B$, if and only if $B \subseteq A$. There may be times when it is more convenient to write $\supseteq$ than $\subseteq$ within proofs or the statement of various theorems.

3.3 Sets and Paradoxes

We end this lecture with an interesting paradox. You may all wonder why there is need for such care in the way that we define sets, and really everything else in mathematics. The following paradox demonstrates a good reason for why such rigor is important.

Russel's Paradox: Let S be the set of all sets that do not contain themselves. Meaning for every element $x \in S$, $x \notin x$. It is already a strange notion for a set to contain itself. These sorts of strange possibilities can arise when we consider *infinite* sets. Now, does S contain itself?

- If $S \in S$ then by definition of S, $S \notin S$, a contradiction.
- So perhaps $S \notin S$. But if $S \notin S$, then, since S is the set of all sets that do not contain themselves, and $S \notin S$, then S must contain itself, so $S \in S$, again a contradiction!

So then no such set cannot exist, even though we can describe it perfectly well.

I'm sure that reading through all that, you may have a hard time wrapping your head around it. So let's try to illustrate a similar paradox by considering things a little closer to home.

The Barber Paradox: Suppose that there is a barber that shaves all those people who do not shave themselves. Who shaves the barber?

- If the barber does not shave himself, then by definition he is someone who does not shave himself, and therefore, must be shaved by the barber, so he does shave himself, a contradiction!
- If the barber shaves himself, then by definition, he must be someone who does not shave himself, because the barber only shaves those people who do not shave themselves, so again a contradiction.

All this to say, there is good reason for us to learn to be precise in our language as well as our mathematics. You can look both of these paradoxes up online. They each have a wikipedia page devoted to them.

4 Lecture - 09/10/2021

We begin this lecture by introducing various operations on sets. Keep in mind that a lot these operations have analogies with the way that the algebra of logic works. Keep in mind the definitions of $\wedge, \vee, \neg$ while going through this section.

4.1 Union and Intersection

Definition. Let A and B be sets. Then:

- The **union** of A and B, denoted $A \cup B$ is the set of elements in A or in B (or in both). You can think of union operation being analogous to the $\vee$ operation in logic. $A \cup B$ can be described using mathematical logic as follows:

$$x \in A \cup B \iff (x \in A) \vee (x \in B).$$

- The **intersection** of A and B, denoted $A \cap B$ is the set of elements in A and B. You can think of the intersection operation being analogous to the $\wedge$ operation in logic. $A \cap B$ can be described using mathematical logic as follows:

$$x \in A \cap B \iff (x \in A) \wedge (x \in B)$$

Examples: Let $A = \{1, 2, \{3\}\}, B = \{1, 3, \{3\}, \{2, 3\}\}$. Then:

- $A \cup B = \{1, 2, 3, \{3\}, \{2, 3\}\}$.
- $A \cap B = \{1, \{3\}\}$.
- $A \cup \emptyset = A$.
- $A \cap \emptyset = \emptyset$.

Definition. Two sets A and B are said to be **disjoint** if $A \cap B = \emptyset$.

We can further extend the definitions of union and intersection to include more sets. Let $A_1, A_2, \ldots, A_n$ be sets. Then we introduce the following notations:

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

When we try to find a new set whose definition is a mixture of unions and intersections of other sets, then parentheses are important. They help us determine, what operations to do first.

Example: Let $A = \{1, 2, 3, 4\}, B = \{3, 4, 5, 6\}$ and $C = \{2, 3, 5, 7\}$. Find $(A \cap B) \cup C$ and $A \cap (B \cup C)$.

Solution. To find $(A \cap B) \cup C$ we must first find $(A \cap B)$. $A \cap B = \{3, 4\}$. Then

$$(A \cap B) \cup C = \{2, 3, 4, 5, 7\}.$$

To find $A \cap (B \cup C)$ we must first find $B \cup C$. $B \cup C = \{2, 3, 4, 5, 6, 7\}$. Then

$$A \cap (B \cup C) = \{2, 3, 4\}.$$

Clearly, here $(A \cap B) \cup C \neq A \cap (B \cup C)$. So we must take care to do set operations inside parentheses first. Many laws that we found in the algebra of logic, transfer to the algebra of sets. For example, the distributive laws for $\wedge$ and $\vee$.

Theorem 4.1.1. *(Distributive Law for Sets) Let A, B, C be sets. Then*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof. There are several ways one can prove that the sets are equal. We will prove this specific statement in two distinct ways. The first will be an analogy to truth tables. I will make two separate tables because a single on doesn't fit on the page. Remember, if the operation is $\cup$ then think of it as $\vee$, if the operation is $\cap$ then think of it as $\wedge$.

$x \in A$	$x \in B$	$x \in C$	$x \in A \cap B$	$x \in A \cap C$	$x \in (A \cap B) \cup (A \cap C)$
T	T	T	T	T	**T**
T	T	F	T	F	**T**
T	F	T	F	T	**T**
T	F	F	F	F	**F**
F	T	T	F	F	**F**
F	T	F	F	F	**F**
F	F	T	F	F	**F**
F	F	F	F	F	**F**

$x \in A$	$x \in B$	$x \in C$	$x \in B \cup C$	$x \in A \cap (B \cup C)$
T	T	T	T	**T**
T	T	F	T	**T**
T	F	T	T	**T**
T	F	F	F	**F**
F	T	T	T	**F**
F	T	F	T	**F**
F	F	T	T	**F**
F	F	F	F	**F**

Together, these tables tell us precisely that $x \in A \cap (B \cup C)$ if and only if $x \in (A \cap B) \cup (A \cap C)$. Completing the proof. □

Let us now proceed to prove the theorem in a slightly different way. This method of proving two sets are equal is often referred to as *element chasing*.

Proof. We need to show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. By the definition of equality of sets, this means we need to prove that both of the following statements are true.

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{and} \quad A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C).$$

($\subseteq$): We first suppose $x \in A \cap (B \cup C)$ and we must demonstrate that $x \in (A \cap B) \cup (A \cap C)$. If $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. Since $x \in B \cup C$, then $x \in B$ or $x \in C$.

Then from here, this portion of the proof splits into two cases, either $x \in B$ or $x \in C$ (if it is in both, then using the argument from either case will work).

Case 1: Suppose that $x \in B$. Then since $x \in A$ as well, it must be that $x \in A \cap B$. But this implies $x \in (A \cap B) \cup (A \cap C)$ (since union can only add to the set $A \cap B$, it can never remove anything). This finishes the proof in the case $x \in B$.

Case 2: Suppose that $x \in C$. The proof for this case follows identically to the one above. Since $x \in A$ as well, it must be that $x \in A \cap C$. But this implies $x \in (A \cap B) \cup (A \cap C)$ (since union can only add to the set $A \cap C$, it can never remove anything). This finishes the proof in the case $x \in C$.

So we have shown in total that if $x \in A \cap (B \cup C)$ then $x \in (A \cap B) \cup (A \cap C)$. Which implies $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

($\supseteq$): We now demonstrate that if $x \in (A \cap B) \cup (A \cap C)$ then $x \in A \cap (B \cup C)$. Suppose that $x \in (A \cap B) \cup (A \cap C)$, then this means that $x \in A \cap B$ or $x \in A \cap C$. These two cases imply, that either: $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$. In any case $x \in A$ and $x \in B$ or $x \in C$. But this last statement just means $x \in B \cup C$, and therefore $x \in A \cap (B \cup C)$. Thus, $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$. □

The proof could have been written with less wording, but given that the reader is not expected to have seen proofs before, we take care to be very explicit about every step. To see a slightly more concise version of the proof, see *Problem 6* on pages 44–45 in the textbook.

The following exercise gives important results. I recommend that you try to work out the details on your own.

Exercise 4.1.1. Let A and B be sets. Show that:

- $A \cap B = A$ if and only if $A \subseteq B$.
- $A \cup B = B$ if and only if $A \subseteq B$.

4.2 Set Differences

Definition. Let A and B be sets. The **set difference** of A and B, written as $A \setminus B$, is the set of all elements of A that are not elements of B.

Definition. The **complement** of a set A, is $A^c = U \setminus A$, where U is some *universal set* that is either given, or is made clear from the context.

Example: Let $U = \{a, b, c, d, e, f, g, h, i\}$, $A = \{a, c, g, h\}$, and $B = \{g, h, i\}$. Then:

- $A \setminus B = \{a, c\}$
- $B \setminus A = \{i\}$
- $A^c = \{b, e, d, f, i\}$
- $(A \cup B)^c = \{b, e, d, f\}$
- $(A \cup B) \setminus U = \emptyset$
- $A \cap B^c = \{a, c\}$

Exercise 4.2.1. Let A and B be sets. Write a sentence or two justifying the following statement (use the definitions of $\setminus$ and $\cap$ and think about why this is intuitively true), then prove give a proof:

$$A \setminus B = A \cap B^c.$$

Here is an example where the universal set U is made clear from the context.

Example: Let $A = \{x \in \mathbb{Z} : x^2 > 4\}$. In words, A is the set of integers whose square is greater than 4. Then it is clear that the universal set here is the entire set of integers, so $U = \mathbb{Z}$. Furthermore, observe the relationship between complements and the inequality within the set:

$$A^c = \{x \in \mathbb{Z} : x^2 > 4\}^c = \{-2, -1, 0, 1, 2\} = \{x \in \mathbb{Z} : x^2 \leq 4\}.$$

If in the above example, the universal set was the set of real numbers $\mathbb{R}$ instead of the integers $\mathbb{Z}$, then we would be dealing with *intervals* of the real number line, which you have likely seen before. Let us briefly review interval notation:

Definition. Let a and b be real numbers such that $a < b$. Then:

- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$

Example: Let us work through a few examples with intervals and set operations.

- $[-5, 3] \cap (0, 6] = (0, 3]$
- $(-\infty, 4)^c = [4, \infty)$
- $(-\infty, 5] \cup (5, \infty) = (-\infty, \infty) = \mathbb{R}$
- $((-\infty, -1) \cup (-1, \infty))^c = \{-1\}$
- $(-3, 2) \cap (2, 5) = \emptyset$
- $\{x \in \mathbb{R} : x^2 > 4\}^c = [-2, 2]$

Recall De Morgan's Laws in the context of mathematical logic. We restate them here for convenience:

$$\neg(p \vee q) \iff (\neg p) \wedge (\neg q) \quad \text{and} \quad \neg(p \wedge q) \iff (\neg p) \vee (\neg q)$$

As it happens, there is direct analogy to De Morgan's Laws in logic, to set operations. The following theorem is called De Morgan's Laws for Sets:

Theorem 4.2.1. *(De Morgan's Laws for Sets) Let A and B be sets. Then*

$$(A \cup B)^c = A^c \cap B^c \quad \textit{and} \quad (A \cap B)^c = A^c \cup B^c$$

Proof. We may prove both of these very quickly by using De Morgan's Laws for logic. We will prove the first one together, and the second one will be left to the reader. To set the stage, let p represent the proposition $x \in A$ and q represent the proposition $x \in B$. Then the proposition $x \in (A \cup B)^c$ is precisely the proposition $\neg(p \vee q)$. Using De Morgan's Law, we know $\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$. Translating this into the language of sets

$$x \in (A \cup B)^c \iff (x \notin A) \wedge (x \notin B) \iff x \in A^c \wedge x \in B^c \iff x \in A^c \cap B^c.$$

This means that $x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$. Therefore, $(A \cup B)^c = A^c \cap B^c$ $\square$

5 Lecture - 09/13/2021 and 09/15/2021

5.1 Cartesian Products

Definition. Let A and B be sets. The **Cartesian Product** of A and B is the set

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

We read $A \times B$ as "A cross B".

Example: Let $A = \{1, 2\}$ and $B = \{2, 3, 4\}$ and $C = \{0\}$.

- $A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$
- $B \times C = \{(2, 0), (3, 0), (4, 0)\}$
- $A^2 = A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
- $A \times B \times C = \{(1, 2, 0), (1, 3, 0), (1, 4, 0), (2, 2, 0), (2, 3, 0), (2, 4, 0)\}$
- $A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$
- $A \times \emptyset = A$
- The usual 2-dimensional x, y-plane, is denoted $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\}$

Exercise 5.1.1. Let A, B, and C be sets. Prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Proof. We need to show that if $(x, y) \in A \times (B \cup C)$, then $(x, y) \in (A \times B) \cup (A \times C)$. If $(x, y) \in A \times (B \cup C)$, then $x \in A$ and $y \in B \cup C$. So that $y \in B$ or $y \in C$.

If $y \in B$, then since $x \in A$, $(x, y) \in A \times B$. If $y \in C$, then $(x, y) \in A \times C$. In either case, we would have that $(x, y) \in (A \times B) \cup (B \times C)$. □

Let us rewrite the proof above using mathematical symbols and logic instead. I would recommend reading through both of these and making sure you see the relationship between the two proofs.

Proof. Let A, B, and C be sets. We remind the reader that making an assumption about whether or not $x \in A$, $y \in B$, or $y \in C$ turns all these statements into propositions. Then

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

Here, in the second line, we took advantage of Distributive Law for logic that says if p, q, r are propositions, then $p \wedge (q \vee r) \iff (p \wedge r) \vee (p \wedge r)$. □

As it turns out, our second proof is saying much more than what was required in the exercise. Since we see $\iff$ between all statements in the proof above, it is actually the case that

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

5.2 Binary Relations on Sets

There is often a time when we may want to define a relationship between two sets. These relationships can be whatever we define, a common example is establishing an ordering on a set of real numbers. Establishing these sorts of relationships, with some constraints will give us a powerful tool to better understand many different mathematical objects.

Definition. Let A and B be sets. A **binary relation** from A to B is a subset of the Cartesian product $A \times B$. A binary relation on just one set, A, is a subset of $A \times A$.

There is different notation used to denote relations. Let $\mathcal{R}$ be a relation from A to B. Then to say that $(a, b) \in \mathcal{R}$, one may also write $a\mathcal{R}b$ instead. This would be read as "a is related to b". *Note*: Just because we say "a is related to b", we are not allowed to assume that "b is related to a" even if the language does sound as though it may suggest such a thing.

Examples:

- Let S be the set of students at UD, and C be the set of all possible courses at UD. Then we can define a relation $\mathcal{R}$, that relates a student s to a class c, if student s is enrolled in class c. The coordinate pair $(s, c) \in \mathcal{R} \subseteq S \times C$ is representative of this relation. Do you think it is possible for $\mathcal{R}$ to equal $S \times C$? What would it mean if the equality was true?
- As noted in the start of this section, consider a relation $\mathcal{R}$ on the set of real numbers, $\mathbb{R}$, where $(a, b) \in \mathcal{R} \subset \mathbb{R}^2$ if $a < b$.
  - (True or False?) $(5, 7) \in \mathcal{R}$.
  - (True or False?) $(7, 5) \in \mathcal{R}$.
  - (True or False?) $(5, 5) \in \mathcal{R}$.

Usually, we are more interested in establishing relations on some specific set A. The last example above is just one of many useful relations. Sometimes, relations can come with certain properties that help us understand and impose some sort of structure onto a set. Let us define some of these properties.

Definition. Let A be a set, and $\mathcal{R}$ be a relation on A.

- We say that $\mathcal{R}$ is **reflexive** if $(a, a) \in \mathcal{R}$ for all $a \in A$.
- We say that $\mathcal{R}$ is **symmetric** if $(a, b) \in \mathcal{R}$, implies that $(b, a) \in \mathcal{R}$.
- We say that $\mathcal{R}$ is **anti-symmetric** if $(a, b) \in \mathcal{R}$ and $(b, a) \in \mathcal{R}$, implies $a = b$.
- We say that $\mathcal{R}$ is **transitive** if $(a, b) \in \mathcal{R}$ and $(b, c) \in \mathcal{R}$, implies $(a, c) \in \mathcal{R}$.

Let us study our relation $\mathcal{R}$ on $\mathbb{R}$ given by $<$ and see which of the properties above it satisfied.

Example: Let $\mathbb{R}$ be the set of real numbers and let $\mathcal{R}_<$ be the relation defined by $<$. We will just write $a < b$ to denote that $(a, b) \in \mathcal{R}_<$.

- *Reflexive?* **No**. Let a be any real number, then it certainly is not true that $a < a$. In order for a relation to not be reflexive, the condition of $(a, a) \in \mathcal{R}_<$ needs to fail just *once*. In our example, this condition actually fails for all elements in $\mathbb{R}$. Therefore, $\mathcal{R}_<$ is not a reflexive relation on $\mathbb{R}$.

- *Symmetric?* **No**. Again, we need just a single counterexample. We know $0 < 2$, is it the case that $2 < 0$? Definitely not! As it turns out, $\mathcal{R}_<$ has no elements for which it is symmetric. If $a < b$, then clearly, it cannot be that $b < a$. Therefore $\mathcal{R}_<$ is not a symmetric relation on $\mathbb{R}$.

- *Anti-symmetric?* **Yes**, this is trivially true (you can think of this as "true by default"). Why? Well, we observed in the last point that if $a < b$, then $b < a$ is never true. So that means whenever $(a, b) \in \mathcal{R}_<$, then $(b, a) \notin \mathcal{R}_<$, and so there are no elements in $\mathcal{R}_<$ that require us to verify that the definition of anti-symmetric holds.
  Note: Let us make a quick observation going back to propositional logic. This is a perfect example of why the implication arrow, $p \to q$ is true if the first proposition p is false. In this example, to verify the definition of anti-symmetric for the relation $\mathcal{R}_<$, the mathematical proposition we must evaluate is:

  $$(a < b) \wedge (b < a) \to a = b.$$

  But we just discussed the fact that that there do not exist real numbers a and b where the proposition $(a < b) \wedge (b < a)$ is true. So that means, $(a < b) \wedge (b < a)$ is ALWAYS false, and therefore $(a < b) \wedge (b < a) \to a = b$ is ALWAYS true, which implies that $\mathcal{R}_<$ is anti-symmetric.

- *Transitive?* **Yes**. Let a, b, and c be real numbers, such that $a < b$ and $b < c$. But this means $a < b < c$ so that $a < c$. Therefore, whenever $(a, b) \in \mathcal{R}_<$ and $(b, c) \in \mathcal{R}_<$, then $(a, c) \in \mathcal{R}_<$. Thus, $\mathcal{R}_<$ is a transitive relation on $\mathbb{R}$.

Important: Note that just because a relation is *not symmetric*, this does not automatically imply that the relation is *anti-symmetric*. As a quick example let $A = \{0, 1, 2\}$. Then, $\mathcal{R} = \{(0, 1), (1, 0), (2, 3)\}$ is a relation on A that is in fact neither symmetric, nor anti-symmetric. However, it is not possible for a relation to be both symmetric and anti-symmetric.

Exercise 5.2.1. Which of the above conditions change if we use the relation $\mathcal{R}_\leq$ defined by $\leq$ instead of the relation $\mathcal{R}_<$ defined by $<$ on the set of real numbers $\mathbb{R}$?

Example: Consider the relation $\mathcal{R}_2$ on $\mathbb{Z}$, where $(a, b) \in \mathcal{R}_2$ if $a - b$ is even. Let us see which of the above properties hold for $\mathcal{R}_2$.

- *Reflexive*: **Yes**. Let $a \in \mathbb{Z}$. Since $a - a = 0$ is even for any $a \in \mathbb{Z}$, then $\mathcal{R}_2$ is reflexive.

- *Symmetric*: **Yes**. Let $a, b \in \mathbb{Z}$. Suppose that $a - b$ is even, then $b - a = -(a - b)$ must also be even since multiplying by (-1) does not change the parity of a number. So $\mathcal{R}_2$ is symmetric.

- *Anti-symmetric*: **No**. Since $\mathcal{R}_2$ is symmetric, then it cannot also be anti-symmetric. As a counter-example, consider that $(4,6) \in \mathcal{R}_2$ and $(6,4) \in \mathcal{R}_2$, but it is not the case that $6 = 4$. So $\mathcal{R}_2$ is *not* anti-symmetric.

- *Transitive*: **Yes**. Suppose that $a - b$ is even, and that $b - c$ is even. We wish to show that as a result $a - c$ is also even. Notice that $a - c = (a - b) + (b - c)$. By assumption, both $a - b$ and $b - c$ were even. The sum of two even numbers is again even, therefore $a - c$ is also even. Thus, $\mathcal{R}_2$ is transitive.

This example can be generalized in the following sense: Observe that given two integers a and b, then $a - b$ being even means that $a - b$ is divisible by two and consequently can be written as $a - b = 2k$ for some integer k. There is nothing particularly special about the number two here. So we leave the reader with the following exercise. Its solution follows very closely to the solution of the above example.

Exercise 5.2.2. Let $\mathcal{R}_n$ be a relation on $\mathbb{Z}$ defined by $(a,b) \in \mathcal{R}_n$ if $a - b$ is divisible by n.

