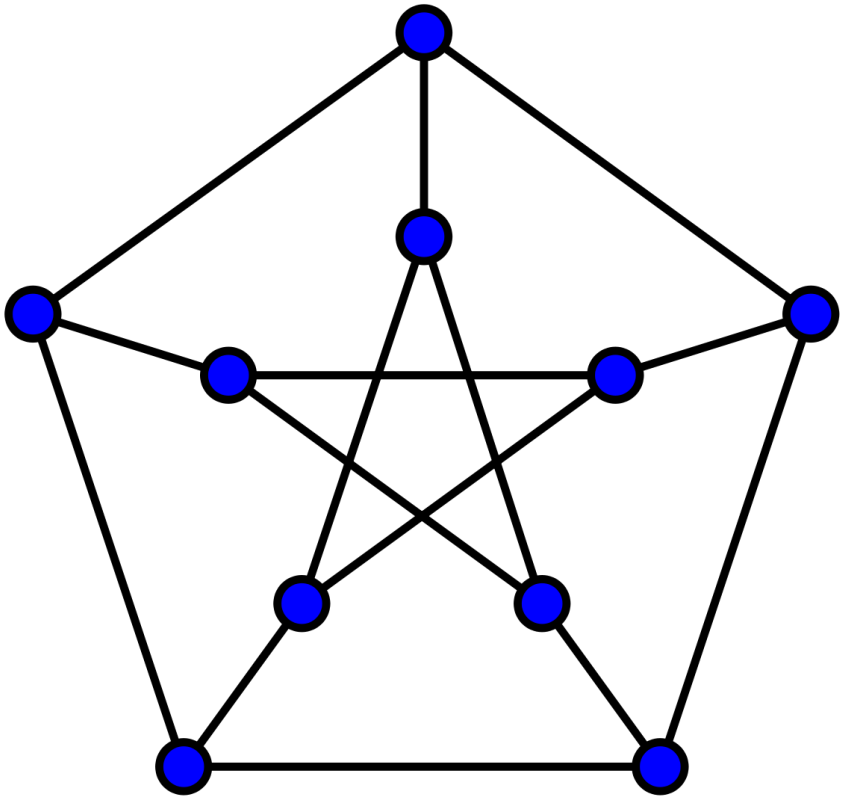
Discrete Math for Engineers (MTH 314): Notes

Adam Szava

Winter 2022

Introduction

This document is a compilation of my notes from Discrete Math for Engineers (MTH 314) from Ryerson University. All information comes from my professor's lectures, the course textbook *Discrete Mathematics by Anthony Bonato*, and online resources.



Contents

1 Chapter 1: Sets and Logic

1.2: Sets

This course begins with the study of sets, and operations we can apply to sets. This forms a basis for the rest of the course (and essentially all of mathematics).

Definition 1.2.1 Sets

A set is an unordered collection of things which doesn't consider repetition.

Each *thing* in a set is called an *element* of that set. We can explicitly define a set by writing out its elements between curly braces:

$$\{\text{element } 1, \text{element } 2, \ldots, \text{element } n\}$$

For example (let's say A is another set):

$$S = \{4, \text{"}apple\text{"}, A\}$$

Here, S is a set which contains three elements:

- The number 4 is an element of S, written as:

$$4 \in S$$

- The string "apple" is an element of S, written as:

$$\text{"apple"} \in S$$

- The set A is an element of S, written as:

$$A \in S$$

The takeaway from this example is that elements of a set can be number (as we have studied before) but they can also by any "thing" you are studying. In linear algebra they were often vectors.

There are a few important sets but before that we want to talk about an important definition regarding sets, a way to think about how *big* a set is compared to another:

Definition 1.2.2 Cardinality

Given a set A, $|A|$ is equal to the number of elements in A.
$|A|$ is called the *cardinality* of A.

For example:

$$\left|\{3,4,5,6\}\right| = 4$$

$$\left|\{3,4,5,5\}\right| = 3$$

The following are some important sets with their cardinality:

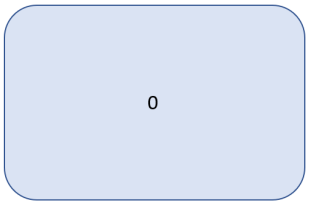
Set Name	**Symbol**	**Description**	**Cardinality**
Null Set or Empty Set	$\emptyset$	The set which contains no elements.	0
Set of Natural Numbers	$\mathbb{N}$	$\{0,1,2,3,...\}$	∞
Set of Integers	$\mathbb{Z}$	$\{\ldots,-2,-1,0,1,2,...\}$	∞
Set of Rational Numbers	$\mathbb{Q}$	The set which contains every possible fraction.	∞
Set of Real Numbers	$\mathbb{R}$	This set extends $\mathbb{Q}$ with irrationals.	∞
Singleton	$\{x\}$	The set which contains one element x.	1
Doubleton/Unordered Pair	$\{x,y\}$	The set which contains two elements x and y.	2

It is important to note that $\emptyset \neq \{0\}$. The empty set contains no elements, the set on the right contains one element, that being 0. Another important thing to consider is that $\emptyset \neq \{\emptyset\}$ the difference between these two sets is the same as the difference between an empty box and a box which contains an empty box.

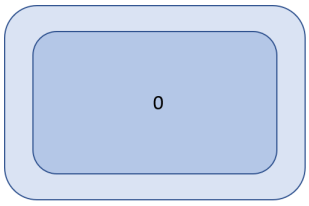
The best way to think about sets is by imagining a box. This will help you in understanding the difference between expressions like:

$$\{0\} \quad \{\{0\}\} \quad \{0,\{0,\{0\}\}\}$$

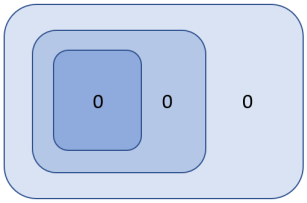
- The first set is the set which contains zero. Think of this as a box which contains the number 0. You can visualize this as follows:



- The second set is the set which contains the set which contains 0. Here, we have a box within a box, a set within a set. You can visualize this as follows:



- The third set contains two elements, one is 0 and the other is another set. This inner set contains two elements as well, another 0 and another set. This third inner set contains only one element which is the number 0. This can be visualized as:



Each blue box in the images represents a set.

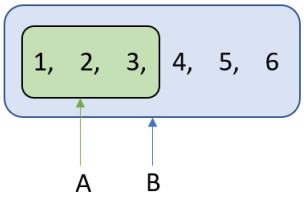
Subsets

If all the elements of one set is contained within another, like for example if:

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

$$B = \{1, 2, 3, 4, 5, 6\}$$

Which can be visualized as:



We say that A is a subset of B denoted $A \subseteq B$.

