MATH221: Mathematics for Computer Science

Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

June 15, 2021

Chapter 1:

Logic

Logic

Logic is a language for reasoning. We are interested in whether a statement is true or false and in determining truth/falsehood of statements from other statements.

Definition

*A **statement** is a sentence that is true or false, but not both.*

Logic

Logic is a language for reasoning. We are interested in whether a statement is true or false and in determining truth/falsehood of statements from other statements.

Definition

*A **statement** is a sentence that is true or false, but not both.*

Which are statements?

1. There are 10 people in this classroom.
2. Is it lunchtime?
3. $3 + 4 = 7$
4. $x < 2$
5. There exists x such that $x < 2$.
6. This sentence is false.

Much of mathematics is about proving a statement is true or showing that it is false.

Example.

(a) Show that the statement, "if $x^2 = 9$, then $x = 1$ or $x = -1$" is false.

Much of mathematics is about proving a statement is true or showing that it is false.

Example.

(a) Show that the statement, "if $x^2 = 9$, then $x = 1$ or $x = -1$" is false.

(b) Prove that the statement, "if $x^2 = 9$, then $x = 3$ or $x = -3$" is true.

Logical Connectives

Connectives are key words or symbols that connect two or more simple statements to form new, more complex statements. We use $p, q, r, \ldots$ to denote simple statements (statement variables).

p: I love MATH221.
q: Bob has to work tonight.

Logical Connectives

Connectives are key words or symbols that connect two or more simple statements to form new, more complex statements. We use $p, q, r, \ldots$ to denote simple statements (statement variables).

p: I love MATH221.
q: Bob has to work tonight.

There are 5 connectives.

Negation:	$\sim p$	"Not p."
Conjunction:	$p \wedge q$	"p and q."
Disjunction:	$p \vee q$	"p or q."
Conditional:	$p \rightarrow q$	"p implies q."
Biconditional:	$p \leftrightarrow q$	"p if and only if q."

- An expression of simple statements and connectives is called a *compound statement*.
- Each simple statement has a *truth value*: T for true, F for false.
- The truth value of a compound statement is determined by logic, using the simple statement values and the connectives. We do this by constructing truth tables.

Truth Tables

(1) Negation. If p is a statement variable, then $\sim p$ has the opposite truth value.

If p is true, then $\sim p$ is false.
If p is false, then $\sim p$ is true.

Truth Tables

(1) Negation. If p is a statement variable, then $\sim p$ has the opposite truth value.

If p is true, then $\sim p$ is false.
If p is false, then $\sim p$ is true.

Example.

p: It is raining now. $\sim p$:

Truth Tables

(1) Negation. If p is a statement variable, then $\sim p$ has the opposite truth value.

If p is true, then $\sim p$ is false.
If p is false, then $\sim p$ is true.

Example.

p: It is raining now.	$\sim p$:
q: Video games are not fun.	$\sim q$:

Truth Tables

(1) Negation. If p is a statement variable, then $\sim p$ has the opposite truth value.

If p is true, then $\sim p$ is false.
If p is false, then $\sim p$ is true.

Example.

p: It is raining now.	$\sim p$:
q: Video games are not fun.	$\sim q$:
r: $x > 2$ or $x < 2$	$\sim r$:

Truth Tables

(1) Negation. If p is a statement variable, then $\sim p$ has the opposite truth value.

If p is true, then $\sim p$ is false.
If p is false, then $\sim p$ is true.

Example.

p: It is raining now.	$\sim p$:
q: Video games are not fun.	$\sim q$:
r: $x > 2$ or $x < 2$	$\sim r$:

Can $\sim r$ be simplified?

The truth values for negation are summarised in a table.

p	$\sim p$
T	
F	

The truth values for negation are summarised in a table.

p	$\sim p$
T	
F	

Note. The truth table above tells us that for any statement p, exactly one of p and $\sim p$ is true. This gives us 2 options for proving p is true: either show it directly, or show it indirectly by proving that $\sim p$ is false (proof by contradiction).

The truth values for negation are summarised in a table.

p	$\sim p$
T	
F	

Note. The truth table above tells us that for any statement p, exactly one of p and $\sim p$ is true. This gives us 2 options for proving p is true: either show it directly, or show it indirectly by proving that $\sim p$ is false (proof by contradiction).

Note. To change priority, use parentheses/brackets/braces.

$\sim p \vee q$ means $(\sim p) \vee q$, which is different from $\sim (p \vee q)$.

(2) Conjunction. If p and q are statement variables, the conjunction is $p \wedge q$. If p and q are both true, $p \wedge q$ is true. Otherwise, $p \wedge q$ is false.

(2) Conjunction. If p and q are statement variables, the conjunction is $p \wedge q$. If p and q are both true, $p \wedge q$ is true. Otherwise, $p \wedge q$ is false.

Example.

p: $x < 2$. q: $x > -1$. $p \wedge q$:

(2) Conjunction. If p and q are statement variables, the conjunction is $p \wedge q$. If p and q are both true, $p \wedge q$ is true. Otherwise, $p \wedge q$ is false.

Example.

p: $x < 2$. q: $x > -1$. $p \wedge q$:

p: It's hot. q: It's sunny. $p \wedge q$:

(2) Conjunction. If p and q are statement variables, the conjunction is $p \wedge q$. If p and q are both true, $p \wedge q$ is true. Otherwise, $p \wedge q$ is false.

Example.

p: $x < 2$. q: $x > -1$. $p \wedge q$:

p: It's hot. q: It's sunny. $p \wedge q$:

The truth table for $p \wedge q$ is the following.

p	q	$p \wedge q$
T	T	
T	F	
F	T	
F	F	

Example. Write the truth value.

1. $3 < 5 \wedge 6 > \pi$
2. $3 > 5 \wedge 6 > \pi$
3. $1 = 2 \wedge 4 = 7$

Example. Write the truth value.

1. $3 < 5 \wedge 6 > \pi$
2. $3 > 5 \wedge 6 > \pi$
3. $1 = 2 \wedge 4 = 7$

Example. Write using simple statements and $\wedge$.

1. I like classical and pop music.
2. 7 is an odd prime number.

(3) Disjunction. If p and q are statement variables, the disjunction is $p \vee q$. If p and q are both false, then $p \vee q$ is false. Otherwise, $p \vee q$ is true.

(3) Disjunction. If p and q are statement variables, the disjunction is $p \vee q$. If p and q are both false, then $p \vee q$ is false. Otherwise, $p \vee q$ is true.

Example. Write using simple statements and connectives.

1. I take the bus or train to school.
2. $|x| > 1$.

The truth table for disjunction is the following.

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

The truth table for disjunction is the following.

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Note. The word "or" can also be used in an exclusive sense, i.e. p or q but not both. Consider the difference in meaning:

Coffee or tea? Milk or sugar?

The truth table for disjunction is the following.

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Note. The word "or" can also be used in an exclusive sense, i.e. p or q but not both. Consider the difference in meaning:

Coffee or tea? Milk or sugar?

The exclusive or statement is sometimes denoted by $\oplus$, but it can be represented by and/or/not symbols.

$p \oplus q =$ "p or q, but not both" $=$

The truth table for disjunction is the following.

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Note. The word "or" can also be used in an exclusive sense, i.e. p or q but not both. Consider the difference in meaning:

Coffee or tea? Milk or sugar?