Example: Let $\mathcal{L}$ be the set of all lines in $\mathbb{R}^2$, the standard x, y-plane. Consider the relation $\mathcal{R}_\parallel$ on $\mathcal{L}$, defined by $(\ell, k) \in \mathcal{R}_\parallel$ if ℓ is parallel to k, denoted $\ell \parallel k$. Determine whether $\mathcal{R}_\parallel$ is reflexive, symmetric, anti-symmetric, or transitive on $\mathcal{L}$.

- *Reflexive*: **Yes**. Let ℓ be a line in $\mathbb{R}^2$. Two lines in $\mathcal{L}$ are parallel if they have the same slope. Clearly any line ℓ has the same slope as itself, so $\ell \parallel \ell$. Therefore, $(\ell, \ell) \in \mathcal{R}_\parallel$ for every line $\ell \in \mathcal{L}$.

- *Symmetric*: **Yes**. Suppose k and ℓ are lines $\mathcal{L}$ such that $k \parallel \ell$, meaning ℓ and k have the same slope. But that also means, $k \parallel \ell$. So if $(\ell, k) \in \mathcal{R}_\parallel$, then $(k, \ell) \in \mathcal{R}_\parallel$. Thus, $\mathcal{R}_\parallel$ is symmetric.

- *Anti-Symmetric*: **No**. Since $\mathcal{R}_\parallel$ is symmetric, then it cannot also be anti-symmetric.

- *Transitive*: **Yes**. Suppose that ℓ, k, m are lines in $\mathcal{L}$ such that $\ell \parallel k$ and $k \parallel m$. Since $\ell \parallel k$, then ℓ and k have the same slope. Since $k \parallel m$, then k and m have the same slope. So putting this together, ℓ and k have the same slope, and k and m have the same slope. Therefore, ℓ and m must also have the same slope, and so $\ell \parallel m$. Thus, $\mathcal{R}_\parallel$ is transitive.

Fun Fact: The set of lines of $\mathbb{R}^2$ together with the set of points of $\mathbb{R}^2$ (all coordinate pairs) form what is called an *affine plane* in geometry. Generally, the notion of parallelism need not be defined with slope. One can simply call two lines parallel if they are equal or if they are disjoint (here a line can be considered just as a set of points). This definition can give quick answers to whether or not $\mathcal{R}_\parallel$ is reflexive, symmetric, or anti-symmetric. (Try it!) But showing transitivity requires a bit more work. See if you can come up with a clever solution:

Exercise 5.2.3. Let $\mathcal{L}$ be the set of all lines in $\mathbb{R}^2$, and let $\mathbb{R}^2$ be the set of all points. The relationship between lines and points satisfy the following two axioms:

(i) Any two distinct points lie on a unique line.

(ii) Given a line ℓ and a point P, there exists a unique line k parallel to ℓ containing P.

We say ℓ is parallel to k, if either $\ell = k$ or ℓ is disjoint from k. Using only these two axioms, prove that $\mathcal{R}_\parallel$ as defined in the example above, is transitive. (*Hint*: Use axiom (*ii*))

6 Lecture - 09/17/2021

6.1 Equivalence Relations

This lecture is dedicated to exploring a specific type of relation on sets, called an *equivalence relation*. Equivalence relations permeate all fields of mathematics. As we will see, equivalence relations allow us to impose structure on sets that will inform us greatly about the general relationship between elements in the set.

Definition. An **equivalence relation** is a relation that is *reflexive, symmetric, and transitive*. We usually denote an equivalence relation by $\sim$ instead of $\mathcal{R}$.

Example: Let A be the set of all people on Earth. Let $\mathcal{R}$ be a relation on A such that person a is related to person b if person a has the same parent as person b. We may write this as:

$$\mathcal{R} = \{(a, b) \in A \times A : a \text{ and } b \text{ have the same parents.}\}$$

Every person a has the same parents as themselves, so $(a, a) \in \mathcal{R}$ for all $a \in A$. If a and b have the same parents, then b and a must as well. So $(a, b) \in \mathcal{R}$ implies that $(b, a) \in \mathcal{R}$. If a and b have the same parents, and b and c have the same parents, then a and c must also have the same parents. Thus $(a, b) \in \mathcal{R}$ and $(b, c) \in \mathcal{R}$ implies that $(a, c) \in \mathcal{R}$. This shows that $\mathcal{R}$ is reflexive, symmetric, transitive, and therefore is an equivalence relation.

Recall the example $\mathcal{R}_2$ on the set of integers $\mathbb{Z}$ in the previous lecture. We said that under this relation, $(a, b) \in \mathcal{R}_2$ if $a - b$ was even. We went through each property and demonstrated that in fact, $\mathcal{R}_2$ is reflexive, symmetric, and transitive, and therefore is an equivalence relation on $\mathbb{Z}$. Let us think about this example more intuitively. Can we restate the condition that relates a and b in $\mathbb{Z}$ in a way that is a tad bit more familiar? Notice that if $a - b$ is even, then that tells you precisely that either a and b were both even to begin with *or* a and b are both odd. As it turns out an odd number minus an even number can never be even. So then, under $\mathcal{R}_2$, a is related b under the condition that a and b are of the same *parity*, that is: either both a and b are even, or both a and b are odd. So $\mathcal{R}_2$ splits the set of all integers into two groups: The set of even integers, and the set of odd integers.

Finally, to really hit the point home in the most concrete way possible, consider the relation $=$ on any set A. Note that $=$ is an equivalence relation. Thinking of an equivalence relation as an equality is the most practical way one can think of equivalence relations. Let us verify quickly that $=$ is in fact an equivalence relation.

- *Reflexive?* **Yes**. Since $a = a$ for all a.
- *Symmetric?* **Yes**. If $a = b$, then $b = a$.
- *Transitive?* **Yes**. If $a = b$ and $b = c$, then $a = b = c$ so $a = c$.

Ultimately, equivalence relations allow us to group elements of set together, just in the same way that we already do in our every day lives. However, the difference is, that an equivalence relation is rigorously defined. There is no room for ambiguity in the definition of an equivalence relation.

Definition. Let $\sim$ be an equivalence relation on a set A and let $a \in A$. We call the set of all elements of A that are equivalent to a, the **equivalence class** of a and denote it by $\overline{a}$. Using set notation $\overline{a} = \{b \in A : b \sim a\}$. The set of all *distinct* equivalence classes of A is called the **quotient set** of A mod $\sim$, and is denoted $A/\sim$.

Example: Let A be the set of all people on Earth. Let $\mathcal{R}$, which we will denote by $\sim$, be a relation on A such that person $a \sim b$ if person a has the same parent as person b. Describe the equivalence classes belonging to $A/\sim$? What is the equivalence class that *you* fall into?

By definition, for any person a in our set A, the equivalence class of a is $\overline{a} = \{b \in A : a \sim b\}$. So $\overline{a}$ is the set of all people b who have the same parent as a, so that means an equivalence class of a is the set of all siblings of A.

Example: We recall again the example of the set $\mathbb{Z}$ and the equivalence relation $\mathcal{R}_2$. Denote $\mathcal{R}_2$ by $\sim_2$. Then the distinct equivalence classes of $\mathbb{Z}/\sim_2$ are precisely the sets of all odd numbers and even numbers. So under $\sim_2$, the equivalence classes of $\mathbb{Z}$ are:

- $\overline{1} = \{\text{Set of all odd integers.}\} = \{\ldots, -3, -1, 1, 3, \ldots\} = \{2k+1 : k \in \mathbb{Z}\} := 2\mathbb{Z}+1$.
- $\overline{4} = \{\text{Set of all even integers.}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{2k : k \in \mathbb{Z}\} := 2\mathbb{Z}$.
- $\overline{17} = \overline{1}$.
- $\overline{10000} = \overline{4}$.
- $\mathbb{Z}/\sim_2 = \{2\mathbb{Z}, 2\mathbb{Z}+1\}$.

Notice that another way to describe the equivalence classes obtain from $\mathcal{R}_2$, is that an integer $x \in \mathbb{Z}$, belongs to the equivalence class $\overline{0}$ if the quotient of x by 2 has remainder 0. Similarly, if the quotient of x by 2 has remainder 1, then $x \in \overline{1}$.

Notation: In general, if we wish to denote the subset of all integers whose quotient by some natural number n has remainder r, where $r < n$, we write

$$n\mathbb{Z} + r = \{nz + r : z \in \mathbb{Z}\}.$$

Exercise 5.2.2 in the last section has you show that the relation $\mathcal{R}_n$ on the set of integers $\mathbb{Z}$ defined by $(a, b) \in \mathcal{R}_n$ if n divides $a - b$, is actually an equivalence relation. The distinct classes of this relation in particular are called *integers modulo* n. These equivalence classes are precisely of the form $n\mathbb{Z} + r$ for some natural number $r < n$. They represent the set of integers whose remainder after being divided by n is r. So if $\sim$ is the equivalence relation $\mathcal{R}_n$, then

$$\mathbb{Z}/\sim = \{n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+n-1\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

We denote $\mathbb{Z}/\sim$ by $\mathbb{Z}_n$. Let's do a few examples:

Example: Let $\sim_5$ be the equivalence relation on $\mathbb{Z}$ defined by $a \sim_5 b$ if $a - b$ is divisible by 5. Describe the set $\overline{2}$. Describe $\mathbb{Z}/\sim_5$.

Solution. To understand $\overline{2}$, we must understand for which integers b, we have that $b \sim_5 2$. Now, $b \sim_5 2$ if and only if $b - 2$ is divisible by 5. Meaning there exists an integer k such that $b - 2 = 5k$, and therefore, $b \sim_5 2$ if and only if $b = 5k + 2$. Following the if and only if

statements backwards, we see that any integer of the form $5k+2$ is related to 2 under $\sim_5$, and therefore $\overline{2} = 5\mathbb{Z}+2$ under $\sim_5$.

We can follow the same argument above to see that there are a total of 5 equivalence classes of $\mathbb{Z}$ under $\sim_5$, they are $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$, and they can be completely described by the remainder of an integer after being divided by 5. In particular

$$\mathbb{Z}/\sim = \mathbb{Z}_5 = \{5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

We now will prove out first theorem using the proof technique called *proof by contradiction*. Generally speaking, a proof of this form goes in the following manner. We are given two propositions, p and q. We are given that p is true, and we want to show that q is true. What we do is we assume for a contradiction that q is *not true*. So we now have two propositions, that we are claiming are true, p and $\neg q$. We now use both of these facts to show a logical contradiction that is a result of holding both of these facts as true. This will mean that q *must* be true.

Theorem 6.1.1. *Let A be a set, and suppose that $\sim$ is an equivalence relation on A. Let $a, b \in A$ be elements such that $\overline{a} \neq \overline{b}$. Then $\overline{a}$ and $\overline{b}$ are disjoint.*

Proof. Here, the proposition p is that $\overline{a}$ and $\overline{b}$ are two *distinct* equivalence classes of $A/\sim$. Proposition q is that $\overline{a}$ and $\overline{b}$ are disjoint. We will now assume that p is true and $\neg q$ is true, and as a result, find a logical contradiction:

So suppose that $\overline{a}$ and $\overline{b}$ are two *distinct* equivalence classes of $A/\sim$ (this is proposition p) and that $\overline{a}$ and $\overline{b}$ are *not* disjoint, and therefore, there exists an element $x \in \overline{a} \cap \overline{b}$ (this is proposition $\neg q$). We will now proceed to contradict the fact that $\overline{a} \neq \overline{b}$.

Let $z \in \overline{b}$, since $x \in \overline{a}$ by assumption, then $x \sim z$. Similarly, $a \sim x$ because $x \in \overline{a}$. Therefore $a \sim x \sim z$, and by the transitive property of equivalence relations, $a \sim z$. Since $a \sim z$, then $z \in \overline{a}$. Since z was an arbitrary element of $\overline{b}$, this shows that if $z \in \overline{b}$ then $z \in \overline{a}$ and so $\overline{b} \subseteq \overline{a}$.

Now suppose $y \in \overline{a}$. As $x \in \overline{a}$, then $y \sim x$. Since $x \in \overline{b}$, then $x \sim b$. Again by the transitive property, this means $y \sim x \sim b$ and therefore $y \sim b$. This shows that if $y \in \overline{a}$, then $y \in \overline{b}$, so that $\overline{a} \subseteq \overline{b}$.

We have now showed that $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$ implying that $\overline{a} = \overline{b}$, a contradiction. Therefore, proposition $\neg q$ must be false, and so proposition q is true. □

Definition. Let A be a set. We say the sets $A_1, A_2, \ldots, A_n$ **partition** A if and only if the following two conditions hold:

(i) $\bigcup_{i=1}^{n} A_i = A$

(ii) For all i, j, $A_i \cap A_j = \emptyset$.

Theorem 6.1.2. *Let A be a set and $\sim$ is an equivalence relation on A. Then the collection of all equivalence classes of A under $\sim$ partition A.*

Proof. Theorem 6.1.1 proves that condition (ii) of the definition of a partition holds for the collection of all equivalence classes of A under $\sim$. Condition (i) must hold by definition as every element of A must belong to an equivalence class. □

7 Lecture - 09/20/2021

7.1 Functions

We begin this section by giving a concrete and unambiguous definition of a function. You have likely encountered functions in your previous classes, especially in algebra, and calculus courses. Our definition of a function will not be restricted to just functions on the set of real numbers.

Definition. A **function** f from a set A to a set B is a relation from A to B, that satisfies the condition that for *each* $a \in A$, there exists *exactly one* element $b \in B$ (not necessarily unique) such that $(a, b) \in f$.

Example: Let $A = \{1, 2, 3\}$ and $B = \{x, y, z, w\}$. Determine which of the following are functions from A to B.

(i) $f = \{(1, x)\}$

(ii) $f = \{(1, y), (2, x), (3, w)\}$

(iii) $f = \{(1, w), (1, y), (2, z), (3, x)\}$

(iv) $f = \{(1, z), (2, z), (3, z)\}$

Solution. Let's go through each one case by case.

(i) $f = \{(1, x)\}$ is not a function, because f is not defined on the entire set A. There is no coordinate pair with first coordinate 2 or 3.

(ii) $f = \{(1, y), (2, x), (3, w)\}$ is a function, because for each $a \in A$, there exists one $b \in B$ such that $(a, b) \in f$.

(iii) $f = \{(1, w), (1, y), (2, z), (3, x)\}$ is not a function because the element $1 \in A$, has two corresponding elements in f, namely $(1, w)$ and $(1, y)$.

(iv) $f = \{(1, z), (2, z), (3, z)\}$ is a function, again, because it meets the definition. Each element in A has corresponds to exactly one element in B.

Given sets A and B, we often write $f : A \to B$ to denote that f is a function from A to B. We write $f(a) = b$, to denote that $(a, b) \in f$. This same fact can also be denoted by $f : a \mapsto b$.

Definition. Let $f : A \to B$ be a function from A to B.

- The set A is called the **domain** of f. We write $\text{Dom}(f)$ to denote the domain of f.
- The set B is called the **target** of f.
- The set $\text{Rng}(f) = \{b : \exists a \in A \text{ such that } (a, b) \in f\} = \{f(a) : a \in A\}$ is called the **range** of f. The range of f is always a subset of B.
- We say that f is **onto** (or **surjective**) if $\text{Rng}(f) = B$. Meaning that f maps A entirely *onto* B. An equivalent characterization is as follows:

  The function f is *onto* if and only if for every $b \in B$, there exists an $a \in A$, such that $f(a) = b$.

- We say that f is **one-to-one** (or **injective**) if f maps every element of A to a distinct element of b. Meaning that for distinct elements a_1, a_2 in A, $f(a_1) \neq f(a_2)$. Equivalently:

  The function f is *one-to-one* if and only if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$.

- We say that f is **bijective** if f is both one-to-one and onto.

Examples: For each function f below, find $\text{Dom}(f)$, $\text{Rng}(f)$. Then determine if f is one-to-one or onto.

(i) $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $f = \{(1, a), (2, a), (3, c)\}$.

(ii) $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $f = \{(1, c), (2, a), (3, b)\}$.

(iii) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x$.

(iv) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.

Solution. Let us

(i) Here $\text{Dom}(f) = A = \{1, 2, 3\}$ and $\text{Rng}(f) = \{a, c\}$. Since $\text{Rng}(f) \neq B$, then f is not onto. Neither is it one-to-one since $f(1) = a = f(2)$.

(ii) Here $\text{Dom}(f) = A = \{1, 2, 3\}$ and $\text{Rng}(f) = \{a, b, c\} = \text{B}$. Since $\text{Rng}(f) = B$, then f is onto. Since f maps each element in A to a distinct element in B, then f is also one-to-one, and therefore f is bijective as well.

(iii) Here $\text{Dom}(f) = \mathbb{R}$. $\text{Rng}(f) = \mathbb{R}$ as well since, $f = \{(x, x) : x \in \mathbb{R}\}$. Since $\text{Rng}(f) = \mathbb{R}$, then f is onto. Finally f is one-to-one, since using the characterization, we suppose that for some $a_1, a_2 \in \mathbb{R}$, $f(a_1) = f(a_2)$, but be definition of $f(x)$, $a_1 = f(a_1) = f(a_2) = a_2$, so $a_1 = a_2$. Therefore, f is one-to-one.

(iv) Here $\text{Dom}(f) = \mathbb{R}$. $\text{Rng}(f) = [0, \infty)$ because $x^2 \geq 0$ for any real number. The function f is not onto, because the target set is $\mathbb{R}$, but the range does not contain any negative real numbers. Similarly, f is not one-to-one because for any real number x, $f(x) = x^2 = f(-x)$.

In the above example (iii) is an example of what we call an *identity function*.

Definition. Let A be a set and $f : A \to A$ be a function. Then f is called the **identity function** on A if $f = \{(a, a) : a \in A\}$. We will denote the identity function on the set A by I_A.

Exercise 7.1.1. Prove that for any set A, the identity function on A is bijective.

Exercise 7.1.2. Suppose that A is a set that contains 3 elements and B is a set that contains 4 elements. Suppose that $f : A \to B$ is a function from A to B and $g : B \to A$ is a function from $B \to A$. Is it possible for f to be onto? Is it possible for g to be onto? Is it possible for f to be one-to-one? Is it possible for g to be one-to-one? Why? How can this be generalized?

Exercise 7.1.3. Suppose that A and B are sets that both contain n elements. Suppose $f : A \to B$ is a function. Prove that f is onto if and only if f is one-to-one. Thereby showing that under such circumstances, if f is one-to-one or onto, then f must be bijective.

8 Lecture - 09/22/2021

8.1 Inverse Functions

Definition. Let A and B be sets and $f : A \to B$ be a bijective function. Then, the **inverse** of f, is a function $f^{-1} : B \to A$ that is also bijective, and defined:

$$f^{-1} = \{(b, a) : (a, b) \in f\}.$$

That is, $f^{-1}(b) = a$ if and only if $f(a) = b$.

Example: Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z, w\}$. Determine whether the following functions have an inverse, and if they do, determine the inverse function.

(i) $f = \{(1, x), (2, y), (3, z), (4, w)\}$.

(ii) $f = \{(1, x), (2, y), (3, y), (4, x)\}$

Solution. Here the function f in (i) does have an inverse. On the ther hand, the function f in (ii) does not have an inverse.

(i) $f^{-1} = \{(x, 1), (y, 2), (z, 3), (w, 4)\}$

(ii) The function f is not a bijection since f contains both $(1, x)$ and $(4, x)$, therefore $f(1) = f(4)$ so f is not one-to-one.

Example: Let us now consider some functions on various common sets that we use. Suppose that the following functions are bijective functions, find the inverse function.

(i) Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x + 2$, find f^{-1}.

(ii) Let $f : [0, \infty) \to [0, \infty)$ be defined by $f(x) = x^2$, find f^{-1}.

Solution. There are many different ways we can solve for inverses. We will proceed as follows:

(i) If $f(x) = x + 2$, then to find the inverse function, we observe that $x = I_{\mathbb{R}}(x) = (f \circ f^{-1})(x) = f(f^{-1}(x)) = f^{-1}(x) + 2$. This means, we must solve $x = f^{-1}(x) + 2$ for $f^{-1}(x)$. Clearly, $f^{-1}(x) = x - 2$ here.

(ii) Following similar steps as above, we solve for $x = f^{-1}(x)^2$. Since our domain and range are $[0, \infty)$, then $f^{-1}(x) = \sqrt{x}$.

8.2 Composition of Functions

Definition. Let $f : A \to B$ and $g : B \to C$ be functions. The **composition** of g and f is the function $g \circ f : A \to C$ defined by $(g \circ f)(a) = g(f(a))$.

Example: Let $A = \{a, b, c\}$, $B = \{x, y\}$, and $C = \{u, v, w\}$. Suppose that

$$f = \{(a, x), (b, y), (c, x)\}, \quad g = \{(x, u), (y, w)\}.$$

Find $g \circ f$.