Definition 1.2.3 Subset

Given two sets A and B, we say that A is a subset of B if all the elements of A are contained within B, denoted:

$$A \subseteq B$$

We say that A is a proper subset of B if there is at least one element of B which is not in A (as in A and B are not the same sets). Proper subsets are denoted:

$$A \subsetneq B$$

We can express in symbols how the sets mentioned above relate to each other:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

As evident by considering this last example, subsets (also called inclusion) are transitive:

Theorem 1.2.1 Transitivity of Inclusion

Given three sets X, Y, and Z, and if:

$$X \subseteq Y$$

and:

$$Y \subseteq Z$$

then:

$$X \subseteq Z$$

Set Builder Notation

Set builder notation is used to describe more complex sets, or specified subsets of larger sets. For example if I want all the even integers, I would denote this as:

$$S = \{n \in \mathbb{Z} \mid n \text{ is even}\}$$

Generally if I want all the elements of a set A with some desired property I would write:

$$S = \{x \in A \mid x \text{ has the desired property}\}$$

For a more abstract example consider all the humans on Earth named Tom. The set describing them (given the set E which contains all humans on Earth) would be:

$$T = \{\text{Person} \in E \mid \text{Person is nammed Tom}\}$$

Set Equality

Two sets are equal if they have exactly the same elements as each other (regardless of order or repetition).

Definition 1.2.4 Set Quality

Given two sets A and B, we say they are equal if every element in A is also in B ($A \subseteq B$) and every element in B is also in A ($B \subseteq A$).

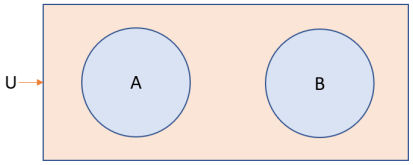
1.3: Operations on Sets

Now we will consider some important operations you can apply to sets. This lets us combine sets in some logical way. We will go through each operation one at a time.

Universe

Before we begin with operations, we need to understand the idea of a *universe*. Given some set A it contextually belongs within another set called it's universe. For example if we are talking about sets of whole numbers, we may assume our universe is the set of all natural numbers. The choice of universe is contextual, and so its definition can change. One thing is generally true about it, every set considered in the question is a subset of it. This is important in the first operation.

Visually you can think of the universe as a box which holds all of the other boxes, for example if a set A and a set B are part of some universe U it would look like:

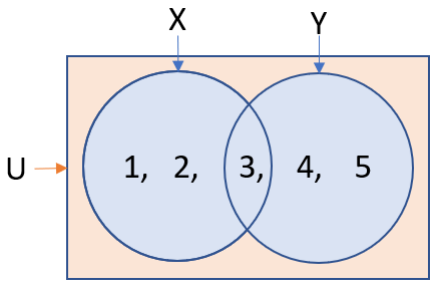


This is called a Venn diagram and it shows how the universe U contains two sets A and B. In this case the two sets do not share any elements, and so are distinct, which is not generally true.

A real example of a universe in action would be the following sets X and Y begin in the universe U:

$$X = \{1, 2, 3\}$$
$$Y = \{3, 4, 5\}$$
$$U = \{1, 2, 3, 4, 5\}$$

Which can be visualized as:



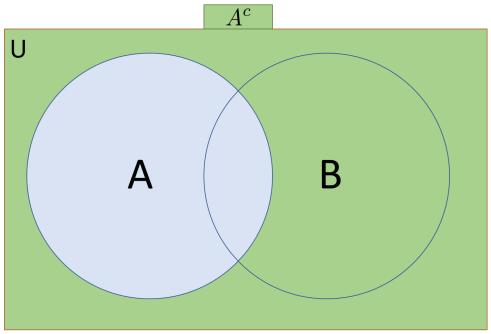
In this case the two sets do share some elements and so there is a portion of the diagram where the two sets are overlapping.

Complement

Definition 1.3.1 Complement (NOT)

Given some set A in a universe U, it's complement, denoted A^c, is the set of all elements in U but not in A. That is:

$$A^c = \{x \in U \mid x \notin A\}$$



The idea of a universe is especially important for this definition. By complementing a set we are essentially making a set of all the elements that are **not** in the original set. But then you have to ask "What are we considering?". If I were to ask "What are all the elements **not** in $\{1, 2, 3\}$"?

Certainly the following elements are not in that set:

- 4
- -5
- π
- "apple"

- The document you are reading right now.

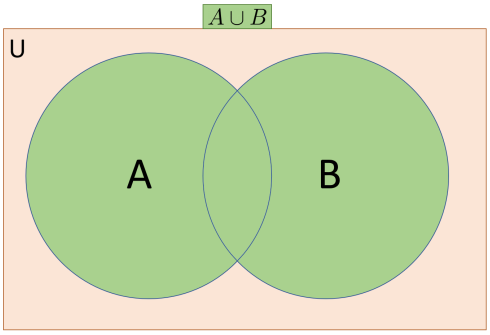
The list of all the things not in a set is uncountably infinite. So we need to specify that when we are taking the complement of a set, we want all the elements **not** in that set, *but still* within our contextual universe U.

Union

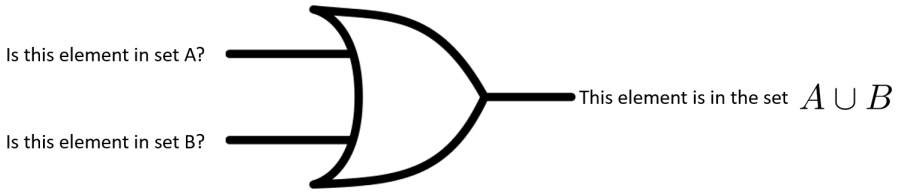
Definition 1.3.2 Union (OR)

Given two sets A and B, we can create a new set called A *union* B denoted $A \cup B$ defined as:

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$



You can think of the union of two sets as an OR gate applied to each of its elements:



Essentially, all the elements of the union are in either one of the two sets. For example, if:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$

Then:

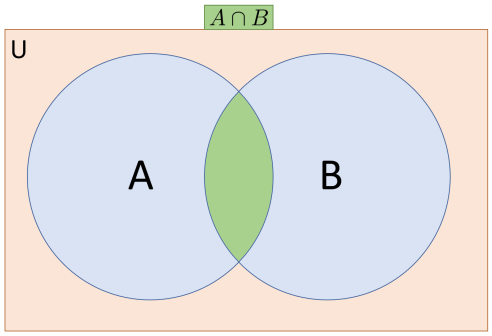
$$A \cup B = \{1, 2, 3, 4, 5\}$$

Intersection

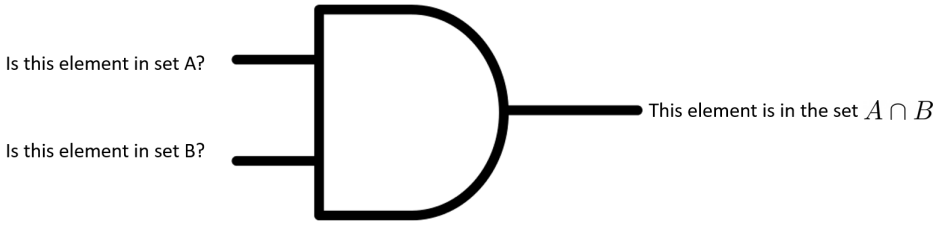
Definition 1.3.3 Intersection (AND)

Given two sets A and B, we can create a new set called A *intersection* B denoted $A \cap B$ defined as:

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$



You can think of the intersection of two sets as an AND gate applied to each of it's elements:



Essentially, all the elements of the intersection of two sets are the common elements to the sets. For example, if:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$

Then:

$$A \cap B = \{3\}$$

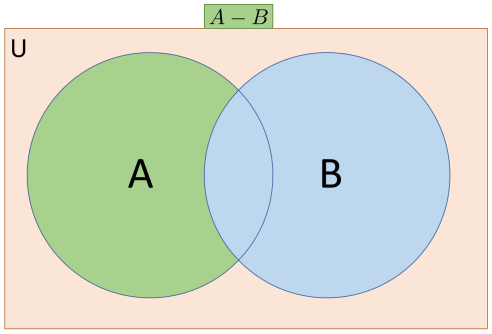
Note that if $A \cap B = \emptyset$ then the sets A and B share no elements, and we call them **disjoint**. The diagram on page 7 shows an example of such sets.