The exclusive or statement is sometimes denoted by $\oplus$, but it can be represented by and/or/not symbols.

$$p \oplus q = \text{“}p \text{ or } q\text{, but not both”} = (p \vee q) \wedge \sim (p \wedge q)$$

The truth table for disjunction is the following.

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Note. The word "or" can also be used in an exclusive sense, i.e. p or q but not both. Consider the difference in meaning:

Coffee or tea? Milk or sugar?

The exclusive or statement is sometimes denoted by $\oplus$, but it can be represented by and/or/not symbols.

$$p \oplus q = \text{“}p \text{ or } q\text{, but not both”} = (p \vee q) \wedge \sim (p \wedge q)$$

Exercise. Make a truth table for $\oplus$.

To make a truth table for compound statements, write the variables, then the basic combinations, then more complex combinations. If there are n variables, there are 2^n rows in the table. Use as many columns as you need.

To make a truth table for compound statements, write the variables, then the basic combinations, then more complex combinations. If there are n variables, there are 2^n rows in the table. Use as many columns as you need.

Example. Make truth tables for the following.

1. $p \vee \sim p$
2. $\sim p \wedge q$
3. $(p \wedge q) \vee \sim r$

(4) Conditional. When you make a logical inference or deduction, you reason from an assumption to a conclusion. The statement has the form, “if something is true, then something else is true”.

(4) Conditional. When you make a logical inference or deduction, you reason from an assumption to a conclusion. The statement has the form, “if something is true, then something else is true”.

If p and q are statement variables, the conditional of q by p is $p \rightarrow q$. If p is true and q is false, then $p \rightarrow q$ is false. Otherwise, $p \rightarrow q$ is true. p is the assumption and q is the conclusion.

(4) Conditional. When you make a logical inference or deduction, you reason from an assumption to a conclusion. The statement has the form, “if something is true, then something else is true”.

If p and q are statement variables, the conditional of q by p is $p \to q$. If p is true and q is false, then $p \to q$ is false. Otherwise, $p \to q$ is true. p is the assumption and q is the conclusion.

Example.

p: I work hard. q: I do well. $p \to q$:

(4) Conditional. When you make a logical inference or deduction, you reason from an assumption to a conclusion. The statement has the form, “if something is true, then something else is true”.

If p and q are statement variables, the conditional of q by p is $p \to q$. If p is true and q is false, then $p \to q$ is false. Otherwise, $p \to q$ is true. p is the assumption and q is the conclusion.

Example.

p: I work hard. q: I do well. $p \to q$:
p: $x = 2$. q: $x^2 = 4$. $p \to q$:

(4) Conditional. When you make a logical inference or deduction, you reason from an assumption to a conclusion. The statement has the form, “if something is true, then something else is true”.

If p and q are statement variables, the conditional of q by p is $p \to q$. If p is true and q is false, then $p \to q$ is false. Otherwise, $p \to q$ is true. p is the assumption and q is the conclusion.

Example.

p: I work hard. q: I do well. $p \to q$:
p: $x = 2$. q: $x^2 = 4$. $p \to q$:

Is $q \to p$ true?

$p \to q$ can be read in many ways

p implies q	q whenever p
if p, then q	p is sufficient for q
q if p	q is necessary for p
q provided p	p only if q

$p \to q$ can be read in many ways

p implies q	q whenever p
if p, then q	p is sufficient for q
q if p	q is necessary for p
q provided p	p only if q

Example. Write using simple statements and connectives, "if $x^2 = 4$, then $x = 2$ or $x = -2$".

$p \to q$ can be read in many ways

p implies q	q whenever p
if p, then q	p is sufficient for q
q if p	q is necessary for p
q provided p	p only if q

Example. Write using simple statements and connectives, "if $x^2 = 4$, then $x = 2$ or $x = -2$".

The truth table for conditional is the following.

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

Note. Why is $p \to q$ true when p is false? Because such statements are accepted as true unless they can be proven false.

Note. Why is $p \to q$ true when p is false? Because such statements are accepted as true unless they can be proven false.

Consider the claim, “if it rains, then I will go home”.

Note. Why is $p \to q$ true when p is false? Because such statements are accepted as true unless they can be proven false.

Consider the claim, “if it rains, then I will go home”.

- If it rains and I go home, then the statement is true.

Note. Why is $p \to q$ true when p is false? Because such statements are accepted as true unless they can be proven false.

Consider the claim, "if it rains, then I will go home".

- If it rains and I go home, then the statement is true.
- If it rains and I don't go home, then the statement is false.

Note. Why is $p \to q$ true when p is false? Because such statements are accepted as true unless they can be proven false.

Consider the claim, "if it rains, then I will go home".

- If it rains and I go home, then the statement is true.
- If it rains and I don't go home, then the statement is false.
- If it doesn't rain, then regardless of whether or not I go home, we cannot prove that the statement is false. Therefore, we accept it as true.

(5) Biconditional. A biconditional statement has the form, "p if and only if q (p iff q)". It is true only if both variables have the same truth value. It is denoted by $p \leftrightarrow q$ and is read

p iff q	p is equivalent to q
p implies and is implied by q	p is necessary and sufficient for q

(5) Biconditional. A biconditional statement has the form, "p if and only if q (p iff q)". It is true only if both variables have the same truth value. It is denoted by $p \leftrightarrow q$ and is read

p iff q	p is equivalent to q
p implies and is implied by q	p is necessary and sufficient for q

Example. p: $x^3 = -8$. q: $x = -2$. $p \leftrightarrow q$:

(5) Biconditional. A biconditional statement has the form, "p if and only if q (p iff q)". It is true only if both variables have the same truth value. It is denoted by $p \leftrightarrow q$ and is read

p iff q	p is equivalent to q
p implies and is implied by q	p is necessary and sufficient for q

Example. p: $x^3 = -8$. q: $x = -2$. $p \leftrightarrow q$:

Example. Write using connectives, "Michael is a bachelor if and only if he is male and never married".

The truth table for biconditional is the following.

p	q	$p \leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

The truth table for biconditional is the following.

p	q	$p \leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

Example. Write the truth value.

1. $x^2 = 1 \Leftrightarrow (x = 1 \vee x = -1)$
2. I get wet if and only if it is raining.

Example. Complete the table.

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$	$(p \to q) \wedge (q \to p)$
T	T				
T	F				
F	T				
F	F				

Example. Complete the table.

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$	$(p \to q) \wedge (q \to p)$
T	T				
T	F				
F	T				
F	F				

Notice that the last two columns are identical. This means that $p \leftrightarrow q$ and $(p \to q) \wedge (q \to p)$ are logically equivalent.

Main Connectives

When building compound statements, use parentheses to avoid ambiguity. The main connective is the one that binds the whole statement together. We must know the ranking of all the connectives in a statement.

Main Connectives

When building compound statements, use parentheses to avoid ambiguity. The main connective is the one that binds the whole statement together. We must know the ranking of all the connectives in a statement.

Example. What is the main connective?

1. $(p \vee \sim q) \rightarrow (p \wedge r)$

Main Connectives

When building compound statements, use parentheses to avoid ambiguity. The main connective is the one that binds the whole statement together. We must know the ranking of all the connectives in a statement.

Example. What is the main connective?

1. $(p \vee \sim q) \rightarrow (p \wedge r)$
2. $p \rightarrow [q \rightarrow (r \vee \sim r)]$

Main Connectives

When building compound statements, use parentheses to avoid ambiguity. The main connective is the one that binds the whole statement together. We must know the ranking of all the connectives in a statement.