Solution. Then, note we have $f(a) = x$, $f(b) = y$, $f(c) = x$, $g(x) = u$, and $g(y) = w$. So

$$(g \circ f)(a) = g(f(a)) = g(x) = u$$
$$(g \circ f)(b) = g(f(b)) = g(y) = w$$
$$(g \circ f)(c) = g(f(c)) = g(x) = u$$

Therefore,

$$g \circ f = \{(a, u), (b, w), (c, u)\}.$$

Example: Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be defined by

$$f(x) = x^2 + 1, \quad g(x) = 3x + 2.$$

That is we may think of these functions as follows:

$$f = \{(x, x^2 + 1) : x \in \mathbb{R}\}, \quad g = \{(x, 3x + 2) : x \in \mathbb{R}\}.$$

(i) Find $g \circ f$. (ii) Find $f \circ g$.

Solution. Since both the domain and target sets of f and g are both $\mathbb{R}$, then we can find both $g \circ f$ and $f \circ g$.

(i) We have that $(g \circ f)(x) = g(f(x)) = g(x^2 + 1) = 3(x^2 + 1) + 2 = 3x^2 + 5$.

(ii) Likewise, $(f \circ g)(x) = f(g(x)) = f(3x + 2) = (3x + 2)^2 + 1 = 9x^2 + 12x + 5$.

The above example demonstrates that it need not be the case that $g \circ f = f \circ g$. In fact, this is almost never the case with arbitrary functions f and g.

Definition. Two functions f and g are *equal* if and only if they have the same domain, same target set, and $f(a) = g(a)$ for all a in the common domain.

Exercise 8.2.1. Let $f : A \to B$ be a bijective function. Show that $(f^{-1})^{-1} = f$.

Proposition 8.2.1. *Let $f : A \to B$ and I_A be the identity function on A and I_B be the identity function on B, then*

$$I_B \circ f = f \circ I_A = f.$$

Proof. Observe that by definition of an identity function,

$$(I_B \circ f)(x) = I_B(f(x)) = f(x) = f(I_A(x)) = (f \circ I_A)(x)$$

proving our assertion. □

Proposition 8.2.2. *Composition of functions is an associative operation. That is, $f \circ (g \circ h) = (f \circ g) \circ h$, where $f : A \to B$, $g : B \to C$, and $h : C \to D$ are any functions.*

Proof. Let $a \in A$, we must show that $(f \circ (g \circ h))(a) = ((f \circ g) \circ h)(a)$. We have

$$(f \circ (g \circ h))(a) = f((g \circ h)(a)) = f(g(h(a))) = (f \circ g)(h(a)) = ((f \circ g) \circ h)(a).$$

Since a was arbitrary, then this proves that composition is an associative operation. □

Proposition 8.2.3. *Let $f : A \to B$ and $g : B \to A$. Then f and g are inverses if and only if $f \circ g = I_B$ and $g \circ f = I_A$.*

Proof. Since the statement is an *"if and only if"*, we must prove the implication in both directions. We first suppose that f and g are inverses, that is $f = g^{-1}$ and $g = f^{-1}$.

Let $b \in B$. Since f and g are inverses, then $(f \circ g)(b) = (f \circ f^{-1})(b)$. By definition of an inverse function, we know that $f^{-1}(b) = a$ if and only if $f(a) = b$. Then $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$. Since $b \in B$ was arbitrary, this means that $(f \circ f^{-1})(b) = b$ for all $b \in B$, and therefore $(f \circ f^{-1})(b) = I_B$, is the identity function on the set B.

Similarly, we may show that since f and g are inverses, then $g \circ f = g \circ g^{-1} = I_A$ using the same train of thought.

Now we suppose that $f \circ g = I_B$ and $g \circ f = I_A$ and we wish to show that f and g are inverses. Notice

$$f \circ g = I_B \to (f \circ g) \circ g^{-1} = I_B \circ g^{-1} = g^{-1}.$$

Since composition is an associative property, then $(f \circ g) \circ g^{-1} = f \circ (g \circ g^{-1}) = f \circ I_A = f$. Therefore $f = g^{-1}$. Using Exercise 8.2.1, we have that

$$f^{-1} = (g^{-1})^{-1} = g,$$

completing the proof. □

Proposition 8.2.4. *Let $f : A \to B$ and $g : B \to A$ be functions, then $g \circ f = I_A$ if and only if $f \circ g = I_B$.*

Example: Show that functions $f : \mathbb{R} \to (1, \infty)$ and $g : (1, \infty) \to \mathbb{R}$ defined by:

$$f(x) = 3^{2x} + 1, \quad g(x) = \frac{1}{2} \log_3(x - 1)$$

are inverses.

Solution. By Proposition 8.2.4, we only need to check $f \circ g = I_{\mathbb{R}}$. If this is the case, then the functions must be inverses. Let $x \in \mathbb{R}$, then

$$(f \circ g)(x) = f(g(x)) = 3^{2(\frac{1}{2}\log_3(x-1))} + 1 = 3^{\log(x-1)} + 1 == (x - 1) + 1 = x.$$

Thus $f \circ g$ is the identity function on $\mathbb{R}$, and therefore f and g are inverses.

9 Lecture - 9/24/2021 and 9/27/2021

9.1 One-to-One Correspondence

Definition. We say that two sets A and B are in **one-to-one correspondence** if there exists a bijection mapping A to B.

This definition is important because it gives us a way to compare the *sizes* of sets. While the word size makes intuitive sense, in particular, when sets contain a finite amount of elements, this intuition can fail when sets do not have a finite amount of elements. We will use the word *cardinality* instead of size, which we will define in shortly. For the next definition, recall our special notation, $[n] = \{1, 2, \ldots, n\}$.

Definition. A **finite** set is a set that is either empty, or is in one-to-one correspondence between the set $[n]$ for some natural number N. A set that is not finite, is called **infinite**. We define the **cardinality** of the empty set to be 0, and the cardinality of a set A that is in one-to-one correspondence with $[n]$ for some natural number n, to have **cardinality** n, denoted $|A| = n$.

As mentioned, in the finite case, this connects well with our intuition. In essence, this definition just informs us that when we have a. finite set, then we can count them and assign a label to the elements in the set them from 1 to n.

Examples: What are the cardinalities of the following sets?

- $|\{1, 2, 6, 93403475\}| = 4$
- $|\{\emptyset\}| = 1$
- $|\{a, b\}| = 2$
- $|\emptyset| = 0$

Definition. We say that two sets A and B have the same cardinality and we write $|A| = |B|$ if and only if A and B are in one-to-one correspondence.

Discussing the cardinality infinite sets, I would recommend tossing out all the intuition we might have about our real world experience. In the next example, we will show that the set of all integers has the same cardinality as the set of all even integers. Intuitively, it seems that all the even integers should make up just "half " of the total amount of integers, and yet, this is not the case.
Example: Show that $\mathbb{Z}$ and $2\mathbb{Z}$ have the same cardinality.

Solution. To demonstrate that $\mathbb{Z}$ and $2\mathbb{Z}$ have the same cardinality, all we need to do is find a bijection that maps $\mathbb{Z}$ to $2\mathbb{Z}$ (or the other way around). How might one do this?

Consider the function $f : \mathbb{Z} \to 2\mathbb{Z}$, defined by $f(x) = 2x$. If we can show that this function is a bijection, from $\mathbb{Z}$ to $2\mathbb{Z}$, then we would have established a one-to-one correspondence between the sets, implying these sets have the same cardinality.

To check whether f is one-to-one, we suppose that there exists integers x_1, x_2, such that $f(x_1) = f(x_2)$. By assummption,

$$2x_1 = f(x_1) = f(x_2) = 2x_2 \to 2x_1 = 2x_2 \to x_1 = x_2.$$

Therefore, f must be one-to-one.

To see that f is onto, we just need to verify that every element in the target set of f has a corresponding element in the domain of f that maps to it. Every element in $2\mathbb{Z}$, takes on the form $2z$ for some integer $z \in \mathbb{Z}$. Then note that $f(z) = 2z$ and since $z \in \mathbb{Z}$, which is the domain of f, then f is onto.

Thus f is a bijection. Thus, $|\mathbb{Z}| = |2\mathbb{Z}|$.

Exercise 9.1.1. Show that the sets $\mathbb{N}$ and $\mathbb{N} \cup \{0\}$ have the same cardinality. Show that $\mathbb{N} \cup \{0\}$ and $\mathbb{Z}$ have the same cardinality.

Example: Show that $(0, 1)$ and $(0, \infty)$ have the same cardinality.

Solution. Let $f(x) = -\ln x$. We want to show that $f(x)$ is a bijection from $(0,1)$ to $(0,\infty)$. To check if $f(x)$ is one-to-one: Suppose that for some $x_1, x_2 \in (0,1)$ such that $f(x_1) = f(x_2)$. Then

$$-\ln x_1 = f(x_1) = f(x_2) = -\ln x_2 \to \ln x_1 = \ln x_2 \to \ln x_1 - \ln x_2 = 0.$$

Using, laws for logarithms, we note $0 = \ln x_1 - \ln x_2 = \ln(x_1/x_2)$. But $\ln(x) = 0$ only has one solution, namely $x = 1$. That means that $x_1/x_2 = 1$ so that $x_1 = x_2$. Therefore, f is one-to-one.

To see that f is onto, suppose that $y \in (0,\infty)$. Consider then $x = e^{-y}$. Note that since $y > 0$, then $-y < -0$ so that $e^{-y} < 1$. It is also the case that exponentials are always positive so this implies that $e^{-y} \in (0,1)$ which is the domain of f. Finally we see

$$-\ln e^{-y} = -(-y)\ln e = y,$$

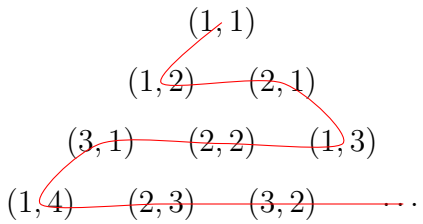
implying that f is onto. So f is a bijection, and therefore, $(0,1)$ and $(0,\infty)$ have the same cardinality.

Definition. We say that a set A is **countably infinite** if and only if $|A| = |\mathbb{N}|$ and we say that A is **countable** if A is either finite or countable infinite. Otherwise, we say that A is **uncountable**. If a set A is countable infinte we denote it's cardinality with $|A| = \aleph_0$, pronounced "Aleph Naught".

The rest of the material we will cover in this lecture has been beautifully illustrated on YouTube many times. I recommend watching the following link to get wonderful visuals. You can also simply google, 'Hilbert's Hotel" to read more about this.

Theorem 9.1.1. *Prove that* $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Proof. Although generally, a 'proof by picture" is not a valid proof, in this case we can heavily utilize a wonderful illustration to get the point across. We want to show that we can assign to each order pair $(x, y) \in \mathbb{N} \times \mathbb{N}$ and cover all possible ordered pairs. In the following figure, imagine that the red curve is an infinitely long string to which each ordered pair is attached, and it continues on in the same fashion for all ordered pairs:



Imagine now that we pull on the end of this string and straighten it out, so that now each ordered pair will line up nicely next to some natural distinct number n as follows:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	$\cdots$
$(1,1)$	$(1,2)$	$(2,1)$	$(1,3)$	$(2,2)$	$(3,1)$	$(1,4)$	$(2,3)$	$(3,2)$	$\cdots$

In this manner, each natural number n will get assigned to exactly one ordered pair. In fact, we can develop a formula that mimics this assignment of ordered pairs to natural numbers

In fact, we can even give an explicit formula that will solve our problem for us exactly, here it is, $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by

$$f(m,n) = \frac{1}{2}(m+n)(m+n-1) + (n-1).$$

We will leave it as an exercise for the reader to prove that f is in fact a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. To convince yourself, check that the above figure of the straightened out string corresponds with this $f(m,n)$. For example, notice

$$f(3,1) = \frac{1}{2}(3+1)(3+1-1) + (1-1) = \frac{1}{2}(4)(3) + (0) = 6,$$

and we see that in the figure $(3,1)$ lines up with **6**. □

We end this section with an ingenious proof of the fact that $\mathbb{R}$ or more generally, any interval of $\mathbb{R}$ is an uncountable set. The following argument is known as "Cantor's Diagonalization Argument". It proceeds as a proof by contradiction.

Theorem 9.1.2. *The interval $(0,1) \subset \mathbb{R}$ is uncountable.*

Proof. If we wish to show that in fact the interval $(0,1)$ is an uncountable set, then we will instead assume it is countable, and demonstrate a contradiction. If $(0,1)$ was a countable set, then to each real number in $(0,1)$ we may correspond with a natural number. Note that if $x \in (0,1)$, then it takes on the form of an infinite decimal, that may or may not be repeating, so

$$x = 0.a_1a_2a_3a_4\ldots$$

where a_i are digits from 0-9. Then we can put all the whole numbers n side by side with the numbers that they correspond to. As an example, perhaps the first few decimals are as follows:

$\mathbb{N}$	Decimals in $(0,1)$
1	$0.\boxed{4}576801\ldots$
2	$0.5\boxed{6}98409\ldots$
3	$0.89\boxed{1}0234\ldots$
4	$0.6710\boxed{0}89\ldots$
$\vdots$	$\ldots$

Considered the boxed values corresponding to each number. For the number corresponding to 1, we box the first decimal digit, for the number corresponding to 2, we box the second decimal digit, and so on. Consider then a decimal, whose n^{th} decimal digit is *not* equal to the boxed value/ So that means we build a decimal whose first decimal digit is not equal to 4, second decimal digit not equal to 6, and so on. For example, we take $x = 0.2345\ldots$ Notice that this x is in $(0,1)$ but it does not correspond to any value of $n \in \mathbb{N}$. Why not? If the decimal we built is a decimal value already in our table that corresponds to some number n, then that would be a contradiction! Because we specifically built our decimal to not have the same n^{th} decimal digit as the decimal that corresponds to n. Therefore, $(0,1)$ is uncountable. □

10 Lecture - 10/04/2021

10.1 The Division Algorithm

We begin this section by concretizing some properties of real numbers, $\mathbb{R}$, and the relation $\leq$ on $\mathbb{R}$. The following properties may seem almost obvious, but it is important that we know precisely what we can and what we can't do with real numbers.

Definition. We call a relation $\mathcal{R}$ on a set A a **partial order**, if the relation is *reflexive*, *anti-symmetric*, and *transitive*.

Recall that $\leq$ defined a partial order on $\mathbb{R}$.

Theorem 10.1.1. *Let a, b and c be real numbers. Then*

1. *$\mathbb{R}$ is **closed** under addition and multiplication, meaning that $a + b$ and $a \cdot b$ are both real numbers.*
2. *Addition and multiplication are **commutative** operations on $\mathbb{R}$, meaning that $a + b = b + a$ and $ab = ba$.*
3. *Addition and multiplication are **associative** operations on $\mathbb{R}$, meaning that $(a+b)+c = a + (b + c)$ and $a(bc) = (ab)c$.*
4. *$\mathbb{R}$ has an **additive identity** (0 in this case) and a **multiplicative identity** (1 in this case), meaning that $a + 0 = a$ and $a \cdot 1 = a$.*
5. *The **distributive property** holds in $\mathbb{R}$, meaning that $a(b+c) = ab+ac$ and $(a+b)c = ac + bc$.*
6. *Every element $a \in \mathbb{R}$ has an **additive inverse**, namely $-a$, so that $a + (-a) = 0$.*
7. *Every element $a \in \mathbb{R}$ with $a \neq 0$, has a **multiplicative inverse**, namely $1/a$, so that $a \cdot (1/a) = 1$.*
8. *If $a \leq b$, then $a + c \leq b + c$.*
9. *If $a \leq b$ and $c \geq 0$, then $ac \leq bc$.*
10. *If $a \leq b$ and $c \leq 0$, then $ac \geq bc$.*

The following is a principle we take for granted and use on a regular basis, even in our every day lives. It allows us to say a lot about natural numbers and integers alike, as we will see in the coming pages.

Well-Ordering Principle: Any nonempty set of natural numbers has a smallest element.

By application of the Well-Ordering principle, we can prove what we have in fact understood to be true since grade school. You probably learned to divide two whole numbers with a remainder early on in child hood, but how do we know that there is only one solution to the problem of dividing two whole numbers with a remainder? This is exactly what we will prove to be true.

Theorem 10.1.2. *Given natural numbers a and b, there exists unique non-negative integers q and r with $r < b$ such that $a = bq + r$.*

Proof. Consider the sequence of natural numbers $b, 2b, 3b, \ldots$. The consider only a subset of this sequence of all multiples of b that are greater than a. By the well-ordering principle, this set will have a least element, and we can call it $(q+1)b$. But that means then that $qb < a < (q+1)b$. Let $r = a - qb$. and notice that since $a < (q+1)b$, then $a - qb < (q+1)b - qb = b$. Finally, $qb + r = qb + (a - qb) = a$. Therefore, we found non-negative integers q and r as claimed.

We now want to demonstrate that this q and r are unique. To prove this, we will instead assume by contradiction that they are not unique. That is, we suppose that there are two distinct pairs of non-negative integrs q_1, r_1 and q_2, r_2 with both $r_1 < b$ and $r_2 < b$ satisfying

$$q_1 b + r_1 = a = q_2 b + r_2 \to q_1 b + r_1 = q_2 b + r_2 \to (q_1 - q_2)b = r_2 - r_1.$$

Now, since both $r_1 < b$ and $r_2 < b$, then note that $-b < r_2 - r_1 < b$. But the left hand side above is a multiple of b. So the only way this is possible is if $q_1 - q_2 = 0$, otherwise we would have a contradiction. So if $q_1 - q_2 = 0 \to q_1 = q_2$, then that would mean

$$r_2 - r_1 = (q_1 - q_2)b = 0 \to r_1 = r_2.$$

But this again a contradiction, because it implies that the pair q_1, r_1 was *not* distinct from q_2, r_2. Therefore, there exist *unique* non-negative integers q and r such that $a = bq + r$. □

In light of the theorem above, we can give special names to the values q and r as they are unique.

Definition. If a and b are natural numbers and q, r are non-negative integers with $r < b$ such that $a = qb + r$, then we call the integer q the **quotient** and the integer r the **remainder** of a *divided* by b.

Exercise 10.1.1. Determine the following.

- Find the quotient q and remainder r, of 17 divided by 5.
- Find the quotient q and remainder r, of 193 divided by 11.

We now extend the result above to the set of all integers $\mathbb{Z}$. We do have to be a little more careful with the precise statement of theorem as it is possible that either a or b may be negative in the division.

Theorem 10.1.3. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists unique integers q, r with $0 \leq r < |b|$ such that $a = bq + r$.*

Proof. Note that if $a = 0$, then it is clear that that the only possible solution to $a = bq + r$ is that $q = r = 0$. Otherwise, we are left with four cases to consider

(i) $a > 0$ and $b > 0$. (ii) $a < 0$ and $b > 0$. (iii) $a > 0$ and $b < 0$. (iv) $a < 0$ and $b < 0$.

The first case is precisely the statement of Theorem 10.1.3.

To tackle Case (ii), observe that $a < 0$ implies that $-a > 0$. Then we can apply Theorem 10.1.3 to $-a$ and b to obtain that there are unique non-negative integers q and $0 \leq r < b$ such that $-a = bq + r$. We now negate the entire equation to obtain $a = -bq - r = b(-q) + (-r)$. If $r = 0$, then we are done, since the quotient would be $-q$ and $r = 0$. If $r > 0$, then the problem is that $-r < 0$. To fix this, observe that

$$a = b(-q) + (-r) = b(-q) - b + b + (-r) = b(-q - 1) + (b - r)$$

where now $0 \leq b - r < b = |b|$.

Cases (iii) and (iv) follow similarly. If $a > 0$ and $b < 0$, then note that $-b > 0$, so applying Theorem 10.1.3 to a and $-b$, we obtain $q = q(-b) + r = (-q)b + r$. Since $-q$ is just another integer, and r remained unaffected, and therefore $0 \leq r < -b = |b|$, then this is a valid solution.

If $a < 0$ and $b < 0$, then a and $-b$ turn into Case (ii), and therefore again $a = (-b)q + r = b(-q) + r$.

This shows existence in all four cases. The proof for uniqueness follows in exactly the same way as it did in the proof of Theorem 10.1.3. This can all be done as one case. □

Exercise 10.1.2. Determine the following. How are the answers different from Exercises 10.1.1?

- Find the quotient q and remainder r, of -17 divided by 5.
- Find the quotient q and remainder r, of 193 divided by -11.

We now introduce two special functions on the set of real numbers $\mathbb{R}$.

Definition. Let $x \in \mathbb{R}$.

- The **floor function** $\lfloor x \rfloor = y$ outputs the closest integer y to x that is *less* than x.
- The **ceiling function** $\lceil x \rceil = y$ outputs the closest integer y to x that is *greater* than x.

Proposition 10.1.1. *If a, b are integers with $a = qb + r$ where q, r are integers and $0 \leq r < |b|$, then*

$$q = \begin{cases} \lfloor \frac{a}{b} \rfloor & \text{if } b > 0 \\ \lceil \frac{a}{b} \rceil & \text{if } b < 0. \end{cases}$$

Make sure that you understand this fact and are able to use it. Take a look at Exercises 10.1.1 and 10.1.2 and apply this proposition there.