Difference

Definition 1.3.4 Difference

Given two sets A and B, we can create a new set called the *difference* of A and B denoted $A - B$ defined as:

$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}$$



You can think of the difference operation $A - B$ as all the elements of A but take away the elements that are also in B. For example, if:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$

Then:

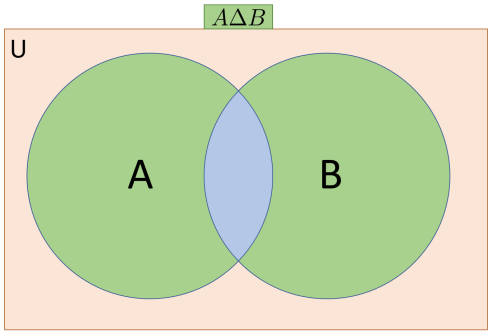
$$A - B = \{1, 2\}$$

Symmetric Difference

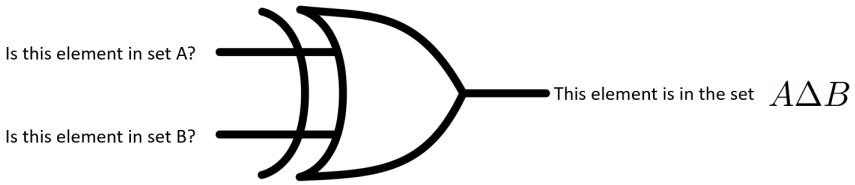
Definition 1.3.5 Symmetric Difference (XNOR)

Given two sets A and B, we can create a new set called the *symmetric difference* of A and B denoted $A\Delta B$ defined as:

$$A\Delta B = (A - B) \cup (B - A)$$



You can think of the symmetric difference of two sets as an XNOR gate applied to each of it's elements:



Essentially, all the elements of the symmetric difference of two sets are in either sets, but **not both**. For example, if:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$

Then:

$$A\Delta B = \{1, 2, 4, 5\}$$

Properties of the Set Operations

There are 12 main properties of the set operations. All sets in this subsection are subsets of the universe U.

1. *Commutative Laws*

   For all sets A and B:

   $$A \cup B = B \cup A$$
   $$A \cap B = B \cap A$$

2. *Associative Laws*

   For all sets A, B, and C:

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

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

3. *Distributive Laws*

   For all sets A, B, and C:

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

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

4. *Identity Laws*

   For every set A:

$$A \cup \emptyset = A$$

$$A \cap U = A$$

5. *Complement Laws*

   For every set A:

$$A \cup A^c = U$$

$$A \cap A^c = \emptyset$$

6. *Double Complement Law*

   For every set A:

$$(A^c)^c = A$$

7. *Idempotent Laws*

   For every set A:

$$A \cup A = A$$

$$A \cap A = A$$

8. *Universal Bound Laws*

   For every set A:

$$A \cup U = U$$

$$A \cap \emptyset = \emptyset$$

9. *De Morgan's Laws*

   For all sets A and B:

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$

10. *Absorption Laws*

    For all sets A and B:

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

11. *Complements of U and $\emptyset$*

$$U^c = \emptyset$$
$$\emptyset^c = U$$

12. *Set Difference Law*

    For all sets A and B:

$$A - B = A \cap B^c$$

Generalizing Intersections and Unions

Let's say we have n sets, listed:

$$A_1, A_2, A_3, \ldots, A_n$$

If we want to take the union of all of them we would write it as::

$$A_1 \cup A_2 \cup A_3 \cdots \cup A_n = \cup_{i=1}^{n} A_i$$

We can then think of this set as:

$$\boxed{\cup_{i=1}^{n} A_i = \{x \mid x \text{ is in some } A_i\}}$$

This is very similar to sigma notation for a sum.

You can do the exact same thing with intersections:

$$A_1 \cap A_2 \cap A_3 \cdots \cap A_n = \cap_{i=1}^{n} A_i$$

We can then think of this set as:

$$\boxed{\cap_{i=1}^{n} A_i = \{x \mid x \text{ is in all } A_i\}}$$

Now we define some new ideas relating to sets:

Definition 1.3.6 Mutually Disjoint Sets

Given sets $A_1, A_2, A_3, \ldots, A_n$ we say they are **mutually disjoint** if for all distinct i and j in $\{1, 2, 3, \ldots, n\}$:

$$A_i \cap A_j = \emptyset$$

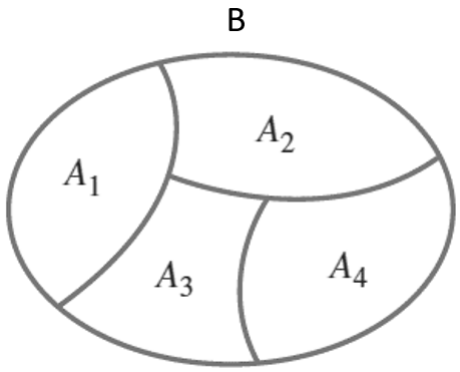
Given some collection of sets, we say they are mutually disjoint if you can pick any pair at random and regardless of which ones you pick they are disjoint (they share no common elements).

Definition 1.3.7 Partitions

Given sets $A_1, A_2, A_3, \ldots, A_n$ we say they **partition** a larger set B if:

- $A_1, A_2, A_3, \ldots, A_n$ are mutually disjoint.
- $$B = \cup_{i=1}^{n} A_i$$

You can partition a larger set into smaller sets by breaking the larger set into finitely many smaller sets *which don't overlap each other*. Each of those smaller pieces is called a *partition*. For example, if you break a set B into 4 partitions:



Power Sets

Definition 1.3.8 Power Sets

Given some set S, we define the set of all subsets to be $\mathcal{P}(S)$, called the **power set** of S.

For example given:

$$S = \{4, 5, 6\}$$

The power set is:

$$\mathcal{P}(S) = \{\emptyset, \{4\}, \{5\}, \{6\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, \{4, 5, 6\}\}$$

Note that the empty set is a subset of every set, and so it is an element of every power set.

You can intuitively thing of the power set of S as the set of all ways you can pick out elements from the set S (of size n), for example:

- You can pick out nothing ($\emptyset$)
- You can pick out any single element (all the singletons).
- You can pick out any pair (all the doubletons)

$$\vdots$$

- You can pick out any $n - groupings$ (all the $n-$tons)

Theorem 1.3.1 Cardinality of $\mathcal{P}(S)$

Given a set S where:

$$|S| = n$$

... then:

$$\left|\mathcal{P}(S)\right| = 2^n$$

Cartesian Product

The Cartesian product of two sets is another operation which can be applied to two sets. Essentially, the Cartesian product is the set of all **ordered pairs** which consist of one element from the first set, and one element from the other.