Example. What is the main connective?

1. $(p \vee \sim q) \rightarrow (p \wedge r)$
2. $p \rightarrow [q \rightarrow (r \vee \sim r)]$
3. $\sim [(p \wedge q) \vee (\sim p \wedge q)]$

Tautology and Fallacy

- A tautology is a compound statement that is always true, for all values of the basic statements (eg. $p \vee \sim p$).

Tautology and Fallacy

- A tautology is a compound statement that is always true, for all values of the basic statements (eg. $p \vee \sim p$).
- A fallacy is a compound statement that is always false, for all values of the basic statements (eg. $p \wedge \sim p$).

Tautology and Fallacy

- A tautology is a compound statement that is always true, for all values of the basic statements (eg. $p \vee \sim p$).
- A fallacy is a compound statement that is always false, for all values of the basic statements (eg. $p \wedge \sim p$).
- Any statement that is neither a tautology nor a fallacy is called a contingent statement.

Tautology and Fallacy

- A tautology is a compound statement that is always true, for all values of the basic statements (eg. $p \vee \sim p$).
- A fallacy is a compound statement that is always false, for all values of the basic statements (eg. $p \wedge \sim p$).
- Any statement that is neither a tautology nor a fallacy is called a contingent statement.
- The negation of a tautology is a fallacy and vice versa.

Example. Show that for any statement p, $p \vee \sim p$ is a tautology and $p \wedge \sim p$ is a fallacy.

Example. Show that for any statement p, $p \vee \sim p$ is a tautology and $p \wedge \sim p$ is a fallacy.

Example. Determine whether $\sim [(\sim p \wedge q) \wedge p]$ is a tautology, fallacy or contingent statement.

Example. Show that for any statement p, $p \vee \sim p$ is a tautology and $p \wedge \sim p$ is a fallacy.

Example. Determine whether $\sim [(\sim p \wedge q) \wedge p]$ is a tautology, fallacy or contingent statement.

Identifying Tautologies/Fallacies

A tautology has all T values in a truth table and a fallacy has all F values, but since 2^n rows are required for a table with n variables, this method gets impractical very quickly (4 variables means 16 rows, 5 variables means 32 rows, etc.). We will see a quicker method now.

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

Example. Is $(p \wedge q) \rightarrow (r \wedge s)$ a tautology?

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

Example. Is $(p \wedge q) \rightarrow (r \wedge s)$ a tautology?

$$(p \wedge q) \underset{F}{\rightarrow} (r \wedge s)$$

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

Example. Is $(p \wedge q) \rightarrow (r \wedge s)$ a tautology?

$$(p \wedge q) \underset{F}{\rightarrow} (r \wedge s)$$

$$(p \underset{T}{\wedge} q) \rightarrow (r \underset{F}{\wedge} s)$$

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

Example. Is $(p \wedge q) \rightarrow (r \wedge s)$ a tautology?

$$(p \wedge q) \underset{F}{\rightarrow} (r \wedge s)$$

$$(p \underset{T}{\wedge} q) \rightarrow (r \underset{F}{\wedge} s)$$

$$(\underset{T}{p} \wedge \underset{T}{q}) \rightarrow (\underset{T}{r} \wedge \underset{F}{s})$$

The method relies on the fact that if F can occur under the main connective, then the statement is not a tautology. If F is not possible, it is a tautology (similar for fallacy). So we assume the main connective yields F, then work backwards to see if a valid combination of values exists.

Example. Is $(p \wedge q) \rightarrow (r \wedge s)$ a tautology?

$$(p \wedge q) \underset{F}{\rightarrow} (r \wedge s)$$
$$(p \underset{T}{\wedge} q) \rightarrow (r \underset{F}{\wedge} s)$$
$$(\underset{T}{p} \wedge \underset{T}{q}) \rightarrow (\underset{T}{r} \wedge \underset{F}{s})$$

So for instance, with the choices $p = q = r =$T and $s =$F, the statement is false. Therefore, it is not a tautology.

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

$[(p \to q) \wedge (q \to r)] \underset{F}{\to} (p \to r)$

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

$$[(p \to q) \wedge (q \to r)] \underset{F}{\to} (p \to r)$$

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

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

$$[(p \to q) \wedge (q \to r)] \underset{F}{\to} (p \to r)$$

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

$$[(p \underset{T}{\to} q) \wedge (q \underset{T}{\to} r)] \to (p \underset{T}{\to} r)$$

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

$$[(p \to q) \wedge (q \to r)] \underset{F}{\to} (p \to r)$$

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

$$[(p \underset{T}{\to} q) \wedge (q \underset{T}{\to} r)] \to (p \underset{T}{\to} r)$$

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

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

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

We assumed the statement is false and arrived at a contradiction. Therefore, the statement is always true.

Example. Is $[(p \to q) \wedge (q \to r)] \to (p \to r)$ a tautology?

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

We assumed the statement is false and arrived at a contradiction. Therefore, the statement is always true.

Exercise. Make the truth table for the above statement and verify that the last column is all T.

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$

$\sim [(p \to q) \underset{F}{\to} (\sim p \vee q)]$

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$$
$$\sim [(p \to q) \underset{F}{\to} (\sim p \vee q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\sim p \underset{F}{\vee} q)]$$

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$$
$$\sim [(p \to q) \underset{F}{\to} (\sim p \vee q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\sim p \underset{F}{\vee} q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\underset{F}{\sim} p \vee \underset{F}{q})]$$

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$$
$$\sim [(p \to q) \underset{F}{\to} (\sim p \vee q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\sim p \underset{F}{\vee} q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\underset{F}{\sim} p \vee q \underset{F}{)}]$$
$$\sim [(\underset{F}{p} \to \underset{F}{q}) \to (\sim \underset{T}{p} \vee \underset{F}{q})]$$

Example. Is $\sim [(p \to q) \to (\sim p \vee q)]$ a fallacy?

$$\underset{T}{\sim} [(p \to q) \to (\sim p \vee q)]$$
$$\sim [(p \to q) \underset{F}{\to} (\sim p \vee q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\sim p \underset{F}{\vee} q)]$$
$$\sim [(p \underset{T}{\to} q) \to (\underset{F}{\sim} p \vee \underset{F}{q})]$$
$$\sim [(\underset{F}{p} \to \underset{F}{q}) \to (\sim \underset{T}{p} \vee \underset{F}{q})]$$

Contradiction, so the statement can never be true. It is a fallacy.

Logical Equivalence

- Two statements are called logically equivalent iff they have identical truth table values.
- The logical equivalence of p and q is denoted by $p \equiv q$.
- p and q are logically equivalent iff $p \leftrightarrow q$ is a tautology.

Logical Equivalence

- Two statements are called logically equivalent iff they have identical truth table values.
- The logical equivalence of p and q is denoted by $p \equiv q$.
- p and q are logically equivalent iff $p \leftrightarrow q$ is a tautology.

Example. Is $p \equiv \sim (\sim p)$?

Logical Equivalence

- Two statements are called logically equivalent iff they have identical truth table values.
- The logical equivalence of p and q is denoted by $p \equiv q$.
- p and q are logically equivalent iff $p \leftrightarrow q$ is a tautology.

Example. Is $p \equiv \sim (\sim p)$?

p	$\sim p$	$\sim (\sim p)$
T	F	T
F	T	F

↑ ↑

Identical, so yes $p \equiv \sim (\sim p)$.