11 Lecture 10-6-2021

11.1 Representing Natural Numbers in Various Bases

One particularly important consequence of the Division Algorithm is that there are *unique* ways of representing whole numbers in different *bases*. The standard way in the modern world for representing natural numbers is in base 10. However, as any computer scientist will tell you, there isn't any real reason that this system is *better* than others. In fact, there may be reasons that other bases are better. The way we do math today is simply a consequence of eons of history and mathematical development.

We often don't stop to think about many of the the things we consider natural or obvious. For example, the idea of negative numbers appeared in many cultures in the early centuries of the common era, they did not appear or become commonly used in Europe until after the 15th century. Another example is the succinct way in which we write our algebraic equations. Equations containing x and y is a very recent invention developed by European mathematicians. Before that much algebra was done writing out entire words for the unknown variable x. The same goes for the various symbols we use for addition, subtraction, etc. On the other hand, much of the actual mathematics of algebra was developed by Arabic mathematicians over a thousand years ago. In the 9th century, Muhammad ibn Musa al-Khwarizmi wrote a text titled "Kitab Al-Jabr", which is exactly where the name "algebra" comes from. Likewise, the symbols we use to represent our usual decimal digits are in fact Arabic numerals: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0$. The history of mathematics is a fascinating topic I would recommend every reader to spend some time studying.

Definition. Given a fixed natural number $b > 1$, the *base b representation* of a natural number N is the expression $(a_{n-1}a_{n-2}\dots a_1a_0)_b$, where $a_0, a_1, \dots, a_{n-1}$ are integers satisfying $0 \leq a_i < b$ that satisfy

$$N = (a_{n-1}a_{n-2}\dots a_1a_0)_b = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1b + a_0.$$

This is precisely what we mean when we base 10. For example, let $N = 1805$, then

$$1805 = (1805)_{10} = 1 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 5.$$

Observe that when we write

$$N = (a_{n-1}a_{n-2}\dots a_1a_0)_b = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1b + a_0.$$

then the sum above that represent N is really the rule for converting a number *from base b to base 10*. How about converting numbers the other way? This is where we implicitly take use of the Division Algorithm.

Let N and $b > 1$ be natural numbers. By the division algorithm, observe that there exist unique non-negative integers q_0 and a_0 such that:

$$N = q_0b + a_0.$$

If $q_0 \neq 0$, we can apply the division algorithm to obtain non-negative integers q_1 and a_1 such that

$$q_0 = q_1b + a_1 \to N = q_0b + a_0 = (q_1b + a_1)b + a_0 = q_1b^2 + a_1b + a_0.$$

If $q_1 \neq 0$ we can apply this process again to obtain a q_2 and a_2 so that

$$q_1 = q_2 b + a_2 \to N = (q_2 b + a_2)b^2 + a_1 b + a_0 = q_2 b^3 + a_2 b^2 + a_1 b + a_0.$$

We keep this up until we obtain a $q_n = 0$. Let's do a few examples.

Example: Find the base 2 representation of 4567.

Solution. Let us follow the process outlined above.

$$\begin{aligned}
4567 &= (2283) \cdot 2 + 1 \\
2283 &= (1141) \cdot 2 + 1 \\
1141 &= (570) \cdot 2 + 1 \\
570 &= (285) \cdot 2 + 0 \\
285 &= (142) \cdot 2 + 1 \\
142 &= (71) \cdot 2 + 0 \\
71 &= (35) \cdot 2 + 1 \\
35 &= (17) \cdot 2 + 1 \\
17 &= (8) \cdot 2 + 1 \\
8 &= (4) \cdot 2 + 0 \\
4 &= (2) \cdot 2 + 0 \\
2 &= (1) \cdot 2 + 0 \\
1 &= (0) \cdot 2 + 1
\end{aligned}$$

The process terminates when we see $(0) \cdot 2$, or more generally, $(0) \cdot b$. Now we read the red from the bottom up. The above equations allow us to conclude that:

$$4567 = 1 \cdot 2^{12} + 0 \cdot 2^{11} + 0 \cdot 2^{10} + 0 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$4567 = (1000111010111)_2$$

Some bases have special names. Base 2 representation of a number is called the **binary** representation. Base 8 is called **octal** and base 16 is called **hexadecimal**. When a number exceeds 10, then we need more numerals since we have to also represent $10, 11, 12, 13, 14, 15$ as single digits. In particular for hexadecimal, the standard assignment is

- $10 = A$
- $11 = B$
- $12 = C$
- $13 = D$
- $14 = E$
- $15 = F$

Example: Find the base 16 representation of 4567.

Solution.

$$\begin{aligned}
4567 &= (285) \cdot 16 + 7 \\
285 &= (17) \cdot 16 + 13 \\
17 &= (1) \cdot 16 + 1 \\
1 &= (0) \cdot 16 + 1
\end{aligned}$$

Therefore,

$$4567 = 1 \cdot 16^3 + 1 \cdot 16^2 + 13 \cdot 16^1 + 7 \cdot 16^0 = (11D7)_{16}.$$

12 Lecture 10-08-2021

12.1 Divisibility

Definition. Given integers a and b, with $b \neq 0$, we say that b is a **factor** or a **divisor** of a and that a is **divisible** by b if and only if $a = qb$ for some integer q. We write $b|a$ to signify that a is divisible by b, and we say "b divides a".

The above definition implies that an integer a is divisible by an integer b precisely when the remainder of a divided by b is 0.

Proposition 12.1.1. *The following holds for any integer z.*

- $z|0$
- $1|z$

Exercise 12.1.1. Prove that if a is an integer, then exactly one of the numbers in the sequence $a, a+1, a+2$ is divisible by 3.

Solution. By the division algorithm, there exist unique integers q and r such that $a = 3q+r$ where $0 \leq r < 3$. This means that $a+1 = 3q+(r+1)$ and $a+2 = 3q+r+2$. There are only three possible choices for r, namely $0, 1$ or 2. If $r = 0$, then $a = 3q$ so that a is divisible by 3. If $r = 1$, then $a+2 = 3q+1+2 = 3(q+1)$ is divisible by 3. If $r = 2$, then $a+1 = 3a+2+1 = 3(q+1)$ is divisible by 3. Thus, no matter what r is, either $a, a+1$, or $a+2$ must be divisible by 3.

Theorem 12.1.1. *Divisibility defines a partial order on $\mathbb{N}$. That is, if $\mathcal{R}$ is the relation that $(a,b) \in \mathcal{R}$ if and only if $a|b$, then $\mathcal{R}$ is reflexive, anti-symmetric, and transitive.*

Proof. We must prove that $\mathcal{R}$ is reflexive, anti-symmetric, and transitive.

Reflexive: $\mathcal{R}$ is symmetric if $(a,a) \in \mathcal{R}$. Meaning $(a,a) \in \mathcal{R}$ if and only if $a|a$. Note that $a = 1 \cdot a$, and therefore by definition of divisibility a divides a, so $\mathcal{R}$ is reflexive.

Anti-Symmetric: Suppose that $(a,b) \in \mathcal{R}$ and $(b,a) \in \mathcal{R}$. This means that $a|b$ and $b|a$. Therefore, there exists an integer q_1 such that $b = q_1 a$, and there exists an integer q_2 so that $b = q_2 a$. Together, this gives us

$$b = q_2 a = q_2(q_1 b) = (q_2 q_1)b.$$

But that means that $q_2 \cdot q_1 = 1$ in order for the equality to hold. Since $a, b \in \mathbb{N}$ and therefore are positive, then it must be that $q_2 = q_1 = 1$ so that $b = a$. This proves that $\mathcal{R}$ is anti-symmetric.

Transitive: Suppose that $(a,b) \in \mathcal{R}$ and $(b,c) \in \mathcal{R}$, we wish to show that $(a,c) \in \mathcal{R}$. This means that assuming that $a|b$ and $b|c$, we wish to show that $a|c$. Since $a|b$, then $b = q_1 a$ for some integer q_1. As $b|c$, then $c = q_2 b$ for some integer q_2. This means

$$c = q_2 b = q_2(q_1 a) = (q_2 q_1)a.$$

Since q_1, q_2 are integers, then $q_1 q_2$ is also an integer, and so $a|c$. Thus $\mathcal{R}$ is transitive, and in total, $\mathcal{R}$ is a partial order. □

Proposition 12.1.2. *Suppose that a, b, c are integers such that $c|a$ and $c|b$, then for any integers x, y, we have that $c|(ax + by)$.*

Proof. Suppose that $c|a$ and $c|b$. This means $a = q_1c$ and $b = q_2c$ for some integers q_1 and q_2. Then note that $ax = q_1cx = (q_1x)c$ and $by = q_2cy = (q_2y)c$. This implies that $c|ax$ and $c|by$. Observe that $ax + by = (q_1x)c + (q_2y)c = (q_1x + q_2y)c$. Since $q_1x + q_2y$ is another integer, this implies that $c|(ax + by)$. □

12.2 Greatest Common Divisor and the Euclidean Algorithm

Definition. Let a, b both be integers, not both zero. An integer g is the **greatest common divisor** (**GCD**) of a and b if and only if

- $g|a$ and $g|b$.
- If c is an integer such that $c|a$ and $c|b$, then $c \leq g$.

We write $g = \gcd(a, b)$ to indicate that g is the GCD.

Examples: Show that:

- $\gcd(5, 7) = 1$.
- $\gcd(21, 14) = 7$
- $\gcd(a, b) = |a|$ if and only if $a|b$.
- In particular, $\gcd(a, 0) = |a|$.

As it turns out, there is a specific algorithm one can follow to determine the GCD of two numbers. This is precisely the algorithm your computer would follow to find the GCD of two integers. Before introducing the algorithm, we prove a lemma that will help establish the why the algorithm works and that it does in fact terminate for any pair of integers a and b.

Lemma 12.2.1. *If $a = qb + r$ for integers a, b, q, r, then $gcd(a, b) = gcd(b, r)$.*

Proof. The trivial cases are when $a = b = 0$, and $b = r = 0$. In both of these cases we obtain $a = b = r = 0$. We need to deal with these first since $\gcd(0, 0)$ is not defined. Otherwise, GCD is well-defined and we proceed as follows.

Let $g_1 = \gcd(a, b)$ and $g_2 = \gcd(b, r)$. Note that $g_2|b$ and $g_2|r$ which by Proposition 12.2.2 implies that $g_2|(qb + r)$. Since $a = qb + r$, then $g_2|a$. Thus $g_2|a$ and $g_2|b$ then by defintion of $\gcd(a, b)$, $g_2 \leq g_1$.

Now, observe that if $a = bq + r$, then $a - bq = r$. By Proposition 12.2.2 g_1 divides $a - qb = r$, so that $g_1|r$ as well as $g_1|b$. Therefore, by definition of $\gcd(b, r)$, $g_1 \leq g_2$.

This brings us to $g_1 \leq g_2 \leq g_2$, and therefore $\gcd(a, b) = g_1 = g_2 = \gcd(b, r)$. □

The Euclidean Algorithm: Let a and b be natural numbers with $b < a$. To find the greatest common divisor of a and b, write

$$a = q_1b + r_1, \quad \text{with } 0 \leq r_1 < b.$$

Now we apply Lemma 12.1.1 over and over until the process terminates.

If $r_1 \neq 0$, then since $\gcd(a, b) = \gcd(b, r_1)$, write $b = q_2 r_1 + r_2$, where $0 \leq r_2 < r_1$.
If $r_2 \neq 0$, then since $\gcd(b, r_1) = \gcd(r_1, r_2)$, write $r_1 = q_3 r_2 + r_3$, where $0 \leq r_3 < r_2$.
If $r_3 \neq 0$, then since $\gcd(r_1, r_2) = \gcd(r_2, r_3)$, write $r_2 = q_4 r_3 + r_4$, where $0 \leq r_4 < r_3$.
Since the r_k's are getting progressively smaller, then we know this process will terminate with some $r_{k+1} = 0$. Then, the GCD of a and b will be given by r_k since

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

Let's do some examples.

Example: Find the GCD of 36 and 81.

$$\begin{aligned} 81 &= 2(36) + 9 \\ 36 &= 4(9) + 0 \end{aligned}$$

Therefore, the GCD of 36 and 81 is 9. It will always be the remainder that appears in the equation before the one that has remainder 0.

Example: Find the GCD of 630 and 196

$$\begin{aligned} 630 &= 3(196) + 42 \\ 196 &= 4(42) + 28 \\ 42 &= 1(28) + 14 \\ 28 &= 2(14) + 0 \end{aligned}$$

Therefore, the GCD of 630 and 196 is 14.

13 Lecture 10/11/2021

Definition. Two nonzero integers a and b are said to be **relatively prime** if and only if $\gcd(a, b) = 1$.

Exercise 13.0.1. Show that $17,369$ and $5,472$ are relatively prime.

13.1 Linear Combinations

An important consequence of the Euclidean Algorithm, is that we can use the algorithm to find integers m and n such that $am + bn = \gcd(a, b)$. Furthermore, $am + bn$ is always a multiple of $\gcd(a, b)$. Given integers a and b, we call an equation of the form $am + bn$ an **integral linear combination** of a and b. As a result we have the following theorem, though we will not go through a rigorous proof of it.

Theorem 13.1.1. *Let a and b be integers. If $g = \gcd(a, b)$, then there exist integers m and n such that $am + bn = \gcd(a, b)$*

The following proposition shows how the above theorem can be applied. We are now entering a place where the proofs will begin to really pull results from multiple places, and we will have to maneuver each piece to fit it into the right slot. A good method for starting

any proof, *even when doing a scratch work proof*, is to list **all** of the assumptions given in the problem and write out what these assumption tell us. Let us carefully go through this process with the following proof.

Proposition 13.1.1. *Suppose a, b and x are all integers such that $a|bx$. If a and b are relatively prime, $a|x$.*

Proof. What are the assumptions given in this problem? Let us list them, and then let us write out what we would like to show. We are given that:

- $a|bx$ meaning that there exists a $c \in \mathbb{Z}$ such that $ac = bx$.
- a and b are relatively prime, meaning that $\gcd(a, b) = 1$, and therefore, there exist integers m and n such that $am + bn = 1$ by the theorem above.

We would like to show that:

- $a|x$ meaning that there exists an integer d such that $ad = x$.

Let m and n be integers such that $am + bn = 1$. Then note that we can multiply both sides by x to obtain $amx + bnx = x$. Since we know that there exists an integer x such that $ac = bx$, then we have that

$$x = amx + bnx = amx + (bx)n = amx + (ac)n = a(mx + cn).$$

We know that $mx + cn$ is just another integer, so we can denote $d = mx + cn$, so that $x = ad$ and therefore, $a|x$. □

The above proof could be written much more succinctly, but as we get further into deeper mathematics, the proofs will become more involved, so it is important to learn to write proofs *correctly*. As one of my own professors once told me, *"A proof is only a proof when it is correct."*

Proposition 13.1.2. *The GCD of two nonzero integers a and b is divisible by every common divisor of a and b.*

Proof. Let $g = \gcd(a, b)$. Therefore, there exist two integers m and n such that $am + bn = g$. Suppose that c is a common divisor of a and b, then c divides any integral linear combination of a and b, meaning $c|(ab + bn)$, meaning $c|g$. □

13.2 Lowest Common Multiple

Definition. If a and b are nonzero integers, we say that ℓ is the **least common multiple** (LCM) of a and b and write $\ell = \text{lcm}(a, b)$ if and only if ℓ is a positive integer satisfying:

- $a|\ell$ and $b|\ell$
- If m is any positive integer such that $a|m$ and $b|m$, then $\ell \leq m$.

Proposition 13.2.1. *Let a and b be integers, then*

$$\gcd(a, b) \cdot lcm(a, b) = |ab|.$$

14 Lecture 10-13-2021

14.1 Prime Numbers

One of the most important topics in this course is this section: prime numbers. Questions about primes are usually very simple to understand, but very hard to answer. Not so long ago, Number Theory was believed to be one of the most pure fields of mathematics, in the sense that it had almost no application to the real world. Mathematicians throughout the centuries studied the phenomena of prime numbers, never knowing what all this work would accumulate to being one of the most fundamental parts of our everyday lives. All of our modern day encryption relies on ciphers which in turn rely on prime numbers. We will touch a bit more on all of this in more detail later, but first, let us give a definition of prime numbers.

Definition. A natural number $p \geq 2$ is called **prime** if and only if the only natural numbers that divide p are 1 and p. A natural number n that is not prime is called **composite**. A composite number n can be written as the produce of two natural numbers $a > 1$ and $b > 1$, meaning $n = ab$.

Examples: Are the following numbers prime or composite: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12?

- **Prime**: 2, 3, 5, 7, 11
- **Composite**: 4, 6, 8, 9, 10, 12

There are many question that one can generate about primes that may be relatively simple to ask. Are there infinitely many primes? Is there a formula or function $f(n)$ so that n maps to the nth prime number? Is there a fast and efficient algorithm to tell if a number is prime or not? And so on. The more we know about primes, the more questions it seems that we are left with. Fortunately, not all these questions are as difficult as they might seem, though there are many still awaiting to be answered. We will first prove that there are infinitely many primes with a proof that was known to Euclid, who lived during the 4th and 3rd centuries B.C. in Alexandria.

Lemma 14.1.1. *Given any natural number $n > 1$, there exists a prime p such that $p|n$.*

Proof. Suppose that the lemma is false, and therefore there exists a natural number that is not divisible by any prime. This implies that the set of all numbers not divisible by any prime is non-empty, and so by the Well Ordering Principle, we have that this set contains a least element, call it m. m cannot be prime, since $m|m$ is always true. So that means m is composite, and therefore, there exists a natural number $a > 1$ such that $a|m$. Since $a < m$, then a is not in the set of all number not divisible by any prime. Therefore, there exists a prime p such that $p|a$. But then, by transitivity, since $p|a$ and $a|m$, then $p|m$, a contradiction. □

Theorem 14.1.1. *There are infinitely many primes.*

Proof. We will proceed with proof by contradiction.Suppose that there is only a finite number of primes, so that we can list them all out. Suppose $p_1, p_2, \ldots, p_k$ is the full list of all the prime numbers. Note then that the number

$$n = p_1 p_2 \cdots p_k + 1$$

is a natural number, and so is divisible by a prime by the lemma above. But since $p_1, p_2, \ldots, p_k$ is the full list of all primes, then there exists some natural number $1 \leq i \leq k$ such that $p_i | n$. By definition , $p_i | p_1 p_2 \cdots p_k$ as well. This means that p_i divides any linear combination of n and $p_1 p_2 \cdots p_k$, in particular,

$$p_i | (n - p_1 p_2 \cdots p_k) \rightarrow p_i | 1.$$

This is a contradiction, since every prime is greater than 1. □

Now that we know there are infinitely many primes, one may want to know if there a formula that can predict when primes occur. Or is there at least a formula which can output only primes, though perhaps not all of them? As of right now, there is no formula that can reliably, or predictably, produce a list of prime numbers. Finding a formula like this would most definitely win you the Fields Medal, which is the mathematicians version of the Nobel Prize. But there are many questions that have stood the test of time for centuries. Here are some examples:

Goldbach's Conjecture: For every even natural number $2n$, there exist two primes p and q such that $p + q = 2n$.

Twin Prime Conjecture: There exist infinitely many primes p such that $p + 2$ is also a prime.

Legendre's Conjecture: For every natural number n, there exists a prime between n^2 and $(n + 1)^2$.

Each of these problems have been around for at least a century or two. Though we have much computational evidence to support these conjectures, no proof is yet known of any of them.

We now discuss a method for finding primes. This method was known to the Greeks. It is called the *Sieve of Eratosthenes*. Start with the first number, 2. Then we color it red, and proceed to cross out all multiples of 2, so we cross out, 4, 6, 8, 10, . . . , etc.

2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11
~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~	21

Then, move to the next number after 2 that hasn't been crossed out yet, 3. Color 3 red, and then proceed to crossing out all other multiples of 3, so cross out 6, 9, 12, 15, . . . , etc.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11
~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~

Then we go again, find the next number after 3 that has yet to be crossed out, 5. Color it red, then cross out all other multiples of 5, so cross out 10, 15, 20, 25, etc.. This process is what we call the Sieve of Eratosthenes. We are left with the primes in red:

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11
~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~

Lemma 14.1.2. *If a natural number n is composite, then then n is divisible by a prime $p \leq \sqrt{n}$.*

Proof. Since n is composite, we may write $n = ab$ a product of two natural numbers $a > 1$ and $b > 1$. Suppose that $a \leq b$. Note that $a \leq \sqrt{n}$. If this were not the case, then we would have that $\sqrt{n} < a \leq b$, which would imply that

$$n = \sqrt{n}\sqrt{n} < ab = n \to n < n$$

a contradiction. Therefore $a \leq \sqrt{n}$. By Lemma 14.1.1, there exists a prime p that divides a, and so by transitivity, $p|a$ and $a|n$ implies that $p|n$ and $p \leq a \leq \sqrt{n}$. □

Proposition 14.1.1. *Suppose that p is a prime such that $p|ab$, then $p|a$ or $p|b$.*

Proof. Recall that in the last lecture, we proved that if $p|ab$ and p and a are relatively prime, then $p|b$. Since p is a prime, then either $p|a$ or p is relatively prime with a, and therefore we obtain that either $p|a$ or $p|b$. □

Corollary. *If $p|a_1a_2 \cdots a_k$, then there exists an i, $1 \leq i \leq k$ such that $p|a_i$.*

Theorem 14.1.2 (The Fundamental Theorem of Arithmetic)**.** *Every natural number $n \geq 2$ can be written uniquely in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

where each p_i is a distinct prime and each e_i is a natural number.