Definition 1.3.9 Cartesion Product

Given two sets A and B, we define the **Cartesian product** of the two sets as:

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

For example, we are very familiar with:

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$

...which is the set of all point on the Cartesian plane.

(Small side tangent incoming...) Now consider $\mathcal{P}(\mathbb{R}^2)$, this is the set of all subsets on the plane. This power set contains anything the can every be drawn on a piece of paper. It contains every book, every picture (in black and white), and the answer to every question.

1.5: Logic

Logic is the structure that holds all of mathematics together. Mathematics as a whole can be thought of as an applied form of logic. This section introduced a basic look into logic.

Logic begins with the idea of a statement, in this definition *sentence, true,* and *false* are left undefined (on purpose because that would get too philosophical):

Definition 1.5.1 Statement

A statement is a sentence which is either true or false.

We typically represent statements as variables, for example we can let P be the statement: $f(x) = x^2$ is continuous.

We connect statements together using *connectives*. The first two connectives are logically identical to AND and OR gates from COE 328. The other connectives take some more thought:

Definition 1.5.2 Connectives

Let P and Q be statements. Then we define the following *connectives*:

1. $P \wedge Q$ means: P and Q, called a *conjunction*. $P \wedge Q$ is true exactly when both P and Q are true.
2. $P \vee Q$ means: P or Q, called a *disjunction*. $P \vee Q$ is true exactly when one of P or Q is true.
3. $P \to Q$ means: if P then Q, called an *implication*. P is the *hypothesis*, and Q is the *conclusion*. $P \to Q$ is false exactly when P is true and Q is false, in all other cases it is true.
4. $P \iff Q$ means: P if and only if Q, called a *biconditional*. $P \iff Q$ is true exactly when both P and Q are true, or P and Q are false.
5. $\neg P$ means: not P, called a *negation*. $\neg P$ is true exactly when P is false.

For example, given that:

$$P = \text{You speak english.}$$

$$Q = \text{You were born in Canada.}$$

Notice that we are not necessarily saying P or Q is true. Similarly, when we make connectives determining if they are true is a whole separate discussion. We are just currently looking at what the notation means...

- $$P \wedge Q = \text{You speak english and you were born in Canada.}$$

  This statement is only true when you speak English and you were born in Canada.

- $$P \rightarrow Q = \text{If you speak English, then you were born in Canada}$$

  This statement is only false when you speak English, but you were not born in Canada. **Important:** Notice that if you do not speak English the statement defaults to true.

- $$P \iff Q = \text{You speak English if and only if you were born in Canada.}$$

  This statement is true if you speak English, and were born in Canada, OR if you do not speak English and were not born in Canada.

Definition 1.5.2 Eqivalent Statements

Two statements P and Q are equivalent if they are true at the same time. We denote this:

$$P \equiv Q$$

There are some basic laws which we can use regarding *connectives*:

Theorem 1.5.1 Connective Laws

Let P, Q, and R be statements. We then have:

1. *Idempotent Laws:*

$$P \wedge P \equiv P$$

$$P \vee P \equiv P$$

2. *Double Negation Laws:*

$$\neg(\neg P) \equiv P$$

3. *Commutative Laws:*

$$P \wedge Q \equiv Q \wedge P$$

$$P \vee Q \equiv Q \vee P$$

4. *Associative Laws:*

$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$

5. *Distributive Laws:*

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

6. *De Morgan's Laws:*

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

7. *Absorption Laws:*

$$P \vee (P \wedge Q) \equiv P$$

$$P \wedge (P \vee Q) \equiv P$$

8. *Implication Law:*

$$P \to Q \equiv \neg P \vee Q$$

Statements like $3 = x + 3$ are sometimes true (in this case when $x = 0$). Sometimes statements are always true, like "$1 = 1$", other times statements are always false, like "$1 = 0$". We have special names for these cases:

Definition 1.5.3 Tautologies and Contradictions

A **tautology** is a statement that is always true, regardless of the truth of the individual statemenets that comprise it.
A **contraidction** is a statement that is always false, regardless of the truth the of the individual statements that comprise it.

Variations of Implications

Given some implication, like:

If the sky is blue, then its day time.

We may consider some logical rearrangements of it, like:

If it is day time, then the sky is blue.

... or:

If it is not day time, then the sky is not blue.

The first logical rearrangement is called the *converse* of the implication, while the second one is called the *contrapositive* of the implication.

Definition 1.5.4 Converse and Contrapositive

Given some implication $P \to Q$:
The **converse** of the implication is the implication $Q \to P$.
The **contrapositive** of the implication is the implication $\neg Q \to \neg P$.

Necessity and Sufficiency

Forgive the next two examples, they illustrate the idea so I went with it...

It is absolutely *necessary* for you to have fingers to play piano. Therefore, if someone is playing piano, we know with certainty that they have fingers, therefore playing piano *implies* having fingers.

Definition 1.5.5 Necessity

If the statement P is necessary for Q to occur, then:

$$Q \to P$$

If you want to climb a wall, there are many ways you can do it but it is *sufficient* to have a ladder. Having a ladder tall enough implies that you can climb the wall.

Definition 1.5.6 Sufficiency

If the statement P is sufficient for Q to occur, then:

$$P \to Q$$

Predicate

The statement:

$$4 = x + 4$$

Is *technically* not a statement until you actually try to assign a value. This is because the above statement is not simply *True* or *False*, its "truth value" depends on what you choose for x. Once you make a choice for x then it becomes either true or false, and so it is a statement. So if our original sentence is not a statement, what is it? It is called a *predicate*.

Definition 1.5.7 Predicate

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The *domain* of a predicate variables is the set of all values that may be substituted in place of the variable.

Quantifiers

But what if our predicate is true/false for all choices of our variable? For example in the predicate:

$$x + x = 2x$$

Regardless of the choice of real number x, the predicate is true, and so we must be able to convert it to a statement without substituting in a value for x. We

want to be able to say: *For all x values, $x + x = 2x$.* You can write that as:

$$\forall x(x + x = 2x)$$

Definition 1.5.8 Universal Quantifier

The **universal quantifier** is $\forall$ and is read "for all". A universal statement $\forall x P(x)$, where $P(x)$ is a predicate, means that for all x in the domain, the predicate $P(x)$ holds true. For $\forall x P(x)$ to be true, the predicate must hold for all choices of x in the domain of $P(x)$. If there is some x in the domain for which $P(x)$ is false, then $\forall x P(x)$ is false, and the choice of x is called a *counterexample*.

What if we don't want to talk about the exact solution to $x + 2 = 3$, rather we want to just talk about the face that the statement has a solution. We want to be able to say: *There exists a value x, such that $x + 2 = 3$.* You can write that as:

$$\exists x(x + 2 = 3)$$

Definition 1.5.9 Existential Quantifier

The **existential quantifier** is $\exists$ and is read "there exists". A existential statement $\exists x P(x)$, where $P(x)$ is a predicate, means that for some x in the domain, the predicate $P(x)$ holds true.
For $\exists x P(x)$ to be true, the predicate must hold for some choice of x in the domain of $P(x)$. If there is no x in the domain for which $P(x)$ is true, then $\exists x P(x)$ is false.