Substitution of Equivalence

We can make substitutions in statements, using equivalent expressions. There are 2 rules.

Substitution of Equivalence

We can make substitutions in statements, using equivalent expressions. There are 2 rules.

1. Rule of Substitution. If in a tautology all occurrences of a variable are replaced by the same statement, the result is another tautology.

Substitution of Equivalence

We can make substitutions in statements, using equivalent expressions. There are 2 rules.

1. Rule of Substitution. If in a tautology all occurrences of a variable are replaced by the same statement, the result is another tautology.

   Example. $p \vee \sim p$ is a tautology, so $q \vee \sim q$ is too, as is $[(p \vee q) \rightarrow r] \vee \sim [(p \vee q) \rightarrow r]$.

Substitution of Equivalence

We can make substitutions in statements, using equivalent expressions. There are 2 rules.

1. Rule of Substitution. If in a tautology all occurrences of a variable are replaced by the same statement, the result is another tautology.

   Example. $p \vee \sim p$ is a tautology, so $q \vee \sim q$ is too, as is $[(p \vee q) \rightarrow r] \vee \sim [(p \vee q) \rightarrow r]$.

2. Rule of Substitution of Equivalence. If in a tautology we replace any part of a statement by a statement equivalent to that part, the result is another tautology.

Substitution of Equivalence

We can make substitutions in statements, using equivalent expressions. There are 2 rules.

1. Rule of Substitution. If in a tautology all occurrences of a variable are replaced by the same statement, the result is another tautology.

   Example. $p \vee \sim p$ is a tautology, so $q \vee \sim q$ is too, as is $[(p \vee q) \rightarrow r] \vee \sim [(p \vee q) \rightarrow r]$.

2. Rule of Substitution of Equivalence. If in a tautology we replace any part of a statement by a statement equivalent to that part, the result is another tautology.

   Example. $p \equiv \sim\sim p$, so the tautology $p \vee \sim p$ can be written $\sim\sim p \vee \sim p$ and is still a tautology.

This kind of substitution often happens in algebra. For instance, it is well-known that $\cos^2 x + \sin^2 x = 1$, so the expression $\frac{1-\sin^2 x}{\cos x}$ can be simplified:

This kind of substitution often happens in algebra. For instance, it is well-known that $\cos^2 x + \sin^2 x = 1$, so the expression $\frac{1-\sin^2 x}{\cos x}$ can be simplified:

$$\frac{1-\sin^2 x}{\cos x} = \frac{\cos^2 x}{\cos x} = \cos x, \ \cos x \neq 0.$$

This kind of substitution often happens in algebra. For instance, it is well-known that $\cos^2 x + \sin^2 x = 1$, so the expression $\frac{1-\sin^2 x}{\cos x}$ can be simplified:

$$\frac{1-\sin^2 x}{\cos x} = \frac{\cos^2 x}{\cos x} = \cos x, \ \cos x \neq 0.$$

Example. $p \to q$ is logically equivalent to $\sim p \vee q$. $q \to (p \to q)$ is a tautology. Prove that $s \to (\sim r \vee s)$ is a tautology.

This kind of substitution often happens in algebra. For instance, it is well-known that $\cos^2 x + \sin^2 x = 1$, so the expression $\frac{1-\sin^2 x}{\cos x}$ can be simplified:

$$\frac{1-\sin^2 x}{\cos x} = \frac{\cos^2 x}{\cos x} = \cos x, \ \cos x \neq 0.$$

Example. $p \to q$ is logically equivalent to $\sim p \vee q$. $q \to (p \to q)$ is a tautology. Prove that $s \to (\sim r \vee s)$ is a tautology.

Proof.

$q \to (p \to q)$	(given)
$q \to (r \to q)$	(substitute r for p)
$s \to (r \to s)$	(substitute s for q)
$s \to (\sim r \vee s)$	(equivalence substitute $\sim r \vee s$ for $r \to s$)

Logical Equivalence Laws

1. Commutative Laws
   (a) $p \vee q \equiv q \vee p$
   (b) $p \wedge q \equiv q \wedge p$
   (c) $p \leftrightarrow q \equiv q \leftrightarrow p$
2. Associative Laws
   (a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$
   (b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
   (c) $(p \leftrightarrow q) \leftrightarrow r \equiv p \leftrightarrow (q \leftrightarrow r)$
3. Distributive Laws
   (a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
   (b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
   (c) $p \rightarrow (q \vee r) \equiv (p \rightarrow q) \vee (p \rightarrow r)$
   (d) $p \rightarrow (q \wedge r) \equiv (p \rightarrow q) \wedge (p \rightarrow r)$

4. Double Negation Law

   $\sim\sim p \equiv p$

5. De Morgan's Laws
   (a) $\sim (p \vee q) \equiv \sim p \wedge \sim q$
   (b) $\sim (p \wedge q) \equiv \sim p \vee \sim q$

6. Implication Laws
   (a) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
   (b) $p \rightarrow q \equiv \sim p \vee q$
   (c) $p \rightarrow q \equiv \sim q \rightarrow \sim p$
   (d) $\sim (p \rightarrow q) \equiv p \wedge \sim q$

Example. To understand De Morgan's laws, write negations of the following.

1. John is 180cm tall and he weighs at least 90kg.
2. Either the bus was late or Jane's watch was slow.

Example. To understand De Morgan's laws, write negations of the following.

1. John is 180cm tall and he weighs at least 90kg.
2. Either the bus was late or Jane's watch was slow.

Example. Prove De Morgan's laws using truth tables.

Example. To understand De Morgan's laws, write negations of the following.

1. John is 180cm tall and he weighs at least 90kg.
2. Either the bus was late or Jane's watch was slow.

Example. Prove De Morgan's laws using truth tables.

Example. Is $(p \wedge \sim q) \wedge (\sim p \vee q)$ a tautology or a fallacy?

Example. To understand De Morgan's laws, write negations of the following.

1. John is 180cm tall and he weighs at least 90kg.
2. Either the bus was late or Jane's watch was slow.

Example. Prove De Morgan's laws using truth tables.

Example. Is $(p \wedge \sim q) \wedge (\sim p \vee q)$ a tautology or a fallacy?

Example. Is $(p \leftrightarrow q) \leftrightarrow (\sim p \leftrightarrow q)$ a tautology or a fallacy?

Example. To understand De Morgan's laws, write negations of the following.

1. John is 180cm tall and he weighs at least 90kg.
2. Either the bus was late or Jane's watch was slow.

Example. Prove De Morgan's laws using truth tables.

Example. Is $(p \wedge \sim q) \wedge (\sim p \vee q)$ a tautology or a fallacy?

Example. Is $(p \leftrightarrow q) \leftrightarrow (\sim p \leftrightarrow q)$ a tautology or a fallacy?

Example. Prove $(p \rightarrow q) \rightarrow r \equiv [(\sim p \rightarrow r) \wedge (q \rightarrow r)]$.

Proof.

Let $\bigstar$ be the tautology $s \to t \equiv \sim s \vee t$.

$(p \to q) \to r \quad \equiv (\sim p \vee q) \to r \qquad \bigstar$

Proof.

Let $\star$ be the tautology $s \to t \equiv \sim s \vee t$.

$$\begin{aligned} (p \to q) \to r &\equiv (\sim p \vee q) \to r && \star \\ &\equiv \sim (\sim p \vee q) \vee r && \star \end{aligned}$$

Proof.