Proof. First we note that every number can in fact be written at least one way as a product of powers of primes. To prove this, we suppose that this is not the case, and therefore, the set of natural numbers that cannot be written as a product of powers of primes is non-empty. By the well ordering principle, this set has a a least element, so call this element m. By Lemma 14.1.1, there exists a prime p, that divides m. Let $n = m/p$. Since $n < m$, then n does not belong to the set of natural number that cannot be written as a product of powers of primes, and therefore we can say $n = p_1^{e_1} \cdots p_k^{e_k}$, but that means that

$$m = p \cdot n = pp_1^{e_1} \cdots p_k^{e_k}.$$

We leave the uniqueness portion for the reader to prove. Assume for a contradiction that there are two different ways to write a natural number n as a product of distinct powers of primes, what would that mean? □

Definition. The **prime factors** or **prime divisors** of an integer $n \geq 2$ are the prime numbers that divide n. The largest power e, such that $p^e|n$ is called the **multiplicity** of a prime divisor p of n.

Examples: Find the prime factorization of the following: 16, 600, 61.

15 Lecture 10-18-2021

We have a few more things to mention about primes, and the rest of this section will be dedicated to working through some example problems.

We introduce the prime counting function, $\pi(x)$ which outputs precisely the numbers of primes that there are less than or equal to x. For example, $\pi(5) = 3$, since prime less than or equal to 5 are $2, 3$, and 5.

Exercises: Find $\pi(10)$, $\pi(20)$, $\pi(100)$. *Hint*: To find $\pi(100)$, use the Sieve of Eratosthenes and only cross out number that are multiples of primes that are less than $\sqrt{100} = 10$. $\pi(10) = 4$, $\pi(20) = 8$, $\pi(100)$

The following theorem is one of the most important results in number theory.

Theorem 15.0.1. *Let $\pi(x)$ be the prime counting function. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1, \quad \textit{equivalently} \quad \pi(x) \sim \frac{x}{\ln x}$$

The above theorem states that the amount of primes $p \leq x$ is about $/\ln x$. If time permits, we may discuss a "elementary proof" of the prime number theorem due to Erdós and independently by Selberg around the same time. As you can imagine, the fact that they both came up with this proof at the same time caused quite the dispute between the two mathematicians.

But before we will attempt to tackle the above, there is a result that we can prove as long as we are familiar with series. Again, we will cover a proof of this twoards the end of the course.

Theorem 15.0.2. *The following summation is divergent:*

$$\sum_{p \text{ prime}} \frac{1}{p}.$$

One of the most famous theorem of all time, if Fermat's Last Theorem. Fermat, who lived during the mid 1600's scribbled once in a book that he had a " truly marvelous proof" of the fact that there are no nonzero integer solutions to the equation $a^n + b^n = c^n$ for $n \geq 3$. To this day, no one knows what this *marvelous* proof was, and the problem remained unsolved until 1993. The proof was over 100 pages long.

Theorem 15.0.3. *Let $n \geq 3$ be a natural number. Then, there are no non-zero integers a, b, c such that*

$$a^n + b^n = c^n.$$

Exercise 15.0.1. Use the Fundamental Theorem of Arithmetic to prove that for every natural number n, the the last digit (the ones) place of 12^n is *not* 0.

Exercise 15.0.2. Show that the sum of two consecutive primes is never twice a prime.

Exercise 15.0.3. Prove that every odd positive integer of the form $3n+2$ has a prime factor of the same form. Then prove that there are infinitely many primes of the form $3k + 2$.

16 Lecture 10-20-2021

16.1 Congruence

In Lecture 6, (Chapter 2 in the book), we introduced a special equivalence relation on the set of integers. Let $\mathcal{R}_n$ be the relation on $\mathbb{Z}$ defined by $(a, b) \in \mathcal{R}_n$ if $n|(a-b)$. We showed that $\mathcal{R}_n$ defines an equivalence relation on $\mathbb{Z}$. Furthermore, we determined that the equivalence classes of $\mathbb{Z}$ modulo $\mathcal{R}_\backslash$ are precisely given by

$$\mathbb{Z}_n = \{n\mathbb{Z}, n\mathbb{Z}+1, n\mathbb{Z}+2, \ldots, n\mathbb{Z}+(n-1)\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

We called the $\mathbb{Z}_n$ the set of integers modulo n. In particular, we had that

$$n\mathbb{Z} + r = \{nz + r : z \in \mathbb{Z}\}$$

is the set of all integers whose remainder after being divided by n is r.

Definition. Let $n > 1$ be a fixed natural number. Given integers a and b, we say that "*a is congruent to b modulo n*", ("a is congruent to b mod n"), if and only if $n|(a-b)$. We use the notation $\equiv$ to denote congruence. In particular if $n|(a-b)$, then we write $a \equiv b \pmod{n}$.

Proposition 16.1.1. *Let a, b and n be integers with $n > 1$. Then the following statements are equivalent:*

1. $n|(a-b)$
2. $a \equiv b \pmod{n}$
3. $a \in \overline{b}$
4. $b \in \overline{a}$
5. $\overline{a} = \overline{b}$.

Proof. Two statements are *equivalent* when we can place an "if an donly if" statement between them. In the case of proving multiple equivalences, there are some short cuts we can take. For example, in the above, if we show that (1) $\to$ (2) $\to$ (3) $\to$ (4) $\to$ (5) $\to$ (1), then we do not need to prove for example that (2) $\to$ (1) because we can follow the string of implications from (2) down the list to see that (2) implies (1).

Let us begin the proof.

- (1) $\to$ (2): If $n|(a-b)$, then by definition $a \equiv b \pmod{n}$
- (2) $\to$ (3): If $a \equiv b \pmod{n}$, then , by definition a is related to b and so $a \in \overline{b}$.
- (3) $\to$ (4): If $a \in \overline{b}$, then $a \equiv b \pmod{n}$ which implies $b \equiv a \pmod{n}$ so that $b \in \overline{a}$
- (4) $\to$ (5): We have proven before that equivalence classes are either equal or disjoint. (4) implies that $a \in \overline{a} \cap \overline{b}$, and therefore, $\overline{a}$ and $\overline{b}$ are not disjoint, so it must be that $\overline{a} = \overline{b}$.
- (5) $\to$ (1): If $\overline{a} = \overline{b}$, then $a \equiv b \pmod{n}$, so $n|(a-b)$.

□

Although we associate an equivalence to every integer, as we have seen, that for $\mathbb{Z}$ modulo n, there are exactly n equivalence classes. They can be represented using the classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. It is customary to then think of $\mathbb{Z}_n$ as just the set $\{0, 1, 2, \ldots, n-1\}$ where each element $a \in \mathbb{Z}$ corresponds to $r \in \mathbb{Z}_n$ if the remainder of a after being divided by n is r, in this case we say that $a \pmod{n}$ is r.

We now prove a final proposition to demonstrate that we can perform computations in $\mathbb{Z}_n$ using **modular arithmetic**. To give an intuitive basis for this sort of thing, think about the difference between using say military time, and our standard 12 hour clock. If in California it is 11am, then in military time, we say it is 11:00. However, at the same time, New York is 3 hours ahead, so the time in New York is 14:00 in military time. But what time is that using the standard 12 hour clock? Well, we divide by 12, and obtain a remainder of 2, and so we say it is 2pm in New York when it is 11am in California. This sort of arithmetic is well defined and we will prove that this is the case.

Proposition 16.1.2. *Let $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$. Then,*

- $a + b \equiv x + y \pmod{n}$
- $ab \equiv xy \pmod{n}$

Proof. First we show that $a+b \equiv x+y \pmod{n}$. Note that this is the case if $n|(a+b-(x+y))$. Observe that $n|(a-x)$ and $n|(b-y)$, so then n divides any linear combination of $(a-x)$ and $(b-y)$, so in particular n divides $(a-x)+(b-y) = (a+b)-(x+y)$. Therefore, $a + b \equiv x + y \pmod{n}$.

Now we show that $ab \equiv xy \pmod{n}$. Note that this is the case if and only if $n|(ab-xy)$. We may rewrite

$$ab - xy = ab + (ay - ay) - xy = (ab + ay) - (ay - xy) = a(b - y) + (a - x)y.$$

Since we know that $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$, then $n|(a-x)$ and $n|(b-y)$ and so n divides $a(b-y)+(a-x)y = ab-xy$. Therefore $ab \equiv xy \pmod{n}$. □

Exercise 16.1.1. Find the following:

- $17 + 4 \pmod{12}$
- $17 \cdot 4 \pmod{12}$
- $2x \pmod{2}$, $x \in \mathbb{Z}$.

Solution. To find $17 + 4 \pmod{12}$, note $17 + 4 = 21$, and $21 = 1 \cdot 12 + 9$. Since $0 \leq 9 < 12$, then 9 is the remainder, and so in fact $17 + 4 \equiv 9 \pmod{12}$.

To find $17 \cdot 4 \pmod{12}$, not $17 \cdot 4 = 68$. $68 = 5 \cdot 12 + 8$. Since 8 is the remainder, we say $17 \cdot 4 \pmod{12}$ is 8, and write $17 \cdot 4 \equiv 8 \pmod{12}$.

To find $2x \pmod{2}$, note that $2x = 2 \cdot x + 0$. So the remainder of $2x$ modulo 2, is 0. Therefore, $2x \equiv 0 \pmod{2}$.

Exercise 16.1.2. Note that $100 \equiv 1 \pmod{9}$. What is $100^2 \pmod{9}$? What about $100^3 \pmod{9}$? Is there something you can say about $100^n \pmod{9}$ for any $n \in \mathbb{N}$?

Exercise 16.1.3. Find a (one) solution, if possible, for the following: $3x \equiv 1 \pmod{5}$, $3x \equiv 1 \pmod{6}$

17 Lecture - 10-22-2021

Recall that if n is a natural number and a is an integer, then we define $a \pmod n$ to be precisely the remainder r, such that $a = qn + r$ and $0 \leq r < n$. We don't use "equal to" signs when working with modular arithmetic, but rather we use $\equiv$, the equivalence sign.

A particularly powerful consequence of Proposition 16.1.2 above, is that we may quickly determine determine the congruence modulo n of an integer raised to a large power.

Example: Find $2^9 \pmod 7$.

Solution. Note that

$$2^3 = 8 \equiv 1 \pmod 7.$$

This means that

$$2^9 = (2^3)^3 = 8^3 \equiv (1)^3 \pmod 7 \equiv 1 \pmod 7.$$

Example: Find $1575 \pmod 9$.

Solution. Note that $10 \equiv 1 \pmod 9$. This means that $10^n \equiv 1^n \pmod 9 \equiv 1 \pmod 9$ for any natural number n. Observe that

$$1575 = 1{\cdot}10^3{+}5{\cdot}10^2{+}7{\cdot}10{+}5{\cdot}10^0 \equiv 1{\cdot}1^3{+}5{\cdot}1^2{+}7{\cdot}1{+}5{\cdot}1 \pmod 9 \equiv 18 \pmod 9 \equiv 0 \pmod 9$$

More generally, given a number in base 10 whose digits are $a_k a_{k-1} \dots a_1 a_0$ we can write out it's expansion by powers of 10 to obtain

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9.$$

Meaning, a number written in base 10 is divisible by 9 precisely when the sum of it's digits are 0 (mod 9), or equivalently, a number written in base 10 is divisible by 9 precisely when the sum of it's digits is divisible by 9. If the sum of the digits is not divisible by 9, then the number is not divisible by 9. Now you have a cool party trick to show your friends!

Proposition 17.0.1. *Let $n > 1$ be a natural number and a be an integer with $\gcd(a, n) = 1$.*

- *There exists an integer s, such that $sa \equiv 1 \pmod n$.*
- *For any integer b, the congruence $ax \equiv b \pmod n$ has a solution.*
- *The solution to $ax \equiv b \pmod n$ is unique, meaning that if x_1 and x_2 are both such that $ax_1 \equiv b \pmod n$ and $ax_2 \equiv b \pmod n$, then $x_1 \equiv x_2 \pmod n$.*

Proof. Recall that if a and n are relatively prime, meaning $\gcd(a, n) = 1$, then there exist integers s and z, such that $as + nz = \gcd(a, n) = 1$. Then, by Proposition 16.1.2,

$$1 = as + nz \equiv as + 0 \cdot z \pmod n \equiv as \pmod n.$$

Therefore, $as \equiv 1 \pmod n$

If $\gcd(a, n) = 1$, then by the first bullet point, there exists an integer s such that $as \equiv 1 \pmod n$. Note that this also implies that $\gcd(s, n) = 1$ since $as + nz = 1$.

Then $ax \equiv b \pmod n$ implies that $(ax)s \equiv bs \pmod n$ and $(ax)s \equiv x \pmod n$. Therefore $x \equiv bs \pmod n$. Note that this proof solved for x uniquely. □

Definition. Let $n > 1$ be a natural number, and a be an integer such that $\gcd(a, n) = 1$, then we call the integer $s \pmod{n}$ such that $as \equiv 1 \pmod{n}$, then we call s the **multiplicative inverse** and denote $s = a^{-1}$.

Theorem 17.0.1 (Fermat's Little Theorem)**.** *If p is prime and $p \not| c$, then $c^{p-1} \equiv 1 \pmod{p}$.*

Proof. Consider the number $x = 1 \cdot 2 \cdots (p-2) \cdot (p-1)$. Since all the numbers in the product are not divisible by p, then $p \not| x$. Observe that the number

$$c \cdot 2c \cdots (p-2)c \cdot (p-1)c = c^{p-1}x.$$

We claim that the following two set are equivalent mod p:

$$\{c, 2c, 3c, \ldots, (p-2)c, (p-1)c\} = \{1, 2, \ldots, (p-2), (p-3)\} \pmod{p}.$$

First, we note that since $\{1, 2, \ldots, (p-1)\}$ is the set of all possible remainder mod p, and so that means for any $y \in \{1, 2, \ldots, p-1\}$, since $p \not| c$, then $cy \pmod{p} \in \{1, 2, \ldots, p-1\}$. Secondly, we know that if $cy_1 \equiv cy_2 \pmod{p}$, then $y1 \equiv y_2 \pmod{p}$. But we know that every $y \in \{1, 2, \ldots, p-1\}$ is distinct mod p, and so in fact

$$\{c, 2c, 3c, \ldots, (p-2)c, (p-1)c\} = \{1, 2, \ldots, (p-2), (p-3)\} \pmod{p}.$$

But if the sets are equal, then

$$xc^{p-1} \equiv x \pmod{p}$$

which implies that $c^{p-1} \equiv 1 \pmod{p}$, as claimed. □

18 Lecture 10-25-2021

18.1 Mathematical Induction

One fundamental method of proof is *mathematical induction*. For those of you who have taken a few courses in computer science, may recognize quite the similarity between mathematical induction and recursion. The idea of this method of proof is as follows:

Suppose we want to prove that the sum of all numbers starting at 1, up to $2k+1$ is a square. In particular, we want to show that for any natural number n,

$$\sum_{k=1}^{n} 2k - 1 = n^2.$$

Since we are claiming that this equality holds true for every n, then we will want to begin by checking that it actually holds true for the very first case. What choice of n is the very first case? Well, $n = 1$, of course! Is it true that

$$\sum_{k=1}^{1} 2k - 1 = 1^2?$$

It is indeed true, since both the summation and the square are 1. But how do we prove it is true for every single n? We can use the following logic. We can assume that the equality holds true up to $n = m$, can we prove that it must then hold for $n = m + 1$.

Again, we assume that the following equality is true.

$$\sum_{k=1}^{m} 2k - 1 = m^2.$$

Then using the above, we have that

$$\sum_{k=1}^{m+1} 2k - 1 = \sum_{k=1}^{m} 2k - 1 + 2(m+1) - 1 = m^2 + 2m + 1 = (m+1)^2.$$

So if the proposition holds for $n = m$, then it holds for $n = m + 1$. But this finishes the proof! We already verified that the equality is true for $n = 1$, but then that means since it is true for $n = 1$, then it is true for $n = 1 + 1 = 2$. But if it is true for $n = 2$, then the same argument shows that the equality holds for $n = 3$, and so on. Therefore, the equality hods true for all $n \in \mathbb{N}$.

Exercise 18.1.1. Can you come up with a visual proof for the summation above? Think about building squares using blocks.

Principal of Mathematical Induction: Given a statement $\mathcal{P}$ concerning the integer n, suppose that

1. $\mathcal{P}$ is true for some particular integer n_0; (**Base Case**)
2. if $m \geq n_0$ is an integer and $\mathcal{P}$ is true for m, then $\mathcal{P}$ is true for $m + 1$. (**Induction Hypothesis**)

Then $\mathcal{P}$ is true for all $n \geq n_0$.

Exercise 18.1.2. Prove that

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

for all natural numbers $n \in \mathbb{N}$.

Solution. Let us check the base case. Here the first instance we must verify is $n = 1$, since $n \in \mathbb{N}$. Note

$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2},$$

so the statement is true for $n = 1$.

Now, we assume by the induction hypothesis, that the statement is true for some natural number $m \geq 1$. Meaning, we assume that the equality below holds true:

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

Then, note that

$$\sum_{k=1}^{m+1} k = \left(\sum_{k=1}^{m} k\right) + (m+1) = \frac{m(m+1)}{2} + m + .$$

Working through some algrebra, we have:

$$\frac{m^2+m}{2} + m + 1 = \frac{m^2+3m+2}{2} = \frac{(m+1)(m+2)}{2}$$

as desired. Therefore, by the principal of mathematical induction,

$$\sum_{k=1}^{n} = \frac{n(n+1)}{2}$$

for all $n \in \mathbb{N}$.

There is also a visual proof of the above fact. Suppose we want to determine 1+2+3+4+5. Then consider a 6 square, and observe that all the numbers below the red diagonal, sum to exactly $1+2+3+4+5$.

1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1

But there is exactly the same number of 1's above the diagonal. Along the diagonal, there are 6 1's. So in total the square has 6^2 1's, and $6^2 - 6 = 6 \cdot 5$ ones that are not on the diagonal. Since there the same number of ones below and above the diagonal, then $1+2+3+4+5 = 6 \cdot 5/2$. In general, to find $1+2+\cdots .+n$. Build a $(n+1)\times(n+1)$ square, exclude the diagonal, and divide by 2 the remaining number of 1's. So you $[(n+1)^2 - (n+1)]/2 = n(n+1)/2$

Exercise 18.1.3.

$$\sum_{k=1}^{n}(3k^2 - 3k + 1) = n^3$$

for all $n \in N$.

19 Lecture 10-27-21

19.1 Strong Induction

Let us do a few more examples before introducing strong induction.

Exercise 19.1.1. Prove that $n! > 2^n$ for all natural numbers $n > 3$.

Solution. We proceed with a proof by induction. The first case we must verify is the first integer n_0 that satisfies $n_0 > 3$, which is $n_0 = 4$. This will be our base case. For $n = 4$, we have

$$4! = 24 > 16 = 2^4.$$

Therefore, the base case holds. Now we assume that the inequality holds true for $m \geq 4$, we wish to show it holds for $m + 1$. By the induction hypothesis, we know that $m! > 2^m$, then

$$(m + 1)! = m!(m + 1) > 2^m(m + 1) > 2^m \cdot 2 = 2^{m+1}.$$

Thus, by induction, $n! > 2^n$ for all $n \geq 4$.

Exercise 19.1.2. Determine what is wrong in the following proof by induction. The proof claims that

$$2 + 4 + \cdots + 2n = (n - 1)(n + 2)$$

for all natural numbers n.

"Assume that $2 + 4 + \cdots + 2m = (m - 1)(m + 2)$ for some integer m. Then

$$2+4+\cdots+2m+2(m+1) = (m-1)(m+2)+2m+2 = m^2+m-2+2m+2 = m^2+3m = m(m+3)$$

as desired. Therefore, $2 + 4 + \cdots + 2n = (n - 1)(n + 2)$ for all natural numbers n."

Exercise 19.1.3. What change can be made to the equation above to make the equality true for all n?

We now introduce the concept of **strong mathematical induction**. The difference between this version and the regular version is that our induction hypothesis is stronger. In the regular version, the induction hypothesis states:

- If $\mathcal{P}$ is a statement about an integer n and *if $m \geq n_0$ is an integer and $\mathcal{P}$ is true for m*, then $\mathcal{P}$ is true for $m + 1$.