One important final note is the negation of the quantifiers. The negation of $\forall x P(x)$ means that there exists some x in the domain such that $P(x)$ is false, as in:

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

The negation of $\exists x P(x)$ means that there is no x in the domain such that $P(x)$ is true, as in:

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

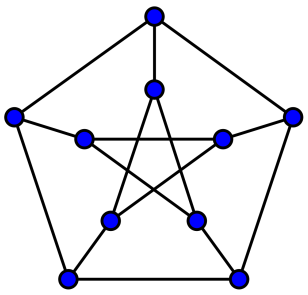
2 Chapter 2: Graphs and Trees

2.1: Introduction to Graphs

Graphs are ways to study the relationship between objects. They serve as a basis for a lot of algorithms in computer science. In this course, we look at a

very surface level introduction to the mathematics of graphs.

Informally, a graph is a collection of nodes (vertices) and lines which connect those dots in some way (edges), for example:



Given this informal understanding, we want to formalize some ideas so we can speak more precisely about graphs.

Definition 2.1.1 Graphs

A **graph** G is a pair of sets, one being the *vertex set of* G $V(G)$, and the other being the *edge set of* G $E(G)$. If G is clear from context we denote the graph G as:

$$G = (V, E)$$

Notice how this matches with our earlier informal definition of how a graph is a combination of two things: nodes and lines.

Definition 2.1.2 Edge Notation

Given vertices u and v, we write uv to denote the edge joining vertex u and v. We say that u and v are thus adjacent. Further, we say that vertices u and v are incident with the edge uv, and that u and v are *endpoints* of that edge uv.

Notice that we can think of edges as a binary relation on the vertices. The edge set is just a list of pairs of vertices which are *related* to each other through the edge.

We now want a way to quantify the size of a graph as compared to other graphs. We do this using the following definitions:

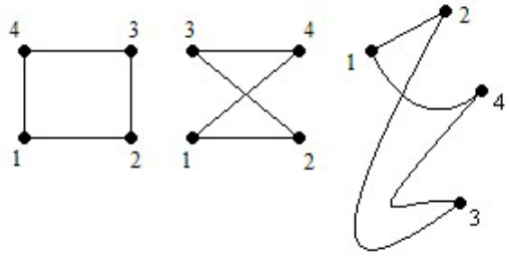
Definition 2.1.3 Order and Size of a Graph

The **order** of a graph G is $\big|V(G)\big|$.
The **size** of a graph G is $\big|E(G)\big|$.

We assume in this course that all graphs have finite size and order. Further, we assume that all graphs are *simple*, meaning:

- No edges from a vertex to itself (called a loop).
- At most one edge between vertices.

We commonly choose to represent graphs visually, with dots as vertices and lines as edges. However they are more of an abstract idea of the relationship between objects. While drawing a graph, you can move vertices, stretch edges, curve edges, and apply any other isomorphism (a change which can be reverted) to the drawing. As long as the vertices and edges are maintained it is the same graph. For example the three following graphs are equivalent:



2.2: Degrees

In the previous section we defined the *degree* of a graph. In this section look at another definition of *degree* being the degree of a **vertex**.

Definition 2.2.1 Degree of a Vertex

Given a graph G and a vertex v from the set $V(G)$, we define the degree of v ($deg_G(v)$) to be the number of edges incident with v.

We only consider one theorem relating to graphs in the course. This theorem shows that there must be a certain relationship between edges and vertices.

Theorem 2.2.1 First Theorem of Graph Theory

If G is a graph, then:

$$\sum_{u \in V(G)} deg_G(u) = 2\big|E(G)\big|$$

This means that the sum of all the degrees of all the vertices is equal to twice the number of edges. This fact is true if you think about how each edge will give you two vertices, and so it will count for two in the sum.

A corollary of this theorem is that the number of odd degree vertices in a graph must be even, otherwise the graph doesn't exist.

3 Chapter 3: Relations and Functions

3.1: Introduction to Relations

In this section we define what a relation is and how you form them.

We will talk abut relations informally, then give the formal definition. Given two sets A and B we want to be able to show that certain elements are related to each other. The way in which the two sets are related to each other is called a **relation** R. For example, given the two following sets:

$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{6, 7, 8, 9, 10\}$$

... and let's say a relation R between these sets is given by:

$$R : \text{x is related to y} \iff x + y = 9$$

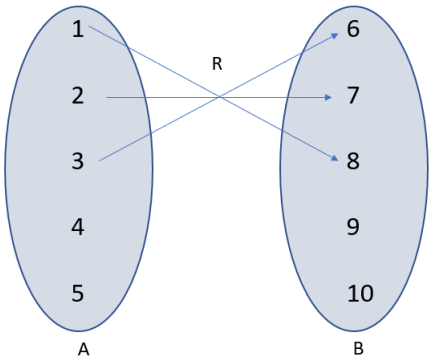
Note: we denote *x is related to y by R* as:

$$xRy$$

Then we can see that:

- $$1R8$$
- $$2R7$$
- $$3R6$$

We often want to draw a diagram to help understand the relation. We draw the relation as arrows connecting elements from the two sets.



Note that we can think of the elements which are related to each other as ordered pairs, as in:

$$1R8 \to (1,8), 2R7 \to (2,7), 3R6 \to (3,6)$$

Thinking about them in this way, you can see that they are all elements of $A \times B$. This relation is just a subset of $A \times B$, in fact all relations between A and B are subsets of $A \times B$, as in the following formal definition:

Definition 3.1.1 Binary Relations

Given sets A and B, a *binary relation* R from A to B is a subset of $A \times B$. R is a set of ordered pairs (a, b) with $a \in A$ and $b \in B$. We write aRb if $(a, b) \in R$.

A set can also be related to itself:

Definition 3.1.2 Properties of Relations

We say that R is a binary relation on A if R is a subset of $A \times A$.

The following are two mini-definitions:

- A **function** is a special kind of binary relation from A to B such that for each $a \in A$ there is a *unique* $b \in B$ such that aFb. Of course we typically write aFb as $f(a) = b$.
- We can also define the inverse of a relation R as R^{-1}, which can be written as:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

3.2: Properties of Relations

Given a *binary relation* R on A, we can define three useful properties it can have:

Definition 3.2.1 Binary Relations on a set A

Given a relation R on A:

- R is **reflexive** if for all $a \in A$, aRa.
- R is **symmetric** if for all $a, b \in A$, $aRb \iff bRa$.
- R is **transitive** if for all $a, b, c \in A$, $aRb \wedge bRc \to aRc$

A relation which is reflexive, symmetric, and transitive is called an **equivalence relation**.

Here are two examples of equivalence relations:

- For $x, y \in \mathbb{R}$, $xRy \iff x = y$.
  - **Reflexive:** $x = x$.
  - **Symmetric:** $x = y \iff y = x$.
  - **Transitive:** $x = y, y = z \to x = z$.
- For lines ℓ_1 and ℓ_2, $\ell_1 R \ell_2 \iff \ell_1 \parallel \ell_2$.
  - **Reflexive:** a line is parallel to itself.
  - **Symmetric:** if $\ell_1 \parallel \ell_2 \to \ell_2 \parallel \ell_1$.
  - **Transitive:** if $\ell_1 \parallel \ell_2, \ell_2 \parallel \ell_3 \to \ell_1 \parallel \ell_3$.

Now we discuss **equivalence classes** which can be constructed from *equivalence relations*.