Let $\star$ be the tautology $s \to t \equiv \sim s \vee t$.

$$
\begin{aligned}
(p \to q) \to r &\equiv (\sim p \vee q) \to r && \star \\
&\equiv \sim (\sim p \vee q) \vee r && \star \\
&\equiv (\sim\sim p \wedge \sim q) \vee r && \text{De Morgan}
\end{aligned}
$$

Proof.

Let $\star$ be the tautology $s \to t \equiv \sim s \vee t$.

$$
\begin{aligned}
(p \to q) \to r &\equiv (\sim p \vee q) \to r && \star \\
&\equiv \sim (\sim p \vee q) \vee r && \star \\
&\equiv (\sim\sim p \wedge \sim q) \vee r && \text{De Morgan} \\
&\equiv (p \wedge \sim q) \vee r && \text{double negative}
\end{aligned}
$$

Proof.

Let $\bigstar$ be the tautology $s \to t \equiv \sim s \vee t$.

$$
\begin{aligned}
(p \to q) \to r &\equiv (\sim p \vee q) \to r && \bigstar \\
&\equiv \sim (\sim p \vee q) \vee r && \bigstar \\
&\equiv (\sim\sim p \wedge \sim q) \vee r && \text{De Morgan} \\
&\equiv (p \wedge \sim q) \vee r && \text{double negative} \\
&\equiv (p \vee r) \wedge (\sim q \vee r) && \text{distributive}
\end{aligned}
$$

Proof.

Let $\bigstar$ be the tautology $s \to t \equiv \sim s \vee t$.

$$
\begin{array}{lll}
(p \to q) \to r & \equiv (\sim p \vee q) \to r & \bigstar \\
& \equiv \sim (\sim p \vee q) \vee r & \bigstar \\
& \equiv (\sim\sim p \wedge \sim q) \vee r & \text{De Morgan} \\
& \equiv (p \wedge \sim q) \vee r & \text{double negative} \\
& \equiv (p \vee r) \wedge (\sim q \vee r) & \text{distributive} \\
& \equiv (\sim\sim p \vee r) \wedge (\sim q \vee r) & \text{double negative}
\end{array}
$$

Proof.

Let $\star$ be the tautology $s \to t \equiv \sim s \vee t$.

$$
\begin{array}{lll}
(p \to q) \to r & \equiv (\sim p \vee q) \to r & \star \\
& \equiv \sim (\sim p \vee q) \vee r & \star \\
& \equiv (\sim\sim p \wedge \sim q) \vee r & \text{De Morgan} \\
& \equiv (p \wedge \sim q) \vee r & \text{double negative} \\
& \equiv (p \vee r) \wedge (\sim q \vee r) & \text{distributive} \\
& \equiv (\sim\sim p \vee r) \wedge (\sim q \vee r) & \text{double negative} \\
& \equiv (\sim p \to r) \wedge (q \to r) & \star \text{ twice}
\end{array}
$$

Predicate Logic

The connectives $\sim, \wedge, \vee, \rightarrow, \leftrightarrow$ are not enough to prove or disprove all types of logical statements. For instance, the argument

All UOW maths subjects are fun.

MATH221 is a UOW maths subject.

Therefore, MATH221 is fun.

is correct, but we cannot determine its validity with the tools we have so far. We need to be able to manage words such as “all” and “some”.

- A *predicate* is a sentence that contains a finite number of variables and becomes a statement when values are substituted.
- The *domain* of a variable is the set of all possible values it can be. The *truth set* is the subset of the domain that makes the predicate true.
- Predicates of one variable x are denoted by $p(x), q(x)$, etc.

Notation

- $\mathbb{R}$: the set of all real numbers
- $\mathbb{Q}$: the set of rational numbers (fractions)
- $\mathbb{Z}$: the set of integers (whole numbers)
- $\mathbb{N}$: the set of natural numbers
- $\in$: “is in”, “belongs to”, “is a member of”
- $\forall$: universal quantifier “for all”
- $\exists$: existential quantifier “there exists”

Example. The predicate $p(x)$: "x is an integer strictly less than 5" with $\operatorname{dom} p = \mathbb{Z}$ has truth set $\{\ldots, -2, -1, 0, 1, 2, 3, 4\}$.

Example. The predicate $p(x)$: "x is an integer strictly less than 5" with $\operatorname{dom} p = \mathbb{Z}$ has truth set $\{\ldots, -2, -1, 0, 1, 2, 3, 4\}$.

Example. The predicate $q(x)$: "$x^2 > x$" with $\operatorname{dom} q = \mathbb{R}$ has truth set

$$\{x : x^2 > x\} = \{x : x < 0 \vee x > 1\} = (-\infty, 0) \cup (1, \infty)$$

The Universal Quantifier $\forall$

One way to change a predicate into a statement is to assign values to the variables. Another way is to add quantifiers.

The Universal Quantifier $\forall$

One way to change a predicate into a statement is to assign values to the variables. Another way is to add quantifiers.

Example. "All humans are mortal."
"Every real number has a nonnegative square." $\forall\, x \in \mathbb{R}, x^2 \geq 0$

The Universal Quantifier $\forall$

One way to change a predicate into a statement is to assign values to the variables. Another way is to add quantifiers.

Example. "All humans are mortal."
"Every real number has a nonnegative square." $\forall\, x \in \mathbb{R}, x^2 \geq 0$

A *universal statement* has the form

$$\forall\, x \in D, p(x).$$

It is true iff $p(x)$ is true for every $x \in D$. If at least one $x \in D$ can be found that makes $p(x)$ false, the statement is false. Such an x is called a *counterexample*.

Example. $\forall\, x \in \mathbb{R}, x^2 > x$.

Example. $\forall\, x \in \mathbb{R}, x^2 > x$. FALSE, counterexample: $x = \frac{1}{2}$.

Example. $\forall\, x \in \mathbb{R}, x^2 > x$. FALSE, counterexample: $x = \frac{1}{2}$.

Example. Write using $\forall$.

1. All dogs are animals.
2. Every integer greater than zero has a prime factor. (True?)

Example. $\forall\, x \in \mathbb{R}, x^2 > x$. FALSE, counterexample: $x = \frac{1}{2}$.

Example. Write using $\forall$.

1. All dogs are animals.
2. Every integer greater than zero has a prime factor. (True?)

Example. Let $D = \{1, 2, 3, 4, 5\}$. Show that the statement "$\forall\, x \in D, x^2 \geq x$" is true. Show that the statement "$\forall\, x \in D, \frac{1}{x^2} < \frac{1}{x}$" is false.

The Existential Quantifier $\exists$

Example. "There is a cat in my house."
"There exist integers m, n such that $m + n = mn$."
$\exists\, m, n \in \mathbb{Z}$ s.t. $m + n = mn$

The Existential Quantifier $\exists$

Example. "There is a cat in my house."
"There exist integers m, n such that $m + n = mn$."
$\exists\, m, n \in \mathbb{Z}$ s.t. $m + n = mn$

An *existential statement* has the form

$$\exists\, x \in D \text{ s.t. } p(x).$$

It is true iff $p(x)$ is true for at least one $x \in D$. It is false iff $p(x)$ is false for all $x \in D$.

Example. Write using $\exists$.

1. There exists a real number whose square is negative.
2. Someone in this room is vegetarian.

Example. Write using $\exists$.