Pay attention to the italicized portion above. The regular version only requires that the induction hypothesis is true for m. In strong induction we assume that the hypothesis is true for all $\ell \leq m$, and want to prove that the statement $\mathcal{P}$ holds for $m + 1$. To state it formally:

Principal of Strong Mathematical Induction: iven a statement $\mathcal{P}$ concerning the integer n, suppose that

1. $\mathcal{P}$ is true for some particular integer n_0; (**Base Case**)
2. if $m \geq n_0$ is an integer and $\mathcal{P}$ is true for all $n_0 \leq \ell \leq m$, then $\mathcal{P}$ is true for $m + 1$. (**Induction Hypothesis**)

Then $\mathcal{P}$ is true for all $n \geq n_0$.

Exercise 19.1.4. A certain store sells envelopes in packages of five and and packages of twelve and you want to buy n envelopes. Prove that for every $n \geq 44$, this store can sell you exactly n envelopes.

Solution. In essence, what we are being asked to show, for any integer $n \geq 44$, we can find non-negative integers x and y such that if we buy x packages of 5 envelopes, and y packages of 12 envelopes, then we would have n envelopes.

In other words, we must show that

$$5x + 12y = n, \quad x, y \geq 0, n \geq 44$$

always has a solution. The base case here is $n = 44$. Let us find a corresponding x and y that give $5x + 12y = 44$. Note $x = 4$ and $y = 2$ is a solution.

Now, suppose that given an integer $m \geq 44$, then for all integers ℓ, $44 \leq \ell \leq m$, that the above equation has a valid solution. We must show that there is a solution for $m + 1$. If $(m + 1) - 5 = \ell \geq 44$, then there exists an x and y such that

$$5x + 12y = \ell.$$

But observe then that

$$5(x + 1) + 12y = 5 + 5x + 12y = 5 + \ell = m + 1,$$

meaning that $m + 1$ has a solution. Our solution only works when $m + 1 \geq 49$, in order for $\ell \geq 44$. That means, we must demonstrate further that actually our base case will consist of demonstrating solutions for $n = 44, 45, 46, 47, 48$. Once we have done so, then we may apply induction to finish the proof.

- $44 = 5(5) + 12(2)$
- $45 = 5(9) + 12(0)$
- $46 = 5(2) + 12(3)$
- $47 = 5(7) + 12(1)$
- $48 = 5(0) + 12(4)$.

Therefore, by induction, we have may always write $n \geq 44$ as $n = 5x + 12y$ for some non-negative integers x and y.

Exercise 19.1.5. Prove the Fundamental Theorem of Arithmetic using strong induction.

Solution. We will show that every integer is either prime or is a product of primes. Note that for $n = 2$, we know that 2 is prime. No suppose by strong induction that that for some m, we have that for all integers ℓ, with $2 \leq \ell \leq m$, is either prime or can be written as a product of primes.

Consider the number $m + 1$, we have shown before that if an integer is not prime, then it is divisible by a prime. If $m + 1$ is prime, then we are done and there is nothing to prove. If $m + 1$ is not prime, then there exists a prime $p|(m + 1)$, so that $\ell = (m + 1)/p$ and $2 \leq \ell < m$. By the induction hypothesis ℓ can be written as a product of primes. This implies that $m + 1 = p \cdot \ell$ can also be written as a product of primes.

Uniqueness of the prime decomposition can be proven separately just like we did before.

20 Lecture 10-29-2021

20.1 Recursively Defined Sequences

In the last couple lectures, we looked at proving equalities, or inequalities using induction. In this section we will be given a *recursive* definition for a sequence of numbers, and we will attempt to guess the sequence, and then use induction that our guess meets the recursive definition. As a simple example, suppose we are given a sequence of terms, $a_1, a_2, a_3, \ldots$ given by the following definition:

$$a_1 = 2, \quad a_{k+1} = 2a_k.$$

Can you guess what exactly the what sequence of number is defined this way? We know that $a_1 = 2$, so the first term should be two. Let's compute a few more and see if we can hypothesize about what the sequence might be.

$$a_1 = 2, \quad a_2 = 2a_1 = 4, \quad a_3 = 2a_2 = 8, \quad a_4 = 2a_3 = 16, \quad \ldots$$

This sequence is looking a lot like $a_n = 2^n$. We can use a quick induction argument to prove that this is the case. The base case is $n = 1$, and we note that $2^1 = 2 = a_1$, so the base case checks out. Then we must verify that 2^n meets the recursive definition that was given. Suppose that $a_n = 2^n$ for some $n \geq 1$, then we must verify that $a_{n+1} = 2a_n$:

$$a_{n+1} = 2^{n+1} = 2 \cdot 2^n = 2a_n.$$

In the above example, we were given that $a_1 = 2$. In general, this is known as the **initial condition** for the recursive sequence. The fact $a_{k+1} = 2a_k$ for this problem is called the **recurrence relation**. Let us do a few more examples.

Exercise 20.1.1. In the following, determine what is the initial condition and what is the recurrence relation. Then determine a formula for the sequence and prove that your formula is correct.

$$a_1 = 1, \quad a_{k+1} = 2a_k + 1.$$

Solution. The initial condition is $a_1 = 1$ and the recurrence relation is $a_{k+1} = 2a_k + 1$. Let us write out the first few terms to see if we can determine a formula.

$$a_1 = 1, \quad a_2 = 3 \quad , a_3 = 7, \quad a_4 = 15, \quad a_5 = 31, \quad \ldots$$

Have you spotted the pattern? It is not so different form our first example. It looks like each term is just one away from a power of two, so we guess.

$$a_n = 2^n - 1.$$

To prove this formula is correct, we check the base case, which is, $a_1 = 2^1 - 1 = 1$. Now we verify that our formula satisfies the recurrence relation:

$$a_{n+1} = 2^{n+1} - 1 = (2^{n+1} - 2) + 1 = 2(2^n - 1) + 1 = 2a_n + 1$$

as required.

Exercise 20.1.2. Let $a_1 = 1$ and $a_{k+1} = 5k + 1$. Determine a formula for the sequence.

Solution. The first few terms are

$$a_1 = 1, \quad a_2 = 6, \quad a_3 = 31, \quad a_4 = 156, \quad \ldots.$$

It might not be immediately clear as to what this sequence is, but perhaps we can rewrite the first few terms in a way that is more useful. We have

$$a_1 = 1, \quad a_2 = 5a_1 + 1 = 5 + 1, a_3 = 5a_2 + 1 = 5(5 + 1) + 1 = 5^2 + 5 + 1$$

can you guess the form that a_4 takes. It will follow the same pattern:

$$a_4 = 5a_3 + 1 = 5(5^2 + 5 + 1) + 1 = 5^3 + 5^2 + 5 + 1.$$

So, we guess that

$$a_n = 5^{n-1} + 5^{n-2} + \cdots + 5 + 1 = \frac{1}{4}(5^n - 1).$$

The right hand side is just a more compact way of writing the sum of terms on the left, but the key is that the formula on the left is correct. Let us prove that this is so.

For $n = 1$, our formula gives $(5^1 - 1)/4 = 1$, and so the base case checks out. Now observe that

$$a_{n+1} = 5^n + 5^{n-1} + \cdots + 5 + 1 = 5(5^{n-1} + 5^{n-2} + \cdots + 5 + 1) + 1 = 5a_n + 1.$$

We now mention some particular sequences.

Definition. Let $a_1 = a$ and let $d \in \mathbb{Z}$ such that

$$a_{k+1} = a_k + d.$$

Such a sequence is called an **arithmetic sequence**. The number d is called the **common difference** of the sequence.

Exercise 20.1.3. Let a_n be an arithmetic sequence with initial condition $a_1 = a$ with common difference d. Prove that

$$a_n = a + (n - 1)d$$

and

$$\sum_{i=1}^{n} a_i = \frac{n}{2}(2a + (n - 1)d).$$

The following sequence was defined by Fibonacci after his observation of how the population of rabbits was growing. Under ideal circumstance, the population would follow the following sequence.

Definition. Let $f_0 = 1$ and $f_1 = 1$. Then define $f_{k+1} = f_k + f_{k-1}$. This sequence is called the **fibonacci sequence**.

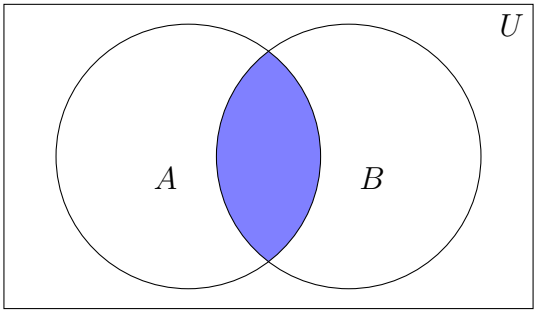
Proposition 20.1.1. *Let f_n be the fibonacci sequence, then*

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1 - \sqrt{5}}{2}\right)^n.$$

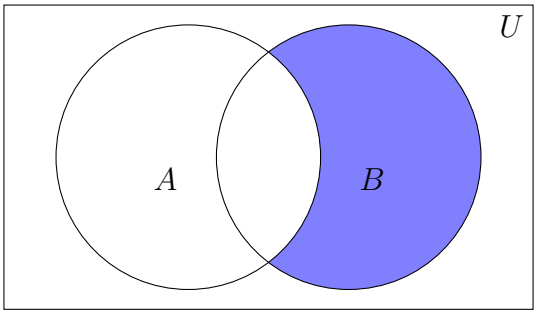
21 Lecture - 11/1/2021

21.1 Principle of Inclusion-Exclusion

Let A and B be sets. Consider the following shading of the Venn Diagram of A and B. How could we represent the cardinality of the shaded region?



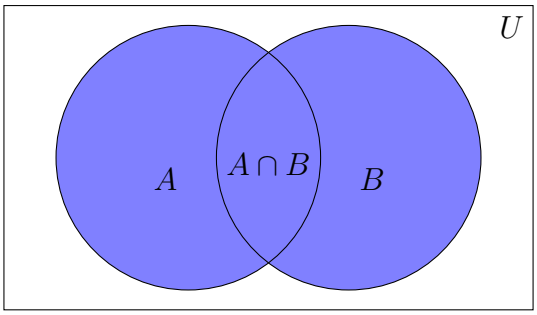
The shaded region is precisely the set of elements appearing in both A and B, otherwise known as the intersection of A and B. So the cardinality of the shaded region is precisely $|A \cap B|$. How would we represent the cardinality of the following using set notation?



In words, the shaded region above, is all of B that is not contained in A. So, what we are looking for is precisely $|A^c \cap B|$.

Proposition 21.1.1. *Let A, B be subsets of some finite universal set U. Then $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof. We can prove this with the help of a Venn diagram. Note that $A \cup B$ is represented by the following Venn diagram.



Note that when we count $|A| + |B|$, the region of $A \cap B$ gets counted twice. Once in $|A|$ and once in $|B|$. So we need to subtract off just one count of $A \cap B$ and so we obtain the desired formula. □

Theorem 21.1.1. *Let A and B be subsets of some finite universal set U. Then:*

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \cap B| \leq \min\{|A|, |B|\}$
- $|A \setminus B| = |A| - |A \cap B|$
- $|A^c| = |U| - |A|$
- $|A \times B| = |A| \cdot |B|$

We have already proven the first bullet point. The rest of the bullet points follow quickly from the definitions of $\cap, \cup$ and complements.

The above can be extended to more than just two sets. In particular, it is often of interest to understand $|A_1 \cap A_2 \cdots \cup A_n|$ where n is some positive integer.

Theorem 21.1.2 (Principle of Inclusion-Exclusion (**PIE**))**.** *Let $A_1, A_2, \ldots, A_n$ is a finite collection of finite sets. Then*

$$|A_1 \cup A_2 \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cdots \cap A_n|$$

Let us do a few examples to see how PIE works. PIE can be an incredibly powerful tool for counting various phenomena. Often times, the most difficult part, is phrasing the question in the right way so that it becomes clear how exactly we are to use PIE.

Example: Suppose that we have took a sample of 100 people, and we want to determine how many of them have at least one of the following social media platforms: Instagram, Snapchat, TikTok. Let $|A| = 42$ be the number of people with an Instagram account, $|B| = 51$ be the number of people with a Snapchat account, and $|C| = 32$ be the number of people with a TikTok account. Suppose further that $|A \cap B| = 13$, $|B \cap C| = 25$ and $|A \cap C| = 32$, and that not a single person in the sample has all three. How many people in the sample don't have any of the given social media accounts?

Solution. We want to know how many people have at least one social media account. This is precisely the count for $A \cap B \cap C$. If some person has at least one of the three social media accounts, then they will appear in one of the sets A, B, C and therefore will appear in $A \cup B \cup C$. By PIE, we have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Then plugging in the numbers we were given, we obtain:

$$|A \cup B \cup C| = 42 + 51 + 32 - 13 - 25 - 32 + 0 = 55.$$

Therefore, the number of people who have at least one social media account is 100. Then the number of people have no social media account is $(A \cup B \cup C)^c = |U| - |A \cup B \cup C|$. Here U, the universal set, is the set of 100 people in the sample. Therefore

$$(A \cup B \cup C)^c = |U| - |A \cup B \cup C| = 100 - 55 = 45.$$

Example: Let $n = 11 \cdot 7 = 77$. Determine the number of positive integers less than 77 that are relatively prime with 77.

Solution. This is an example of a question that first has us determine the sets A_i that we will use in our application of PIE. First, we note that any number that is relatively prime with 77, cannot share any factors of 7. Meaning, if $\gcd(a, 77) = 1$, then a is not divisible by 7 or 11. Our universal set is

$$U = \{1, 2, 3, \ldots, 77\}.$$

One way we can determine the answer to this question, is to first count the number of natural numbers in U that are *not* relatively prime with 77, and subtract this from the number 77. Meaning, if we determine how many numbers in U are divisible by either 7 or 11, then we could subtract this number from 77 to obtain how many numbers less than 7 *are* relatively prime with 7. Let $A_1 \subset U$ be the set of numbers divisible by 7 and $A_2 \subset U$ be the set of numbers divisible by 11. We claim that the answer to the problem is

$$|(A_1 \cup A_2)^c| = |U| - |A_1 \cup A_2| = 77 - |A_1 \cup A_2|.$$

By PIE

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Notice

$$A_1 = \{7, 14, 21, \ldots, 77\} \quad A_2 = \{11, 22, 33, \ldots, 77\}$$

So

$$|A_1| = 77/7 = 11 \quad \text{and} \quad |A_2| = 77/11 = 7.$$

Now ${}_1 \cap A_2$ is the set of all numbers in U that are divisible by both 7 and 11. But since 7 and 11 are prime, then in fact, we have proven on the previous homework that $A_1 \cap A_2$ is the set of all numbers divisible by 77. But there is only one number in U that is divisible by 77, and that is 77. So $|A_1 \cap A_2| = 1$. Therefore

$$|(A_1 \cup A_2)^c| = 77 - (7 + 11 - 1) = 60.$$

There are 60 natural numbers less than 77 that are relatively prime with 77.

22 Lecture 11-8-2021

22.1 Addition Rule

Note that given sets $A_1, A_2, \ldots, A_n$ that are pairwise disjoint, then the intersection of any number of the sets is empty. In this case we end up with just

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i|.$$

Sometimes, there are questions that can be reduced to the form above by making a clever choice of A_i. A simple example is as follows:

Example: In how many ways can you get a sum total of six when rolling two dice?

Solution. After thinking for a second, we observe that the only way to get a sum total of six, is when:

- You roll two 3's
- You roll a 2 and a 4
- You roll a 1 and a 5

So we may define A_1 to be the set of all possible ways to roll two threes, A_2 to be the set of all possible ways to roll a 2 and a 4, and A_3 to be the set of all possible ways to roll a 1 and a 5. So $A_1 = \{(3,3)\}$, $A_2 = \{(2,4),(4,2)\}$ and $A_3 = \{(1,5),(5,1)\}$. Each of these sets is disjoint, and in total, they account for all possible ways to obtain a sum total of six when rolling two dice. Therefore,

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| = 5.$$

Often times, these sorts of questions appear in probability, and so the sets $A_1, A_2, \ldots, A_n$ are referred to as **events**. Each individual set A_i contains all the possible ways that it's corresponding event can occur. We call two events **independent** when their associated sets are disjoint.

The questions above asked in how many ways can the *event* that we roll a sum total of six happen when we roll two dice? Then in our solution we would interpret A_1 as the event that we roll two 3's, A_2 as the event that a 2 and a 4 were rolled, and A_3 the event that a 1 and a 5 were rolled. Since the A_i's were disjoint, then they are considered to be independent events.

22.2 Multiplication Rule

In the last lecture, we noted that $|A \times B| = |A| \cdot |B|$. More generally, it is true that

$$|A_1 \times A_2 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

If $A_1, A_2, \ldots, A_n$ are events, then the number of ways in which a sequence of events can occur. Observe that we may answer the example question above using this method instead.

Solution. First consider rolling the first die. If the die is either 1, 2, 3, 4, 5, then for each of these cases, there is exactly one choice for the what the roll of the second die should be so that the sum total is 6. If the first die is a 6, then the sum total of two dice will be greater than 6. So then there are 5 choices for the first die, and 1 choice foe the second die, giving us $5 \cdot 1 = 5$ possible ways of rolling two dice to obtain a sum total of 6.

Example: How many problems in the range 1000-9999 have **no** repeated digits.

Solution. Notice, the thousands place is between 1 and 9, and so 0 is not included. So there are 9 choices for the first digit. Then, there are still 9 choices for second digit, since it can be a zero. But now, for the third digit, it must be distinct from the first two digits, and so there are 8 choices for the third digit, and finally, there are 7 choices for the last digit. Thus there are $9 \cdot 9 \cdot 8 \cdot 7 = 4536$ numbers in the range 1000-9999 that do not have any repeating digits.

23 Lecture 11-10-2021

23.1 Combining the Rules

Exercise 23.1.1. Using only digits 2, 4, 6, 8:

- How many two digit numbers can be formed?
- How many three digit numbers can be formed?
- How many two or three digit numbers can be formed?

Solution. We are given four distinct numbers. Then we can put any of the four into the tens place and any of the four into the ones place, and so there are $4^2 = 16$ different two digit numbers that can be made. Taking this a step further, we may put any of the four digits into the hundreds place, giving us $4^3 = 64$ three digit numbers that can be made using 2, 4, 6, 8. Finally, since there are 4^3 three digit numbers and 4^2 two digit numbers, and as sets, three digit number and two digit numbers are disjoint, this means that there are $4^3 + 4^2 = 80$ numbers that can be made from 2, 4, 6, 8 that are either two or three digits long.

Exercise 23.1.2. How many three digit numbers contain the digits 2 and 5, but none of the digits 0, 3, 7?

Solution. We have three open spots to put a 2, a 5, and the one other digit that is not 0, 3, or 7. We may choose any of the spots to put the 2 in, so three choices, and then we have two choices for where we can put the 5, and then we have one choice for where to an arbitrary digit x. So there are 6 different ways this can be arranged, in particular,

$$25x \quad 2x5 \quad 52x \quad 5x2 \quad x25 \quad x52.$$

In each of the cases above, if x is not 0, 3, 7 nor 2, or 5, then we obtain *distinct* numbers for any of the remaining choices for x. That is, if we choose x to be either $1, 4, 6, 8, 9$, then we obtain distinct numbers for any of the 6 possibilities.

For example, if we replace x with 1, then we get

$$251 \quad 215 \quad 521 \quad 512 \quad 125 \quad 152.$$

all of which are distinct. So there are 6 three digit numbers obtained for any one choice of x from values $1, 4, 6, 8, 9$. However, if we instead use 2 or 5, observe that

$$252 \quad 225 \quad 522 \quad 522 \quad 225 \quad 252.$$

there are only three distinct numbers above, likewise

$$255 \quad 255 \quad 525 \quad 552 \quad 525 \quad 552.$$

we obtain three more distinct numbers. So in total there are $6 \cdot 5 + 3 + 3 = 36$ distinct three digit numbers the contain a 2 and a 5, but do not contain a 0, 3, or 7.

23.2 Pigeonhole Principle

Let A and B be finite sets with $|A| > |B|$. Recall that *any* function $f : A \to B$ cannot be one-to-one since there are more elements in the domain than in the target set. That is, there will always exist an $x \in B$ such that there are two distinct $y, z \in A$ with $f(y) = f(z) = x$.

Theorem 23.2.1 (The Pigeonhole Principle)**.** *Let m, n be natural numbers, with $m < n$. If n objects are put into m boxes, then at least one box will have two or more objects.*

Exercise 23.2.1. Prove that there are two people in our classroom of 25 students that have the same birthday month. In fact, prove that three people have the same birthday month.

Solution. Let each month represent a box, so we have 12 boxes in total. But each student's name into the box corresponding to their birthday month. Since we have put 25 objects into 12 boxes, then by the pigeonhole principle, we must have at least one box containing 2 names.

To see that there should be a box with at least 3 names, consider putting in 24 names into the boxes. If no box has 3 names in it, then that would mean each box has exactly 2 names in it, since $2 \cdot 12 = 24$. But then even in this case, we are left with one more name to place into a box. No matter which box we put it into, we end up with 3 names in that box.