Definition 3.2.2 Equivalence Classes

Given an equivalence relation R on a set A. For each $a \in A$.
we denote the **equivalence class** of a, by:

$$[a] = \{b \in A \mid aRb\}$$

Informally we think of the equivalence class of a as the set of all the elements in relation to a.

For example, the equivalence class of a line ℓ_1 denoted $[\ell_1]$ (using the parallel equivalence relation) is the set of all lines with the same slope.

Here are some properties of equivalence classes:

Theorem 3.2.1 Properties of Equivalence Classes

Given an equivalence relation R on a nonempty set A.

- For all $a \in A, [a] \neq \emptyset$.
- If xRy, then $[x] = [y]$.
- If $(x, y) \notin R$, then $[x] \cap [y] = \emptyset$.

Once again consider the equivalence relation between lines of parallelism. We verify all the properties by:

- The equivalence class of any line is not empty since every line is parallel to itself.
- If two line are related to each other, then they have the same slope and so are both related to all other lines with this slope.
- If two lines are not related to each other, this means they have different slopes. Since an equivalence class of a line contains all lines which have the same slope, the intersection of two equivalence classes with different sloped lines is the null set.

In a sense, we are partitioning the set of all lines into an infinite number of disjoint sets (one for every possibles slope) who's union is the set of all lines. This is the exact definition of a partition.

Theorem 3.2.2 Equivalence Classes as Partitions

The set of all equivalence classes of an equivalence relation R on a set A forms a partition of A.

But how do we find this equivalence relation?

Theorem 3.2.3 Partitioning Equivalence Relation

Let P be a partition of a set A. Define *the equivlence relation induced by* P to be R_P, defined as:

$$aR_Pb \iff x \text{ and } y \text{ are in the same partition.}$$

Then R_P is an equivlence relation.

For example, given the set $A = \{1, 2, 3\}$ with a partition P of $\{\{1, 2\}, \{3\}\}$. Then we have that R_P begin all the combinations of elements in the same partition:

$$R_P = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$$

Note that the first set of the partition is [1] and also [2], while the second set is [3].

3.3: Partial Orders

Partial orders give us a way to rank objects. Given some set of object, we can denote that one succeeds another using a partial order. We typically think about partial orders as a graph for convenience (More on this later). First we define a new property:

Definition 3.3.1 Antisymmetry

Let R be a binary relation on a set A. We say that R is *antisymmetric* if aRb and bRa implies that $x = y$.

A relation being antisymmetric means that it is only symmetric if the elements are the same.

Definition 3.3.2 Partial Order

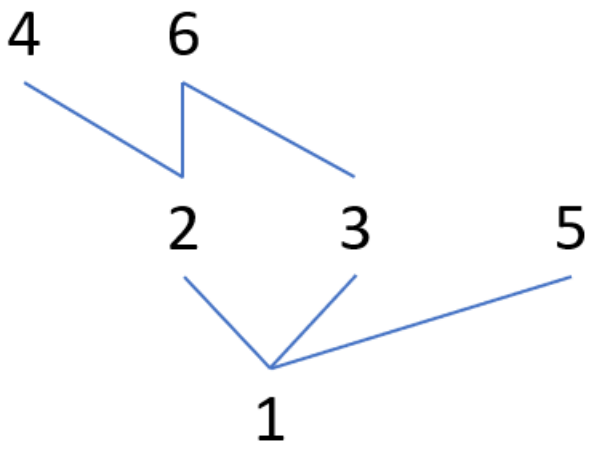
A binary relation R on a set A is a **partial order** if it is reflexive, antisymmetric, and transitive.
We use the symbol $\preceq$ to denote this relation.

Given this definition, we look at partial orders as a way to compare elements in a set. If two elements are related by the partial order R (either directly of transitively) we define those two object as **comparable**, otherwise they are **incomparable**. If every pair of element is comparable, then the partial order is called a **total order**.

To get an idea of what a partial order is, we use *Hasse* diagram. A *Hasse* diagram is a *directed graph* where:

- All directed edges point up (as to visually represent a hierarchy).
- Loops are omitted.
- Directed edges due to transitivity are omitted.
- All arrows are eliminated (since we made them all point up anyway).

For example, if we are given the set $\{1, 2, 3, 4, 5, 6\}$ and the partial order $|$ (the divides relation), then the *Hasse* diagram would be:



We then have a bunch of definitions for ways the think about the greatest, and least elements in the entire partial order, or just parts of it:

Definition 3.3.3 Maximal and Minimal Elements

Given a partial order $\preceq$ on A:

- An element $a \in A$ is **maximal** if for each $b \in A$, either $b \preceq a$ or a and b are incomarable.
- An element $a \in A$ is the **greatest element** if for each $b \in A$, $b \preceq a$.
- An element $a \in A$ is **minimal** if for each $b \in A$, either $a \preceq b$ or a and b are incomparable.
- An element $a \in A$ is called the **least element** if for each $b \in A$, $a \preceq b$.

So for example, in the *Hasse* diagram above:

- 1 is the least element and is minimal.
- $4, 5, 6$ are maximal elements.

3.4: Functions

We are very familiar with functions from our calculus classes, here we will just look at functions from the perspective of binary relations.

The idea is we think of the relation as a *map* or a *correspondence* between an element from some set $a \in A$ and some set $b \in B$, and aRb means they correspond to each other. The added restriction is that there can only by one b for every a.

Definition 3.4.1 Functions

A **function** f from a set A to a set B, usually denoted:

$$f \mid A \to B$$

... is a relation between elements of the set A (called the **domain**) and elements of the set B (called the **codomain**), so that for all elements $a \in A$ there is a *unique* element $b \in B$ that is related to a by f.

Typically we write $y = f(x)$ in which case we are thinking of y as the *image of* x *under* f, meaning that x gets sent to by the influence of f.

Very importantly, codomain is **not** necessarily the same thing as range. Codomain the set of all possible outputs from the function (what universal set those outputs belong to) while the *range* (which we define next) also called the *image* is the set of all the elements of the codomain that **actually** get mapped to.

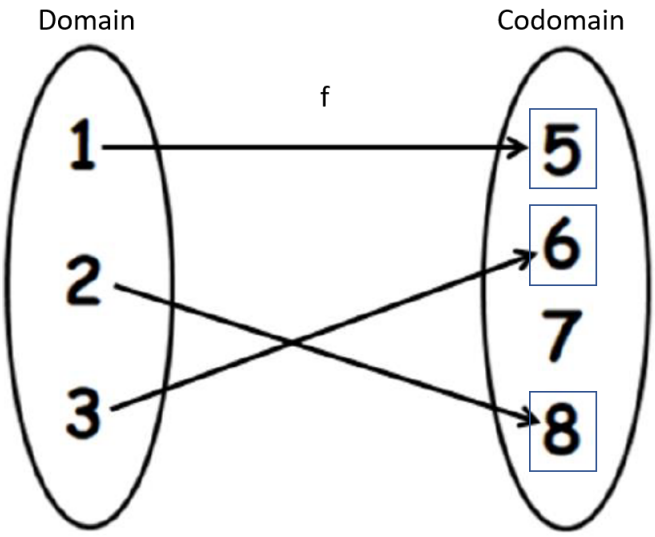
Definition 3.4.2 Range

The **range** of a function f on a set A (also called the **image**) is defined as:

$$\{b \in B \mid b = f(a) \text{ for some } a \in A\}$$

The **range** of a function is always a subset of the codomain.