1. There exists a real number whose square is negative.
2. Someone in this room is vegetarian.

Example. Show that the statement "$\exists\ m \in \mathbb{Z}$ s.t. $m^2 = m$" is true.

Example. Write using $\exists$.

1. There exists a real number whose square is negative.
2. Someone in this room is vegetarian.

Example. Show that the statement "$\exists\ m \in \mathbb{Z}$ s.t. $m^2 = m$" is true.

Example. Let $E = \{5, 6, \ldots, 10\}$. Show that the statement "$\exists\ m \in E$ s.t. $m^2 = m$" is false.

Example. Write using $\exists$.

1. There exists a real number whose square is negative.
2. Someone in this room is vegetarian.

Example. Show that the statement "$\exists\ m \in \mathbb{Z}$ s.t. $m^2 = m$" is true.

Example. Let $E = \{5, 6, \ldots, 10\}$. Show that the statement "$\exists\ m \in E$ s.t. $m^2 = m$" is false.

Example. Rewrite using informal language.

1. $\forall\ x \in \mathbb{R}, x^2 > 0$
2. $\exists\ m \in \mathbb{Z}$ s.t. $m^2 = m$
3. $\forall$ students $s \in S$, $\exists$ maths subject y s.t. s likes y
4. $\forall\ x \in \mathbb{R}, x^2 \neq -1$

Negation of Universal Statements

Consider the statement, “all mathematicians wear glasses”. What is the negation of the statement?

Negation of Universal Statements

Consider the statement, “all mathematicians wear glasses”. What is the negation of the statement?

It is natural to think, “no mathematician wears glasses”, but that is not correct. The negation is, “there exists a mathematician who doesn’t wear glasses”. If just one counterexample can be found, the universal statement is false.

Theorem (Negation of a universal statement)

The negation of the statement

$$\forall\, x \in D, p(x)$$

is logically equivalent to the statement

$$\exists\, x \in D \text{ s.t. } \sim p(x).$$

Theorem (Negation of a universal statement)

The negation of the statement

$$\forall\, x \in D, p(x)$$

is logically equivalent to the statement

$$\exists\, x \in D \text{ s.t. } \sim p(x).$$

Example. Write negations.

1. No computer hacker is over 40 years old.
2. All prime numbers are odd.
3. Every blonde person has blue eyes.
4. $\forall x \in \mathbb{R}, \frac{1}{x} > 1$.

Negation of Existential Statements

Consider the statement, “some fish breathe air”. What is the negation of the statement?

Negation of Existential Statements

Consider the statement, “some fish breathe air”. What is the negation of the statement?

It is, “no fish breathes air”. One might think it is, “some fish do not breathe air”, but this and the original statement can both be true at the same time.

Negation of Existential Statements

Consider the statement, “some fish breathe air”. What is the negation of the statement?

It is, “no fish breathes air”. One might think it is, “some fish do not breathe air”, but this and the original statement can both be true at the same time.

Theorem

The negation of the statement

$$\exists\, x \in D \text{ s.t. } p(x)$$

is logically equivalent to the statement

$$\forall\, x \in D, \sim p(x).$$

Example. Write negations.

1. There is a triangle whose sum of angles is 200°.
2. There is a 120-year-old woman in Australia.
3. $\exists\, x \in \mathbb{R} \text{ s.t. } x^2 = -1$.

Example. Write negations.

1. There is a triangle whose sum of angles is 200°.
2. There is a 120-year-old woman in Australia.
3. $\exists\, x \in \mathbb{R} \text{ s.t. } x^2 = -1$.

In summary, the negation of a $\forall$ statement is an $\exists$ statement and vice versa.

Example. Write negations and decide which statements are true.

1. $\exists\, x \in \mathbb{R} \text{ s.t. } 3x = 1$.
2. $\forall\, \varepsilon > 0, \forall\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Q} \text{ s.t. } |x - y| < \varepsilon$.

Methods of Proof

Consider the following sequence of statements.

If x is a pig, then x is pink.
Peppa is a pig.
Therefore, Peppa is pink.

Methods of Proof

Consider the following sequence of statements.

If x is a pig, then x is pink.
Peppa is a pig.
Therefore, Peppa is pink.

An *argument* is a sequence of statements, all but the final of which are called *assumptions* and the final of which is called hte *conclusion*. The word 'therefore' is normally placed at the front of the conclusion.

Methods of Proof

Consider the following sequence of statements.

If x is a pig, then x is pink.
Peppa is a pig.
Therefore, Peppa is pink.

An *argument* is a sequence of statements, all but the final of which are called *assumptions* and the final of which is called hte *conclusion*. The word 'therefore' is normally placed at the front of the conclusion.

The logical form of the above argument is

If p, then q.
p.
Therefore, q.

An argument is valid if the conclusion is true whenever all the assumptions are true, no matter what particular statements are substituted for the variables.

An argument is valid if the conclusion is true whenever all the assumptions are true, no matter what particular statements are substituted for the variables.

Definition

*A **proof** is a valid argument used to establish a result.*

An argument is valid if the conclusion is true whenever all the assumptions are true, no matter what particular statements are substituted for the variables.

Definition

*A **proof** is a valid argument used to establish a result.*

Note. The assumptions in an argument or a proof can be axioms, previously proved theorems, or may follow from previous statements by a mathematical or logical rule.

Example. Prove that if $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even, then $x^n \geq 0$.

Example. Prove that if $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even, then $x^n \geq 0$.

Proof.

$n \in \mathbb{N}$ is even	(given)
$n = 2m$ for some $m \in \mathbb{N}$	(definition of even number)
$x^n = x^{2m}$	(substitution)
$= (x^m)^2$	(rule of exponents)
≥ 0	($y^2 \geq 0 \; \forall \; y \in \mathbb{R}$) $\square$

Example. Prove that if $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even, then $x^n \geq 0$.

Proof.

$n \in \mathbb{N}$ is even	(given)
$n = 2m$ for some $m \in \mathbb{N}$	(definition of even number)
$x^n = x^{2m}$	(substitution)
$= (x^m)^2$	(rule of exponents)
≥ 0	($y^2 \geq 0 \; \forall \; y \in \mathbb{R}$) $\square$

Note. A proof should be *complete* (contain all necessary statements) and *concise* (not contain extra or unneeded statements).

Testing Validity

To test an argument for validity, follow these steps.

1. Identify the assumptions and conclusion.
2. Construct a truth table of all statements.
3. If the conclusion is true in every case where all the assumptions are true, then the argument is valid. If there is at least one row of all true assumptions and false conclusion, the argument is invalid.

Example. Is the argument valid?

$$\begin{aligned} p &\to (q \vee \sim r), \\ q &\to (p \wedge r), \\ \therefore\ p &\to r. \end{aligned}$$

Example. Is the argument valid?

$$p \to (q \vee \sim r),$$
$$q \to (p \wedge r),$$
$$\therefore p \to r.$$

p	q	r	$p \to q \vee \sim r$	$q \to p \wedge r$	$p \to r$
T	T	T			
T	T	F			
T	F	T			
T	F	F			
F	T	T			
F	T	F			
F	F	T			
F	F	F			

Exercise. Test the validity of the following arguments.

(a)

$$p \vee (q \vee r),$$
$$\sim r,$$
$$\therefore p \vee q.$$

(b)

$$p \rightarrow q,$$
$$p,$$
$$\therefore q.$$

Exercise. Test the validity of the following arguments.