Theorem 23.2.2 (The General Pigeonhole Principle)**.** *Let m, n be natural numbers, with $m < n$. If n objects are put into m boxes, then at least one box will have $\lceil \frac{n}{m} \rceil$ objects.*

Exercise 23.2.2. Suppose there exists a city where each person has at least 50,000 hairs on their head, and less than 200,000 hairs on their head. Suppose also that this city has a population of 150,001. Prove that two people in this city have the same number of hairs on their head. What if the populations was 300,001? What could we say then?

Solution. For each possible number of hairs, make a box labeled with that number, and put a person's name into that box if they have that number of hairs. We have boxes labeled $50,000, 50,001, \ldots, 199,999$ which is a total of 150,000 boxes. Since there are 150,001 names to put into the boxes, then as there are only 150,000 boxes, the pigeonhole principle informs us that one box has two names in it. Meaning two people have the same number of hairs on their head. If the population was 300,001, then there would be

$$\left\lceil \frac{300,001}{150,000} \right\rceil = 3$$

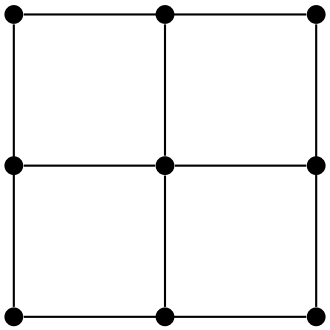
many people with the same number of hairs on their head.

Exercise 23.2.3. Show that among $n + 1$ arbitrarily chosen integers, there must exist two whose difference is divisible by n.

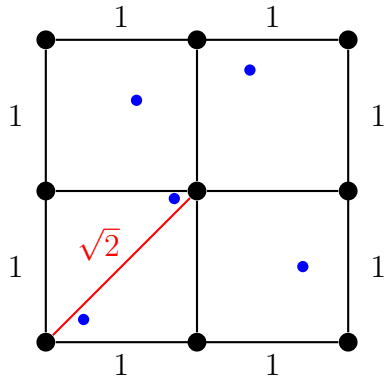
Solution. Let $a_1, a_2, \ldots, a_{n+1}$ be the given numbers. Note that if we consider the given integers, modulo n, then setting $r_i \equiv a_i \pmod{n}$ with $0 \leq r_i < n$, we have $n + 1$ integers modulo n, and only n possible modulo classes, from 0 to $n - 1$. By the pigeonhole principle then, there exists i and j such that $r_i = r_j$, but that means $a_i \equiv a_j \pmod{n}$ implying by definition of congruence, that $n|(a_i - a_j)$.

Exercise 23.2.4. Given five points inside a square whose side lengths are 2, prove that there exist two points that are within a distance of $\sqrt{2}$ of each other.

Solution. Observe that if we have a square with sides of length two, then we can break this square up into four subsquares whose side lengths are 1 as follows:



Then given 5 points to place into the box, since there are 4 subsquares, then by the pigeonhole principle one of the subsquares will end up with two points. But notice that any two points inside one subsquare are within $\sqrt{2}$ of each other since the diagonal of any of the smaller squares has length $\sqrt{2}$. If two points fall into one subsquare, the farthest apart that they could be is at opposing diagonals, which are at a distance of $\sqrt{2}$.



24 Lecture 11-12-2021

24.1 Permutations

Recall that $n! = n(n-1)(n-2)\cdots(2)(1)$, is the produce of all consecutive integers from 1 up to n.

Exercise 24.1.1. Suppose we are given 5 symbols, say, a, b, c, d, e. How many distinct strings can be made of length three, that use each symbol only once?

Solution. We have three open spots to choose from. As soon as we choose one symbol to be put into a certain position, then that symbol cannot be used again. So in the first spot there are 5 symbols to choose from, the second spot there are 4 symbols to choose from, and the last spot, there are 3 symbols to choose from. So in total, we obtain $5 \cdot 4 \cdot 3 = 60$ different three letter strings can be made using a, b, c, d, e where each symbol appears at most once.

Denote

$$P(n,r) = \frac{n!}{(n-r)!} = n(n-1)(n-2)\cdots(n-r+1)$$

Theorem 24.1.1. *Given a set of n distinct symbols, the number of ways to make distinct strings of length r, that use each symbol at most once, is exactly $P(n,r)$.*

Definition. Given a set of n symbols, a permutation of the symbols is just an ordering of the symbols in a line. An r-permutation of n symbols, is just a permutation of r of the n symbols.

Exercise 24.1.2. A NASCAR race is about to begin. The cars are numbered, 2, 13, 18, 65, 77, 98. Before the race starts, the cars are driving in a single file line.

1. In how many ways can this happen?
2. In how many ways can this happen if the first car is car 2?
3. In how many ways can this happen if car 13 is immediately followed by car 98?
4. In how many ways can this happen if car 13 falls right between car 18 and car 77, with no other cars appearing between 18 and 17?
5. In how many ways can this happen if car 13 is between car 18 and car 77, with no other restrictions.

Solution. Let us address these in order.

1. There are six distinct cars, and if we can order them in any way, then we have $6! = 720$ possible ways to order them.
2. If the first car is 2, then the first position is fixed, but we may order the remaining cars in any way. Since there are five cars, left then we may order them in $5! = 120$ different ways.
3. If car 13 must appear directly ahead of car 98, then we can think of cars 13 and 98 as one car. We suppose that there are now just five cars, labeled by parentheses (2), (13, 98), (18), (65), (77). There are 5! ways to order 5 cars, and in all these orderings we will have car 13 directly ahead of car 98. So this account for all possible orderings of the six cars, where 13 is directly followed by 98. So $5! = 120$ total orderings.
4. The possible ways that 13 can be sandwiched between 18 and 77 is either (18, 13, 77) or (77, 13, 18). Notice these two cases cannot overlap with one another, since they involved a different ordering of the same cars. So we must count and add in how many ways we see $(18, 13, 77)$ appearing and $(77, 13, 18)$ appearing. Again if we consider $(18, 13, 77)$ as one car, then we have a total of four cars: $(18, 13, 77), (2), (65), (98)$, and there are 4! ways of ordering them. Likewise, there are 4! ways of ordering the six total cars to end up with (77, 13, 18). So in total there are $4! + 4! = 48$ orderings of the six cars where 13 is sandwiched between 77 and 18.

5. Notice, given any ordering of the six cars, we can permute 13, 18, and 77 in the positions that they are in to obtain different orderings. There are $3! = 6$ ways to permute these three cars, while keeping the others fixed. In exactly two of the orderings does the car 13 appear between 18 and 77. So, in total there are $6! \cdot (2/6) = 240$ different orderings of the six cars where car 13 appears between 18 and 77.

25 Lecture - 11-15-2021

25.1 Combinations

In the last lecture, we discussed permutations, in this lecture, we will discuss combinations. The primary difference between a combination and permutations, is that we consider *different* orderings of the same object as *different* permutations. On the other hand, different orderings of the same objects still form the same **combination**. In summary:

- Given n symbols, the number of distinct r-permutation is

$$P(n, r) = \frac{n!}{(n-r)!}.$$

- Given n symbols, the number of ways to *choose* r symbols is

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{P(n,r)}{r!}.$$

  $\binom{n}{r}$ is called a *binomoial coefficient*. Usually we read/say $\binom{n}{r}$ as "n choose r".

So if we were given the letters a, b, c, d, e, the following two strings abc and acb are different permutations, but they are the same combination, because the letters are exactly the same.

Notice that from the definition

$$\binom{n}{r} = \binom{n}{n-r}.$$

An intuitive way to see this, is that any time we choose r distinct objects from a collection of n objects, we are also choosing $n - r$ distinct objects to be left behind. This idea creates a bijection between the set of all possible combinations of r objects from n objects, to the set of all possible combinations of $n - r$ objects from n objects.

Theorem 25.1.1. *Let $r \leq n$ be natural numbers. Thee number of ways to put r identical objects into n distinct boxes so that each box has at most one object is $\binom{n}{r}$*

Exercise 25.1.1. Given a group of 20 people, in how many ways can we create a group of 5 people?

Solution. There are 20 people, and we want to choose any 5 to put into a group together. So there are $\binom{20}{5}$ to do this.

Exercise 25.1.2. Suppose you toss a coin eight times. In how many ways can you get five heads and three tails? How about three heads and five tails?

Solution. We have a total of eight coin tosses. We want to choose five of them to be heads. If exactly five are heads, then this is equivalent as choosing the remaining three to be tails. By choosing which coin tosses are heads, we uniquely determine all eight coin tosses. There are $\binom{8}{5}$ ways to choose five tosses to be heads out of a total of eight tosses. Since the rest are heads, then there is only one way to fill in the rest of the tosses once the five heads have been chosen. So there are $\binom{8}{5} = 56$ ways you can get 5 heads and three tails. Likewise, there are $\binom{8}{3} = 56$ ways to get three heads and five tails out of eight coin tosses.

Exercise 25.1.3. An urn contains 15 distinctly numbered red balls, and 10 distinctly numbered white balls. A sample of five balls is selected.

1. How many different samples are possible?
2. How many samples contain all red balls?
3. How many samples contain three red balls and two white balls?

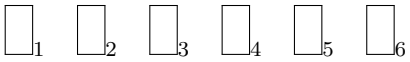
Solution. We have:

1. Since there are 25 total distinct balls, and we choose 5, there are $\binom{25}{5}$ ways to sample 5 balls from the urn.
2. Since there are 15 red balls, then there a $\binom{15}{5}$ ways sample 5 red balls.
3. There are $\binom{15}{3}$ ways to sample 3 red balls and $\binom{10}{2}$ ways to sample 2 white balls. Using the product rule tells us that there are $\binom{15}{3}\binom{10}{2}$ ways to sample three red balls together with two white balls.

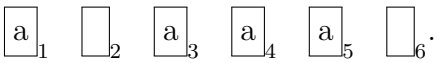
26 Lecture 11-17-2021

26.1 Repetitions

In the previous lecture, we determined that the number of ways to put r identical objects into n distinct boxes, with $r \leq n$, and such that *each box has at most one object*, is $\binom{n}{r}$. What if we removed the constraint that each box has at most one object? Notice, under this scenario, we no longer require the constraint that $r \leq n$. Well, let's take a look at this idea using an illustration with $n = 6$ and $r = 4$. So we have 6 boxes, and let's say we want to see in how many different ways we can put four letter a's into the boxes.

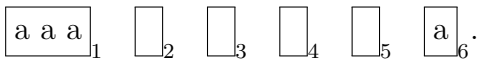


For example, here is one possibility

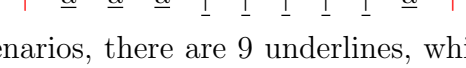


Observe that we could represent this scenario in the following way.

Imagine the red lines as being fixed and as the outer most portion of the boxes on the sides, namely boxes 1 and 6. The rest of the vertical bars represent the remaining sides, where two neighboring boxes share a vertical bar as a side. Since box 1 has an "a" in it, then we first write an "a" and then a vertical line. Since box 2 is empty, what follows right away is another vertical line. Since there is nothing between the two vertical lines, that represent that there is nothing in the corresponding box. Let's convert another scenario:



This one now looks like



Observe that in both scenarios, there are 9 underlines, which corresponds to 6 boxes + 4 objects -1. In general, given r identical objects and n distinct boxes, the number of ways in which the r objects can be placed into the n boxes is

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

This is because we may draw $n + r - 1$ underscores, and out of those, we choose where to place $n - 1$ vertical lines. Between two vertical lines is what denotes what belongs to the box it corresponds to.

Exercise 26.1.1. How many different outcomes are possible when five dice are rolled?

Solution. Choose the boxes to be the possible values that a die can take. So we have 6 boxes, labeled 1 through 6. We may now consider the die as identical objects and put each die into the box that corresponds to the value that was rolled with it. So if a two 5's, three

4's were rolled, then we would put two dice into box 5 and three dice into box 4. Then there are

$$\binom{5+6-1}{5} = \binom{10}{5} = 252$$

possible outcomes for five dice being rolled. Each outcome can be represented as we did in the example above.

Exercise 26.1.2. In how many ways can the letters of the word "Banana", be rearranged to create distinct strings?

Solution. The word "Banana" has three distinct letters, "b", "a", and "n". Create three boxes and label them using these three letters. Banana also has exactly six letters, one b, two n's and three a's. So we must choose one of six positions to go into box b, two of six positions to go into box n, and the rest go into box a. Using the multiplication rule, this gives us that there are $\binom{6}{1}\binom{5}{2} = 60$ ways to rearrange the letters in the word "banana" to create distinct strings.

Exercise 26.1.3. Show that there is a one-to-one correspondence between the number of ways to put ten identical marbles into three boxes and the number of ordered triples of non-negative integers (x, y, z) such that

$$x + y + z = 10.$$

How many distinct triples are there?

Solution. Notice that this is the exact same question as asking in how many ways can we put 10 identical objects into 3 distinct boxes. If we label the boxes x, y, z, then the number of objects in that box will correspond to the value of x, y, z in $x + y + z = 10$. Each possible way to put 10 objects into three boxes will correspond to a unique triple x, y, z. So then the solution is

$$\binom{10+3-1}{3-1} = \binom{12}{2}.$$

Exercise 26.1.4. There are 15 questions on a multiple choice exam with 5 possible answers for each question. In how many ways can the exam be answered? In how many ways can it be answered so that exactly 8 questions are correct?

Solution. Since there are 5 possible solutions for each questions then the total number of ways that the exam can be answered is $5 \cdot 5 \cdots 5 = 5^{15}$. To see in how many ways can the exam be answered so that exactly 8 questions are correct is as follows. First out of the 15, we choose which 8 we wish to answer correctly. There are $\binom{15}{8}$ ways to do this. Since there is only one correct answer per question, that leaves us with only 1 choice out of 5 possible answers for those 8 questions. Then, the remaining questions must be answered incorrectly. There are 4 out of 5 ways to answer the questions incorrectly, so in total, the answer is

$$\binom{15}{8}1^8 4^7 = \binom{15}{8}4^7.$$

27 Lecture 11-19-2021

27.1 The Binomial Theorem

Many years ago, you may recall having learned about Pascal's triangle. We will now revisit it and uncover some new things about it.

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

And on it goes. There are many curious things one can observe about Pascal's triangle, some of which we are now equipped to prove. First, observe that

$$\begin{array}{rl} 1 & = 1 \\ 1 + 1 & = 2 \\ 1 + 2 + 1 & = 4 \\ 1 + 3 + 3 + 1 & = 8 \\ 1 + 4 + 6 + 4 + 1 & = 16 \end{array}$$

If we consider the very top to be row zero, then there is a pattern suggested that the sum of all the elements of row n of Pascal's Triangle is equal to 2^n. There is also another observation we can make, and that is:

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

So we have that row n entry i in Pascal's triangle can be given by $\binom{n}{i-1}$, since the first entry in a row corresponds to 0. So putting the two observations together, we can hypothesize that

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

A key importance that Pascal's triangle plays, is that it in fact tells us the coefficients in the expansion of $(x+y)^n$.

Theorem 27.1.1 (The Binomial Theorem)**.** *Let n be a natural number, then*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Proof. □

The fact that

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

now falls out as a quick corollary of the binomial theorem. If we set $x = y = 1$, we observe that we have

$$2^n = (1+1)^n = \sum_{i=0}^{n} \binom{n}{i} 1^i 1^{n-i} = \sum_{i=0}^{n} \binom{n}{i}.$$

Exercise 27.1.1. Determine the coefficient of x^4y^4 in the expansion of $(2x-y)^8$.

Solution. By the binomial theorem, we have that

$$(2x-y)^8 = \sum_{i=0}^{8} \binom{8}{i} (2x)^i (-y)^{8-i}.$$

Observe that the term x^4y^4 appears in the above summation precisely when $i = 4$. Then we obtain that the coefficient of x^4y^4 is

$$\binom{8}{4} 2^4 (-1)^4 = 1120$$

Exercise 27.1.2. Compute the constant term that appears in the expansion of $(x - \frac{1}{x})^{10}$.

Solution. By the binomial theorem, we have that

$$\left(x - \frac{1}{x}\right)^{10} = \sum_{i=0}^{10} \binom{10}{i} x^i \left(-\frac{1}{x}\right)^{10-i} = \sum_{i=0}^{10} \binom{10}{i} \left(x^{10-2i}\right) (-1)^{10-i}.$$

The constant term, is coefficient of x^0, which is given precisely when $i = 5$. So the coefficient is

$$\binom{10}{5} (-1)^5 = -252.$$

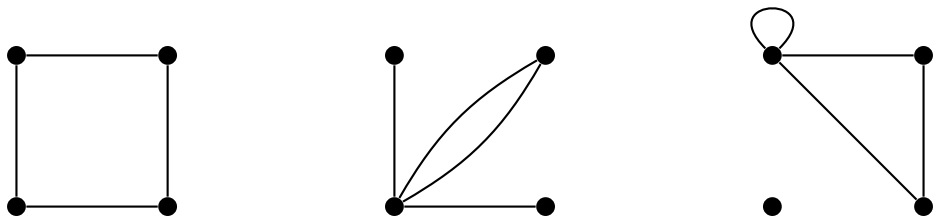
28 Lecture 11/28/2021

28.1 Graphs

What is a *graph*? In more practical terms, a graph is a network. A "node" in the network is called **vertex** of the graph. A connection joining two nodes in the network, is called an **edge** of the graph. Here are some examples of graphs

Definition. An **undirected graph** $G(V, E)$ usually written as just G, is a pair of sets, (V, E). V is the set of vertices of G and the edge set E consists of 2-subsets of V. We refer to undirected graphs as just graphs.

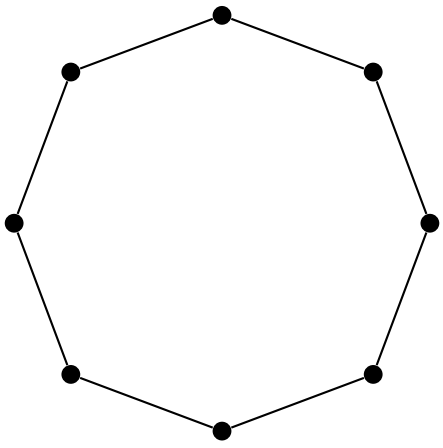
Let's take a look at some networks and determine which fit the definition of a graph, and which do not.



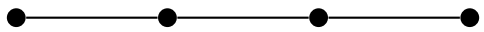
The network above on the left, is a graph. Any two vertices have at most one edge, and there are no loops. The middle network is not a graph in the formal sense, because between two vertices there is multiple edges. Since the edge set is a set, then there can be no repetitions in a set, and so the edges given by the middle network would not form a set, but a multiset.The network above on the right has a loop at on of its vertices. A loop has the same start and end point, and so as an edge, a loop is not a 2-subset of the vertex set, but is just a 1-subset. This disqualifies the network on the right from being a graph

The networks above that do not fit the definition of a graph, are called **psuedographs**. We will not spend much time exploring these. Our primary interest will be that of graphs. Here are some common types of graphs:

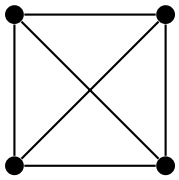
- The cycle graph of length n, is a graph that forms a cycle on n vertices. That is if we put the vertices in a circle, then the only edges that would appear are the ones connecting nearest vertices. Here is an example of a C_8, the cycle on 8 vertices.



- Paths, denoted P_n have $n+1$ vertices and n edges. Here is an example of P_3, a path of length 3.



- The complete graph on n vertices, denoted K_n. This is the graph where any two vertices are adjacent. The complete graphs has $\binom{n}{2}$ vertices (why?). Here is an example of K_4, the complete graph on 4 vertices.



Definition. We say that vertices x, y of some graph G are **adjacent** if $\{x, y\}$ is an edge in G. We often write xy to refer to the corresponding edge in E. In this case, the vertices x and y are said to be **incident** to the edge xy. Given a vertex x, and vertex y that is adjacent to x is called a **neighbor** of x. The set of all neighbors of x is called the **neighborhood** of x. The **degree** of a vertex x is the size of the neighborhood of x. Denote the degree of a vertex x by $d(x)$.

Theorem 28.1.1. *Let G be a graph with sets V and E. Then*

$$\sum_{x \in V} d(x) = 2|E|.$$

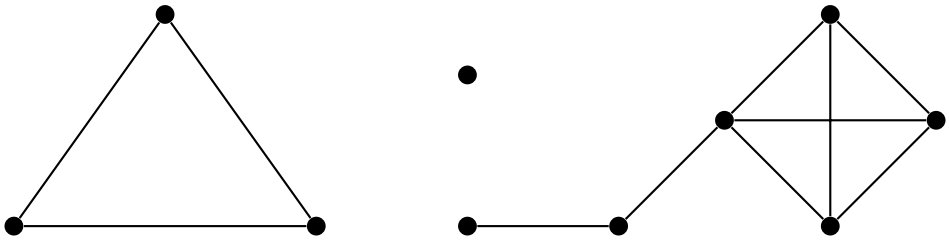
Proof. Notice that $d(x)$ counts the number of neighbors of the vertex x, meaning it counts the number of edges that contain x in the graph G. If xy is an edge, then the edge gets counted in $d(x)$ *and* in $d(y)$. The edge xy is incident only to x and y so it does not get counted when summing the degrees of other vertices, $d(z)$ where $z \neq x, y$. So in the sum of all the degrees, each edge gets counted exactly twice. Therefore, the total sum of the degrees of all the vertices is twice the number of edges. □

29 Lecture 12-1-2021

29.1 More on Graphs

Definition. The **degree sequence** of a graph G is an ordered list of the degrees of all the vertices in a graph. The list is usually ordered in descending order.