Consider the following example of a function, draw with a mapping diagram. The domain and codomain are labelled, as well as the **range** being the boxed elements of the codomain.



The image of a element of the domain under the function f is the element in the codomain which corresponds to the element in the domain. The inverse image is the opposite.

Definition 3.4.3 Inverse Image

Given a function $f \mid A \to B$ and $b \in B$, define **the inverse image of b** as:

$$\{a \in A \mid f(a) = b\}$$

In other words, the inverse image of an element is a **set** of all the elements which map to it. This set *could* be a singleton (as we will see it is a singleton for injective functions). The inverse image is a subset of the domain of f.

Given some subsets of the domain, we may ask what subset of the range (which itself is a subset of the codomain) is mapped to by this subset of the domain. We use the notation $f(U)$ given that $U \subseteq A$ to denote this subset:

Definition 3.4.4 Functions Acting on Sets

Given a function $f \mid A \to B$ and subsets $U \subseteq A$ and $V \subseteq B$, we define:

- $$f(U) = \{b \in B \mid b = f(u) \text{ for some } u \in U\}$$
  OR: The union of all the images of $u \in U$
- $$f^{-1}(V) = \{a \in A \mid f(a) = v \text{ for some } v \in V\}$$
  OR: The union of all the inverse images of $V \in V$

The image of a subset U of the domain is the subset of the range of the function which results from mapping elements of that subset U. The inverse image of a subset V of the codomain is a subset of the domain which results from finding the inverse image of elements of that subset V.

Injective, Surjective, and Bijective Functions

A function is **injective** or **one-to-one** no distinct pair of elements of the domain map to the same element in the range.

Definition 3.4.5 Injective/One-to-One

A function $f \mid X \to Y$ is **injective** or **one-to-one** if:

$$\forall a, b \in X \mid \text{if } f(a) = f(b) \to a = b$$

... or equivalently:

$$\forall a, b \in X \mid \text{if } a \neq b \to f(a) \neq f(b)$$

A function is **surjective** or **onto** if the range is equal to its codomain, as in the function maps *onto* all of the codomain.

Definition 3.4.6 Surjective/Onto

A function $f \mid X \to Y$ is **surjective** or **onto** if:

$$\forall b \in Y \exists a \in X \mid f(a) = b$$

Equivalently we say the range of f is Y. The example above is **injective** but not **surjective**.

To show that a function is *surjective*, start with the general form of an element in Y and try to solve for the corresponding element in X.

In the case where a function is both, we say that it is **bijective**.

Definition 3.4.7 Bijections

A function $f \mid X \to Y$ is **bijective** if it is **injective** and **surjective**.

Bijective functions have inverse relations which are also functions. Given a function $f \mid X \to Y$, we define $f^{-1} \mid Y \to X$ so that for some $y \in Y$, $f^{-1}(y)$ is the unique element $x \in X$ such that $f(x) = y$.

4 Chapter 4: Combinatorics

4.2: The Sum Rule

4.3: The Product Rule

4.6: Combinations

4.7: Pascal's Triangle

5 Chapter 5: Number Theory

5.1: Introduction to Number Theory

Number theory is the study of numbers, usually the integers. Here, we study properties of these numbers with some formality, and try to understand patterns that they exhibit.

The first definition (and the only thing in this section) is formally what we mean by *even* and *odd* numbers:

Definition 5.1.1 Parity

An integer x is even if $x = 2k$ for some integer k.
An integer x is odd if $x = 2k + 1$ for some integer k.

Simply put, an even number is a multiple of two, and an odd number is one number higher than an even number.

We then have the following theorem which talks about combining these types of numbers.

Theorem 5.1.1 Properties of Parity

- If x and y are both even, then so is $x + y$ and xy.
- If x is even and y is odd, then $x + y$ is odd.
- If x is odd and y is odd, then $x + y$ is even.
- x^2 is even if and only if x is even.

5.2: Divisors

Divisors are a fundamental part of number theory. We are often interested in if a number divides into another number or not. Divisors let us define useful types of numbers and algorithms.

Definition 5.2.1 Divisors

Given some integers a and b, we say that a *divides* b or: $a \mid b$ if:

$$a \mid b \iff b = ka, \text{ for some integer } k$$

We say that b is divisible by a, and that a is a divisor of b.

For example:

- $$5 \mid 30 \iff 30 = 6(5)$$
- $$-3 \div 12 \iff 12 = -4(-3)$$
- $$12 \div 12 \iff 12 = 1(12)$$
- $$3 \div 0 \iff 0 = 3(0)$$

Now we discuss a very important function in Number Theory, the *greatest common divisor* function takes in two numbers, are returns the largest divisor that both numbers have.

Definition 5.2.2 Greatest Common Divisors

The *greatest common divisor* of nonzero integers a and b is the largest integer that divides both a and b. We denote this $gcd(a, b)$.

For example:

- $$gcd(12, 8) = 4$$
- $$gcd(9, 18) = 9$$
- $$gcd(1, 4) = 1$$
- $$gcd(24, 16) = 8$$
- $$gcd(-16, 4) = 4$$
- $$gcd(0, a) = a$$

Notice in the last example we can let one of a or b be zero, but not both.

We now define what a prime number is, which is a fundamental idea to a lot of number theory:

Definition 5.2.3 Prime Numbers

A number $p > 1$ is prime if its only positive divisors are 1 and p. Otherwise the number is composite.
The first few prime number starting at 2 include:

$$2, 3, 5, 7, 11, 13, 17, 19 \ldots$$

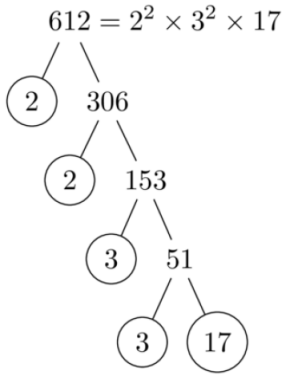
Prime numbers form a *periodic table of numbers* as every number (composite or prime) is made up of a **unique** product of prime numbers (called *prime factorization*). For example:

- $$15 = 3 \cdot 5$$

- $$100 = 5^2 \cdot 2^2$$

Note that we do not call 1 a prime number because if we did, then every number would not have a **unique** prime factorization, as you could multiply by 1 any number of times.

There are an infinite number of primes, and so every number, no matter how big, can be represented as its prime factorization. You can use the following diagram to visualize prime factorization:



5.3: The Euclidean Algorithm

The Euclidean algorithm is an algorithm to find $gcd(a, b)$ in a systematic way.

We use the fact that if a and b are integers with some divisor k, this means that we can write a and b as:

$$a = k \cdot ?_a \cdot ?_a \cdots ?_a$$

$$b = k \cdot ?_b \cdot ?_b \cdots ?_b$$

Where k is of course a factor of both numbers (since it is a divisor), but both numbers are also made up of some other numbers multiplied together (which I just represented as some question marks).