(a)
$$p \vee (q \vee r),$$
$$\sim r,$$
$$\therefore p \vee q.$$

(b)
$$p \to q,$$
$$p,$$
$$\therefore q.$$

The simple argument (b) is true and it has a special name: *modus ponens*.

Definition

*An argument consisting of 2 assumptions and a conclusion is called a **syllogism**. The most famous syllogism is the modus ponens, Latin for 'method of affirming'.*

If p, then q,
p,
Therefore, q.

Definition

*An argument consisting of 2 assumptions and a conclusion is called a **syllogism**. The most famous syllogism is the modus ponens, Latin for 'method of affirming'.*

If p, then q,
p,
Therefore, q.

Example. Is the statement "$n \in \mathbb{N}$ is even $\Rightarrow$ n^2 is even" true? Prove it.

Definition (Mathematical Induction)

If $p(n)$ is a statement with $\operatorname{dom} p = \mathbb{N}$ *such that*

1. $p(1)$ *is true and*
2. $p(k)$ *true* $\Rightarrow p(k+1)$ *true,*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Definition (Mathematical Induction)

If $p(n)$ is a statement with $\operatorname{dom} p = \mathbb{N}$ such that

1. *$p(1)$ is true and*
2. *$p(k)$ true $\Rightarrow$ $p(k+1)$ true,*

then $p(n)$ is true for all $n \in \mathbb{N}$.

Example. Prove that $4^n - 1$ is a multiple of 3 $\forall\ n \in \mathbb{N}$.

Proof.

$p(n) : \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m + 1$

Proof.

$p(n) : \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m + 1$

(a) $p(1)$: $4^1 = 4 = 3 + 1$

Proof.

$p(n) : \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m + 1$

(a) $p(1)$: $4^1 = 4 = 3 + 1$

(b) Assume $p(k)$, prove $p(k + 1)$.

Proof.

$p(n) : \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m+1$

(a) $p(1)$: $4^1 = 4 = 3+1$

(b) Assume $p(k)$, prove $p(k+1)$.
Let $4^k = 3m+1, m \in \mathbb{Z}$ (this is $p(k)$).

Proof.

$p(n): \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m+1$

(a) $p(1)$: $4^1 = 4 = 3+1$

(b) Assume $p(k)$, prove $p(k+1)$.
Let $4^k = 3m+1, m \in \mathbb{Z}$ (this is $p(k)$).

$p(k+1)$: $\frac{4^{k+1}-1}{3} = \frac{4 \cdot 4^k - 1}{3} = \frac{4(3m+1)-1}{3} = \frac{12m+4-1}{3} = 4m+1 \in \mathbb{Z}$

Proof.

$p(n): \frac{4^n-1}{3} = m \in \mathbb{Z} \Rightarrow 4^n = 3m+1$

(a) $p(1)$: $4^1 = 4 = 3+1$

(b) Assume $p(k)$, prove $p(k+1)$.
Let $4^k = 3m+1, m \in \mathbb{Z}$ (this is $p(k)$).

$p(k+1)$: $\frac{4^{k+1}-1}{3} = \frac{4 \cdot 4^k - 1}{3} = \frac{4(3m+1)-1}{3} = \frac{12m+4-1}{3} = 4m+1 \in \mathbb{Z}$

Therefore, $4^n - 1$ is a multiple of 3 for all $n \in \mathbb{N}$. □

The Law of Syllogism

Is the following a tautology?

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

The Law of Syllogism

Is the following a tautology?

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

That is the law of syllogism: if p implies q and q implies r, then p implies r.

The Law of Syllogism

Is the following a tautology?

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

That is the law of syllogism: if p implies q and q implies r, then p implies r.

Example. Suppose these 2 statements are true.

1. If it rains today, then I'll drive to school.
2. If I drive to school today, then I'll go over my petrol budget.

The Law of Syllogism

Is the following a tautology?

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

That is the law of syllogism: if p implies q and q implies r, then p implies r.

Example. Suppose these 2 statements are true.

1. If it rains today, then I'll drive to school.
2. If I drive to school today, then I'll go over my petrol budget.

Then by the law of syllogism, we can infer another truth.

3. If it rains today, then I'll go over my petrol budget.

The Law of Syllogism

Is the following a tautology?

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

That is the law of syllogism: if p implies q and q implies r, then p implies r.

Example. Suppose these 2 statements are true.

1. If it rains today, then I'll drive to school.
2. If I drive to school today, then I'll go over my petrol budget.

Then by the law of syllogism, we can infer another truth.

3. If it rains today, then I'll go over my petrol budget.

Exercise. Prove the law of syllogism is a tautology.

Proving $\exists$ Statements

How do we prove a statement of the form $\exists\ x \in D$ `s.t.` $p(x)$?

Proving $\exists$ Statements

How do we prove a statement of the form $\exists\ x \in D$ `s.t.` $p(x)$?
We need to find at least one $x \in D$ that makes $p(x)$ true.

Proving $\exists$ Statements

How do we prove a statement of the form $\exists\ x \in D$ s.t. $p(x)$?
We need to find at least one $x \in D$ that makes $p(x)$ true.

Example. Prove that there is an even number that can be written two different ways as the sum of 2 prime numbers.

Proving $\exists$ Statements

How do we prove a statement of the form $\exists\ x \in D$ s.t. $p(x)$?
We need to find at least one $x \in D$ that makes $p(x)$ true.

Example. Prove that there is an even number that can be written two different ways as the sum of 2 prime numbers.

Proof.

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 3 + 5$$
$$10 = 3 + 7 = 5 + 5$$

Example. Prove that there exist $m, n \in \mathbb{N}$ whose sum of reciprocals is an integer.

Example. Prove that there exist $m, n \in \mathbb{N}$ whose sum of reciprocals is an integer.

Proving $\forall$ statements

How do we prove a statement of the form $\forall\, x \in D, p(x)$?

Example. Prove that there exist $m, n \in \mathbb{N}$ whose sum of reciprocals is an integer.

Proving $\forall$ statements

How do we prove a statement of the form $\forall\, x \in D, p(x)$? There are two options, the *method of exhaustion* and the *generalised proof*.

Example. Prove that there exist $m, n \in \mathbb{N}$ whose sum of reciprocals is an integer.

Proving $\forall$ statements

How do we prove a statement of the form $\forall\, x \in D, p(x)$? There are two options, the *method of exhaustion* and the *generalised proof*.

The method of exhaustion checks that $p(x)$ is true for every $x \in D$. This is fine when D is small, but becomes too much work for D large. If D is infinite, this method is of no use.

Example. Prove that every even number between 4 and 18 can be written as the sum of 2 primes.

Example. Prove that every even number between 4 and 18 can be written as the sum of 2 primes.

Proof.

$4 = 2 + 2$ $\quad 6 = 3 + 3$ $\quad 8 = 3 + 5$ $\quad 10 = 5 + 5$

$12 = 5 + 7$ $\quad 14 = 7 + 7$ $\quad 16 = 5 + 11$ $\quad 18 = 5 + 13$ $\square$

Exercise. Prove that every even number can be written as the sum of 2 primes.

The generalised proof is constructed so that it applies to every possibility. It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

The generalised proof is constructed so that it applies to every possibility. It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

Example. Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is even.

The generalised proof is constructed so that it applies to every possibility. It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

Example. Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is even.

Proof.

Let $a, b \in \mathbb{Z}$. $10a + 8b = 2(5a + 4b)$, and since $a, b \in \mathbb{Z}$, we have $5a + 4b \in \mathbb{Z}$.