Example: What are the degree sequences of the following graphs?



The degree sequence of the triangle, the graph above on the left, is (2, 2, 2). The graph on the right, is slightly more complicated, but we just need to write down the degrees of all the vertices, and then order them in descending order. Doing so, yields (4, 3, 3, 3, 2, 1, 0).
Example: Are the following lists the degree sequence of any graphs? If not, explain why, if yes, draw a graph that has the given list as its degree sequence.

- 5, 3, 3, 2, 1, 1
- 2, 2, 2, 0

Solution. Notice the sum of all the numbers in the first list is $5 + 3 + 3 + 2 + 1 + 1 = 15$. However, we already saw that the sum of all the degrees of a graph must be twice the the number of edges, which is an *even* number. Since 15 is odd, then 5, 3, 3, 2, 1, 1 cannot be the degree sequence of any graph.

In general, there is a process for constructing a graph with a given degree sequence, assuming that such a graph exists. Let's consider the following degree sequence: 6, 6, 5, 4, 3, 3, 2, 1. To each element in the sequence let's associate some unique label, so we have vertices $x_1, x_2, x_3, x_4, x_5, x_6$, where

$$d(x_1) = 6,\ \ d(x_2) = 6,\ \ d(x_3) = 5,\ \ d(x_4) = 4,\ \ d(x_5) = 3,\ \ d(x_6) = 3\ \ d(x_7) = 2\ \ d(x_8) = 1.$$

It is not immediately clear what sort of graph has this degree sequence, so we reduce the problem by a small step as follows. Take the first vertex, x_1. Since $d(x_1) = 6$, we subtract one from the degrees of the 6 vertices following x_1 in the sequence, namely from $x_2, x_3, x_4, x_5, x_6, x_7$. This way, we go from one degree sequence to a smaller one as follows.

$$(6, 6, 5, 4, 3, 3, 2, 1) \to (\not{6}, 6-1, 5-1, 4-1, 3-1, 3-1, 2-1, 1) = (5, 4, 3, 2, 2, 1, 1).$$

Repeat this process until we get to a degree sequence whose graph we can easily construct. Following this process, the next step gives us

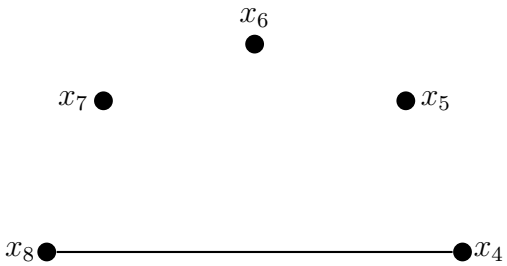
$$(5, 4, 3, 2, 2, 1, 1) \to (3, 2, 1, 1, 0, 1).$$

We notice that the list is no longer ordered, so we must swap the places of vertices x_7 and x_8 so that it remains ordered. So the next step is

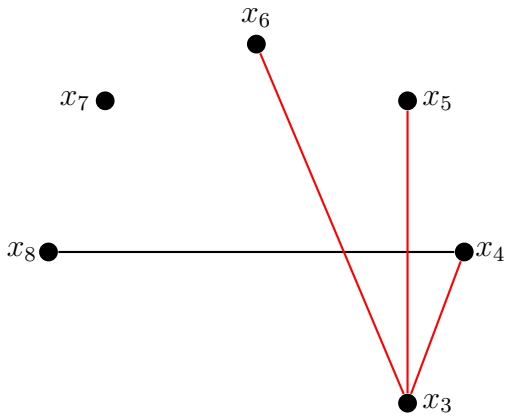
$$(3, 2, 1, 1, 1, 0) \to (1, 0, 0, 1, 0)$$

Again, we must reorder two positions. Now we swap x_8 and x_5 to obtain the sequence $(1, 1, 0, 0, 0)$. Now, this sequence is one from which we can easily construct a graph. We will use the graph for this sequence as the basis for which to build the graph whose degree sequence is the original sequence we started with. We begin with the sequence $(1, 1, 0, 0, 0)$ which corresponds to vertices x_4, x_5, x_6, x_7, x_8 with $d(x_4) = 1 = d(x_8) = 1$, $d(x_5) = d(x_6) = d(x_7) = 0$.

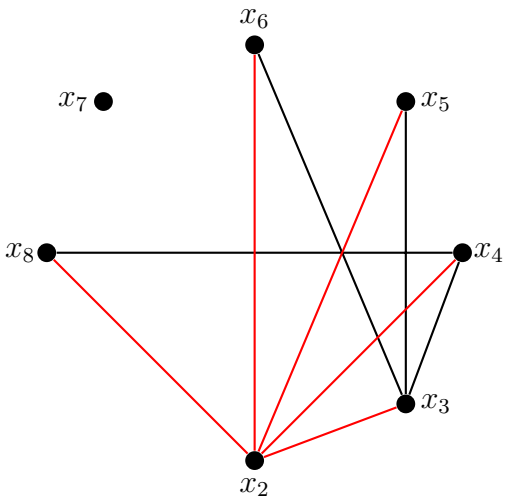
Deg. Seq. $= (1, 1, 0, 0, 0)$



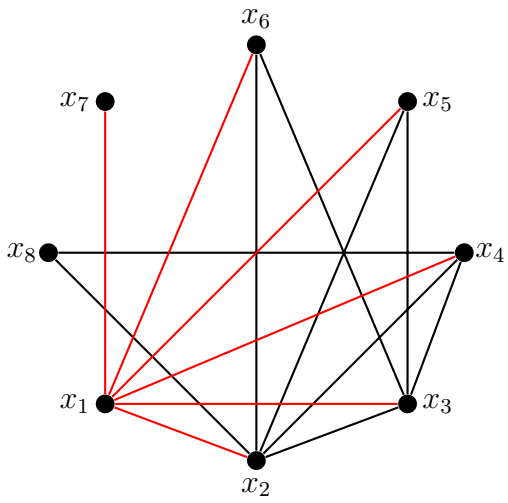
Deg. Seq. $= (3, 2, 1, 1, 1, 0)$



Deg. Seq. $= (5, 4, 3, 2, 2, 1, 1)$



Deg. Seq. $= (6, 6, 5, 4, 3, 3, 2, 1)$

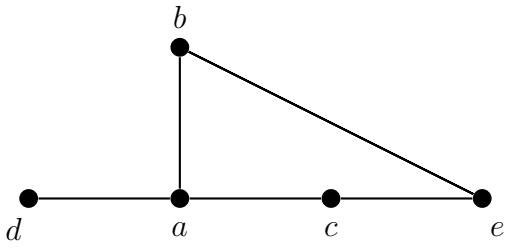


30 Lecture 12-3-2021

30.1 Bipartite Graphs

Definition. A **walk** of length k in a graph G is an ordered list of vertices of G, $x_1, x_2, \ldots, x_k, x_{k+1}$ (not necessarily distinct vertices) such that $x_i x_{i+1}$ is an edge in G for each i from 1 to $k+1$. We say that a walk is a **closed walk** if $x_1 = x_{k+1}$.

Example: Suppose that we are given the following graph G.



Which of the following lists are walks in G? Which are closed walks?

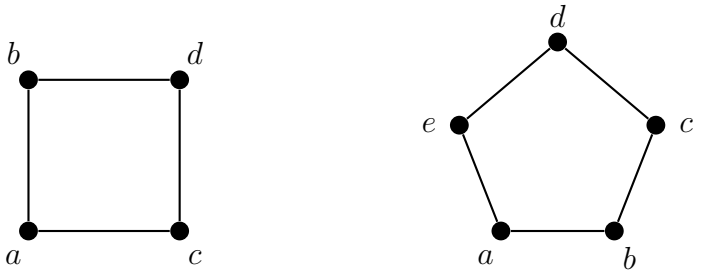
1. a, b, d, a, c
2. e, b, a, c, a
3. d, a, d
4. d, a, b, e, c, a, d

We see that the (1) is not a walk, because bd is not an edge. (2) is a walk, but is not a closed walk. (3) is a walk, and is also closed. And finally, (4) is also a closed walk.

Definition. A graph G is **connected** if between any pair of vertices, x, y in G, there exists a path (or a walk) connecting them. Otherwise, G is called **disconnected**, and G is the union of smaller connected graphs, which we will call the **connected components** of G.

Definition. A **bipartite graph** G, is a graph whose vertex set can be partitioned into two sets, A and B so that every edge of G is incident with one vertex from A and one vertex from B. No edges are incident to two vertices from the same part.

Example: Which of the following graphs are bipartite, and which are not?



The 4 cycle in the top left, is bipartite, since we can choose vertices that are at a diagonal to be in the same part. So, set $A = \{a, d\}$ and $B = \{b, c\}$. The second example, is not, why? Try to put vertices in different parts to avoid having edges between vertices in the same part and observe what happens.

Theorem 30.1.1. *A graph G is bipartite if and only if there are no closed walks of odd length in G.*

Proof. We first show that if a graph G is bipartite, then it has no closed walks of odd length. Since G is bipartite, then there is a partition of the vertex set V into sets A and B, such that any two vertices in A or any two vertices in B have no edges between them. So all the edges of G appear between parts A and B. Suppose for a contradiction that we do find a closed walk of odd length in G, say it has length $2k+1$, some odd number. Then the walk has $(2k+1)+1$ vertices and since it is closed, then the first and last vertex are the same. Then the walk is of the form

$$x_1, \quad x_2, \quad x_3, \quad \ldots, \quad x_{2k}, \quad x_{2k+1}, \quad x_1$$

Now, x_1 must belong to either A or B, so without loss of generality, we may assume that $x_1 \in A$. Since the above list is a walk then x_1x_2 is an edge, and therefore $x_2 \in B$, implying $x_3 \in A$ and so on. This tells us that as we go down the list, any vertex with an odd subscript is in A and any vertex with an even subscript is in B. So we have

$$\begin{array}{cccccccc} x_1, & x_2, & x_3, & \ldots, & x_{2k}, & x_{2k+1}, & x_1 \\ A, & B, & A, & \ldots, & B, & A, & B \end{array}$$

But how can x_1 be both in A and B when A and B must be disjoint sets? Impossible! A contradiction. Therefore, it is not possible to have a closed walk of odd length in a bipartite graph.

Now, we must prove that if G is a graph in which no closed walks of odd length exist, then G is bipartite. We will use the fact that there exist no closed walks of odd length in G to demonstrate sets A and B that partition the vertex set of G and such that there are no edges amongst vertices inside each part. Let $x \in V$ be any vertex in our graph G. I claim that for every other vertex in $y \in V$ either:

- There exists no walk from x to y (G is disconnected in this case).
- There exist only walks of even length from x to y,
- There exist only walks of odd length from x to y.

If G is disconnected, that is there is no walk of any length from x to y, then this does not affect whether a graph is bipartite or not, and instead we work with connected components of G, and once we have partitioned each connected component we put them together, to obtain the result we're after. What is left to demonstrate, is that there cannot exist a vertex y such that from x to y there are two walks, one of odd length, and one of even length.

Suppose for a contradiction that there does exist such a vertex y such that there exists two walks from x to y, one of length $2j$ one of length $2k+1$. Then note that we can put these two walks together to obtain a closed walk of length $2k+2j+1$ from x back to x. But this is a closed walk of odd length! Another contradiction! Thus, each vertex in y belonging to the same component as x either has an odd length walks from x to y or an even length walks from x to y. Let x together with all the vertices y for which there is an even length walk from x to y be the vertex be called the set A, and let the remaining vertices be the set

B. The remaining vertices in this case happen to be all those for which there is a walk of odd length from x to y.

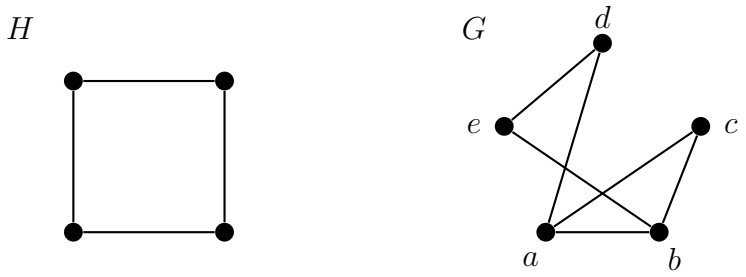
Now we claim that there are no edges between any two vertices in A or any two vertices in B. Suppose $y, z \in A$. If yz is an edge, then there since there is an even length walk from x to y (and likewise from x to z) then after taking an even length walk from x to y and then taking the edge yz, we end up with an odd length walk from x to z, which as we have mentioned, is impossible, since there can only be even length walks from x to z. Therefore, G is a bipartite graph with parts A and B $\square$

31 Lecture 12-6-2021

31.1 Subgraphs

Definition. Let H and G be graphs. We say that H is a **subgraph** of G, if the vertices of H are a subset of the vertices of G and the edges of H are a subset of the edge set of G. If H is a subgraph of G, then we denote this by $H \subset G$.

The definition of a subgraph is a very natural one, so let's do a few examples to get the idea across. A key part of determining whether one graph is a subgraph of another, is by labeling your vertices. A labeling, gives you a precise description of the vertex and edge sets, and therefore allows you to verify the definition of a subgraph directly. Suppose we are given the following two graphs H and G:

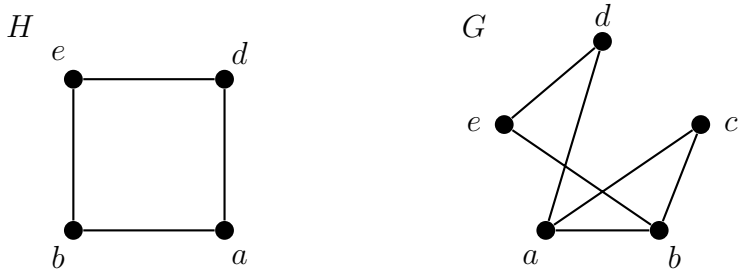


Is H a subgraph of G? Let V_H denote the vertex set of H and V_G denote the vertex set of G. Likewise, E_H and E_G will be the edges sets of H and G respectively. We observe that

$$\begin{aligned} V_G =& \{a, b, c, d, e\} \\ E_G =& \{ab, be, ed, da, ac, cb\}. \end{aligned}$$

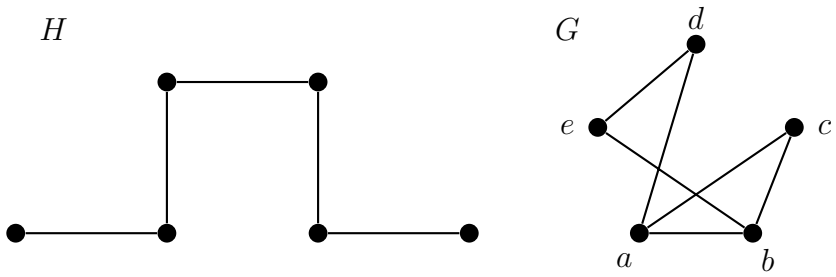
So now the question is, does there exist a labeling of the of the vertices of H, using the letters from V_G such that $V_H \subset V_G$ and $E_H \subset E_G$?

As it turns out, there is! Consider the following:



Using this labeling, we see that $V_H = \{b, c, d, e\} \subset V_G$ and $E_H = \{ed, da, ab, be\} \subset E_G$. Therefore, H *is* a subgraph of G.

Let's use the same graph G, but a different graph H and see if we can figure that one out. Consider:



Here H is actually just P_5, a path of length 5. It has 6 vertices and 5 edges. Now, is $H \subset G$? In this case, the answer, is no! The reason being, that H has more vertices than G. If we were to attempt to look for a path of lenght 5 in G, then G would need to have a*at least* 6 distinct vertices, but it does not. Since G has only 5 vertices, then it is not possible for H to be a subset of G.

Some criteria to keep in mind when attempting to determine whether one graph is a subgraph of another is the following.

Theorem 31.1.1. *Let H and G be graphs.*

- *If H has more vertices than G, then $H \not\subset G$.*
- *If H has more edges than G, then $H \not\subset G$.*
- *If the maximum degree amongst all vertices of H is larger than the degrees of all vertices in G, then $H \not\subset G$.*
- *If the degree sequence of G is $(g_1, g_2, \ldots, g_n)$ and the degree sequence of H is $(h_1, h_2, \ldots, h_m)$, and there exists an i such that $h_i > g_i$, then $H \not\subset G$.*

The list of potential criteria goes on, but these are some of the most common and useful one you can use.

This is the end of the material for the course, so I hope that you enjoyed it! I had a lot of fun preparing material, and it was a great experience. I hope you all can say the same. Keep working hard, and good luck with your finals this semester, and in your future course. :)

32 Appendix - Notation and LaTeX Commands

You will need to include a few packages in your code to make sure all the following notation works properly. This can be done by having this code in your preamble (that is, it should appear *before* `\begin{document}`.):

```
\usepackage{amsmath,enumerate, amsfonts, amssymb, amsthm}
```

All the following LaTeX code will need to be typed inside the *equation environment*. So you it will need to be inside `$ ----- $` the dollar signs.

32.1 Basics

- Superscripts, $3^5, x^a, (7x)^{n-1}$ - Tex Code: `3^5, x^a, (7x)^{n-1}`
- Subscripts, a_1, C_{k+1} - Tex Code: `a_1, C_{k+1}`
- Inequalities, $<, >, \leq, \geq, \neq$ - Tex Code: `<, >, \leq, \geq, \neq`
- Bold Font (no need for `$ $` environment, just use plain text), **THIS IS BOLD** - Tex Code: `\textbf{THIS IS BOLD}`
- Italic Font (no need for `$ $` environment, just use plain text), *This is Italic* - Tex Code: `\textit{This is Italic}`

32.2 Common Sets

- Natural Numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$ - Tex Code: `\mathbb{N}`
- Integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ - Tex Code: `\mathbb{Z}`
- Rational Numbers, $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}\}$ - Tex Code: `\mathbb{Q}`
- Real Numbers, $\mathbb{R}$, contains all rational numbers and all irrational numbers like square roots, and π, and many others. - Tex Code: `\mathbb{R}`
- Complex Numbers, $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\}$ - Tex Code: `\mathbb{C}`
- The Empty Set, $\emptyset$ - Tex Code: `\emptyset`

32.3 Logic Notation

- Not , $\neg$ - Tex Code: `\lnot`
- And (Conjunction), $\wedge$ - Tex Code: `\land`
- Or (Disjunction), $\vee$ - Tex Code: `\lor`
- Implies, $\rightarrow$ - Tex Code: `\rightarrow`
- If and only if, $\leftrightarrow$ - Tex Code: `\leftrightarrow`
- Logically Equivalent, $\iff$ - Tex Code `\iff`

32.4 Quantifiers

- There exists, $\exists$ - Tex Code: `\exists`
- For all, $\forall$ - Tex Code: `\forall`

32.5 Set Notation and Relations

- Curly Braces, $\{\dots\}$ - Tex Code: `\{ \}`
- In, Not in, $\in$, $\notin$ - Tex Code: `\in, \not\in`
- Subset, $\subseteq$ - Tex Code: `\subseteq`
- Super Set, $\supseteq$ - Tex Code: `\supseteq`
- Standard dots, $\dots$ - Tex Code: `\dots`
- Power Set, $\mathcal{P}(A)$ - Tex Code: `\mathcal{P}(A)`
- Not Equal, $\neq$ - Tex Code: `\neq`
- Set Difference, $A \setminus B$ - Tex Code: `A \setminus B`
- Proper Subset, either $\subset$ or $\subsetneq$ - Tex Code: `\subset or \subsetneq`, respectively
- Union, Intersection, $\cup, \cap$ - Tex Code: `\cup, \cap`
- Union from $i = 1$ to n, $\bigcup_{i=1}^{n}$ - Tex Code: `\bigcup_{i=1}^n`
- Intersection from $i = 1$ to n, $\bigcap_{i=1}^{n}$ - Tex Code: `\bigcap_{i=1}^n`
- Cartesian Product, $\times$ - Tex Code: `\times`
- Relations, $\mathcal{R}$ - Tex Code: `\mathcal{R}`
- Equivalent, Equivalence relation, $\sim$ - Tex Code: `\sim`
- Equivalence Class, Line on top, $\overline{x^2 + y^2}$ - Tex Code: `\overline{x^2 + y^2}`

32.6 Functions

- Floor Function, $f(x) = \lfloor x \rfloor$ - Tex Code: `f(x) = \lfloor x \rfloor$`
- Ceiling Function, $f(x) = \lceil x \rceil$ - Tex Code: `f(x) = \lceil x \rceil$`