The important take away is that k is also a divisor of $b - a$ since:

$$b - a = (k \cdot ?_a \cdot ?_a \cdots ?_a) - (k \cdot ?_b \cdot ?_b \cdots ?_b) = k\left((?_a \cdot ?_a \cdots ?_a) - (?_b \cdot ?_b \cdots ?_b)\right)$$

Which is clearly also divisible by k. Therefore we can conclude that a, b and $b - a$ all have the same common divisors, and so have the same greatest common divisor, meaning:

Theorem 5.3.1 Simplifying GCDs

If a and b are integers that are not both zero, then:

$$gcd(a, b) = gcd(a, b - a)$$

We can use this theorem to reduce GCD question to smaller numbers, which makes it easier to compute. In fact we can apply this theorem as long as many times as we want to make the numbers as small as possible, which is the *Euclidean Algorithm*.

The following is a full example of using the Euclidean Algorithm to find greatest common divisors:

Example 5.3.1 Euclidean Algorithm

Find gcd(68,132)

Applying Theorem 5.3.1 (here on called "the theorem"):

$$gcd(68, 132) = gcd(68, 132 - 68) = gcd(68, 64)$$

Applying the theorem again (and switching the order of the numbers around):

$$gcd(64, 68) = gcd(64, 68 - 64) = gcd(64, 4)$$

... and again:

$$gcd(4, 64) = gcd(4, 64 - 4) = gcd(4, 60)$$

... and again (I skipped many iterations):

$$gcd(4, 8) = gcd(4, 8 - 4) = gcd(4, 4) = 4$$

Therefore:

$$\boxed{gcd(68, 132) = 4}$$

5.4: Linear Diophantine Equations

5.5: Congruences

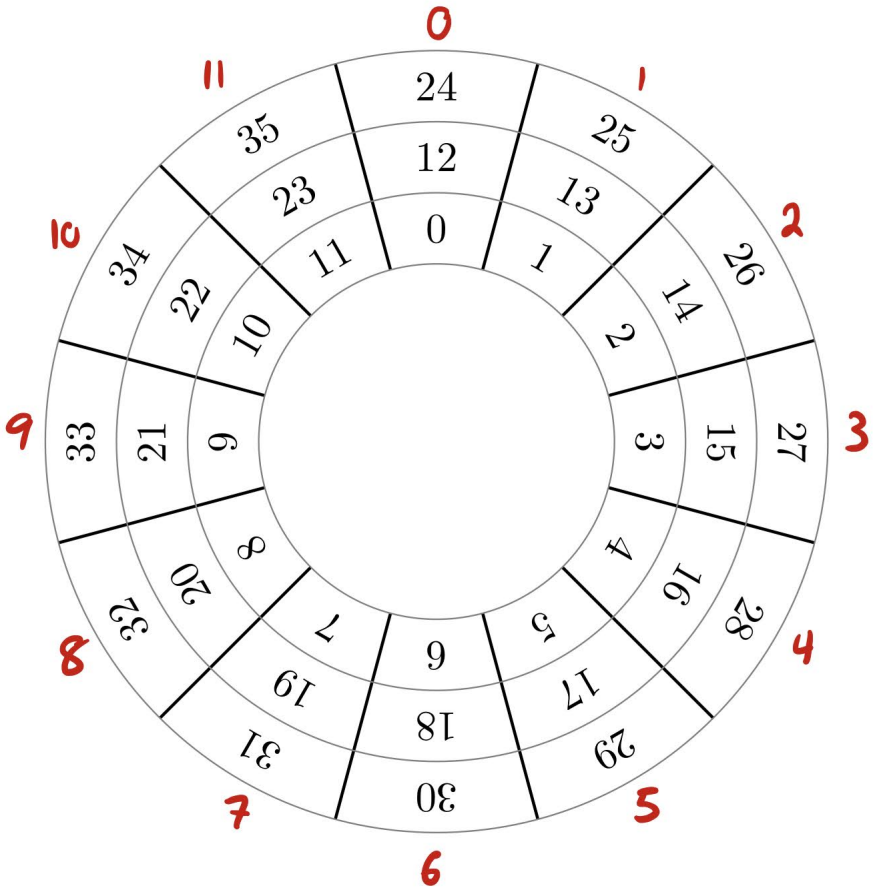
Congruence is an important equivalence relation which uses the divisibility of two numbers. When saying two numbers are congruent, we are saying that their remainder is the same when divided by some number n, or in other words, they are the same amount off of a multiple of n. In this sense 5 and 8 are *"the same"* since they are both 2 off from a multiple of 3 (we call this congruence mod 3). Below is the formal definition:

Definition 5.5.1 Congruence

Let n be a positive integer greater than one. We say that a is congruent to b modulo n, denoted: $a \equiv b(mod\ n)$ if:

$$a \equiv b(mod\ n) \iff m \mid (a-b) \iff a = b + km, k \in \mathbb{Z}$$

You can think of congruences as a clock, for example the following diagram shows the numbers *mod 12*:



All the numbers in the same "column" (labeled 0-11) are congruent to each other because they are the same distance away from a multiple of 12 (hence mod 12). For example:

- $$14 \equiv 2(mod\ 12)$$

- $$26 \equiv 2(mod\ 12)$$

Since both 14 and 26 are 2 above a multiple of 12. In general a great way to think about congruences is:

$$a \equiv b(mod\ n) \iff a \text{ is } b \text{ above a multiple of } n$$

This definition also allows for negative numbers, as in:

$$1 \equiv -3(mod\ 4)$$

Since 1 is 3 *below* a multiple of 4.

There are many properties of congruences, listed in the following theorem:

Theorem 5.5.1 Properties of Congruences

Given integers a, b, c, d and a positive integer n, we have:

- **Reflexivity:**
$$a \equiv a(mod\ n)$$
- **Symmetry:**
$$\text{If } a \equiv b(mod\ n) \text{ then } b \equiv a(mod\ n)$$
- **Transitivity:**
$$\text{If } a \equiv b(mod\, n) \text{ and } b \equiv c(mod\, n), \text{ then } a \equiv c(mod\, n)$$
- $$\text{If } a \equiv b(mod\ n), \text{ then: } a + c \equiv b + c(mod\ n)$$
- $$\text{If } a \equiv b(mod\ n), \text{ then: } ac \equiv bc(mod\ n)$$
- $$\text{If } a \equiv b(mod\, n) \text{ and } c \equiv d(mod\, n), \text{ then } a+c \equiv b+d(mod\, n)$$
- $$\text{If } a \equiv b(mod\, n) \text{ and } c \equiv d(mod\, n), \text{ then } ac \equiv bd(mod\, n)$$
- $$\text{If } a \equiv b(mod\ n) \text{ then } a^k \equiv b^k(mod\ n), k \in \mathbb{N} - \{0\}$$

Notice the similarities between equations and congruences:

- They are both equivalence relations.
- You can add/multiply both sides by numbers to get a new one.
- You can add or multiply two together to get a new one.

Since congruence is an equivalence relation, it can have equivalence classes:

Definition 5.5.2 Congruence Classes

Given $a, b \in \mathbb{Z}$ and some integer $n > 0$, we define the congruence class of a as:

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a(mod\ n)\}$$

For example:

- $[0]_2$ represents the set of all even numbers.
- $[1]_2$ represents the set of all even numbers.
- $[2]_2 = [0]_2$, since $2 \in [0]_2$ because $2 \equiv 0(mod\ 2)$.