The generalised proof is constructed so that it applies to every possibility. It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

Example. Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is even.

Proof.

Let $a, b \in \mathbb{Z}$. $10a + 8b = 2(5a + 4b)$, and since $a, b \in \mathbb{Z}$, we have $5a + 4b \in \mathbb{Z}$.
$\Rightarrow 2(5a + 4b)$ is even.

$\therefore 10a + 8b$ is even. $\square$

The generalised proof is constructed so that it applies to every possibility. It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

Example. Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is even.

Proof.

Let $a, b \in \mathbb{Z}$. $10a + 8b = 2(5a + 4b)$, and since $a, b \in \mathbb{Z}$, we have $5a + 4b \in \mathbb{Z}$.
$\Rightarrow 2(5a + 4b)$ is even.

$\therefore 10a + 8b$ is even. □

Note. It doesn't matter which two integers are chosen for a and b; the proof is valid for all such choices.

Disproving $\exists$ Statements

To disprove a statement means to prove its negation. Recall the negation of an existential statement.

$$\sim (\exists\, x \in D \text{ s.t. } p(x)) \equiv \forall\, x \in D, \sim p(x)$$

Disproving $\exists$ Statements

To disprove a statement means to prove its negation. Recall the negation of an existential statement.

$$\sim (\exists\, x \in D \text{ s.t. } p(x)) \equiv \forall\, x \in D, \sim p(x)$$

So to disprove an $\exists$ statement, we must prove a $\forall$ statement, via method of exhaustion or generalised proof.

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Proof.

The negation is, “every prime number greater than 2 is odd”.

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Proof.

The negation is, “every prime number greater than 2 is odd”.
Let $x > 2$ be prime. Suppose x is even. Then $x = 2n, n \in \mathbb{N}$.

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Proof.

The negation is, “every prime number greater than 2 is odd”. Let $x > 2$ be prime. Suppose x is even. Then $x = 2n, n \in \mathbb{N}$.

$\Rightarrow \frac{x}{2} = \frac{2n}{2} = n \in \mathbb{Z}$, so x is divisible by 2 and is not prime. This contradicts our original statement ‘let $x > 2$ be prime’.

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Proof.

The negation is, “every prime number greater than 2 is odd”. Let $x > 2$ be prime. Suppose x is even. Then $x = 2n, n \in \mathbb{N}$.

$\Rightarrow \frac{x}{2} = \frac{2n}{2} = n \in \mathbb{Z}$, so x is divisible by 2 and is not prime. This contradicts our original statement ‘let $x > 2$ be prime’.

We supposed that x was even and arrived at a contradiction, so x must be odd. □

Example. Disprove the statement, “there exists an even prime number greater than 2”.

Proof.

The negation is, “every prime number greater than 2 is odd”. Let $x > 2$ be prime. Suppose x is even. Then $x = 2n, n \in \mathbb{N}$.

$\Rightarrow \frac{x}{2} = \frac{2n}{2} = n \in \mathbb{Z}$, so x is divisible by 2 and is not prime. This contradicts our original statement ‘let $x > 2$ be prime’.

We supposed that x was even and arrived at a contradiction, so x must be odd. □

This is an example of *proof by contradiction*, which we will see in more detail later.

Disproving $\forall$ Statements

To disprove a $\forall$ statement, we must prove an $\exists$ statement.

$$\sim (\forall\ x \in D, p(x)) \equiv\ \exists\ x \in D\ \texttt{s.t.}\ \sim p(x)$$

So we need to find one $x \in D$ such that $p(x)$ is false (a counterexample).

Disproving $\forall$ Statements

To disprove a $\forall$ statement, we must prove an $\exists$ statement.

$$\sim (\forall\, x \in D, p(x)) \equiv\ \exists\, x \in D \text{ s.t. } \sim p(x)$$

So we need to find one $x \in D$ such that $p(x)$ is false (a counterexample).

Example. Disprove the statement, "$\forall\, x \in \mathbb{R}, x < 0 \vee x > 0$".

Disproving $\forall$ Statements

To disprove a $\forall$ statement, we must prove an $\exists$ statement.

$$\sim (\forall\, x \in D, p(x)) \equiv\ \exists\, x \in D \text{ s.t. } \sim p(x)$$

So we need to find one $x \in D$ such that $p(x)$ is false (a counterexample).

Example. Disprove the statement, "$\forall\, x \in \mathbb{R}, x < 0 \vee x > 0$".

Proof.

The negation is $\exists\, x \in \mathbb{R}$ s.t. $x \geq 0 \wedge x \leq 0$.

Disproving $\forall$ Statements

To disprove a $\forall$ statement, we must prove an $\exists$ statement.

$$\sim (\forall\, x \in D, p(x)) \equiv\ \exists\, x \in D \text{ s.t. } \sim p(x)$$

So we need to find one $x \in D$ such that $p(x)$ is false (a counterexample).

Example. Disprove the statement, "$\forall\, x \in \mathbb{R}, x < 0 \vee x > 0$".

Proof.

The negation is $\exists\, x \in \mathbb{R}$ s.t. $x \geq 0 \wedge x \leq 0$.

Let $x = 0$. Then $x \geq 0 \wedge x \leq 0$. □

Example. Disprove the statement, "$\forall\, a, b \in \mathbb{R}, a^2 = b^2 \to a = b$".

Example. Disprove the statement, "$\forall\, a, b \in \mathbb{R}, a^2 = b^2 \to a = b$".

Example. Prove or disprove: $\forall\, x \in \mathbb{R}, \exists\, y \in \mathbb{R}$ s.t. $x + y = 0$.

Example. Disprove the statement, "$\forall\, a, b \in \mathbb{R}, a^2 = b^2 \to a = b$".

Example. Prove or disprove: $\forall\, x \in \mathbb{R}, \exists\, y \in \mathbb{R}$ s.t. $x + y = 0$.

Generalised Proof I: Direct Proof

A direct proof works in a straightforward manner from assumptions to conclusion. We often rewrite assumptions in logic notation.

Example. Disprove the statement, "$\forall\, a, b \in \mathbb{R}, a^2 = b^2 \to a = b$".

Example. Prove or disprove: $\forall\, x \in \mathbb{R}, \exists\, y \in \mathbb{R}$ s.t. $x + y = 0$.

Generalised Proof I: Direct Proof

A direct proof works in a straightforward manner from assumptions to conclusion. We often rewrite assumptions in logic notation.

Example. Prove that if $3x - 9 = 15$, then $x = 8$.

Example. Disprove the statement, "$\forall\, a, b \in \mathbb{R}, a^2 = b^2 \to a = b$".

Example. Prove or disprove: $\forall\, x \in \mathbb{R}, \exists\, y \in \mathbb{R}$ s.t. $x + y = 0$.

Generalised Proof I: Direct Proof

A direct proof works in a straightforward manner from assumptions to conclusion. We often rewrite assumptions in logic notation.

Example. Prove that if $3x - 9 = 15$, then $x = 8$.

Proof.

$$\begin{aligned} 3x - 9 &= 15 \\ 3x &= 15 + 9 = 24 \\ x &= \frac{24}{3} = 8 \end{aligned}$$

□

Example. Prove that the sum of any two even numbers is even.

Example. Prove that the sum of any two even numbers is even.

Proof.

Let a, b be even. Then $\exists\ c, d \in \mathbb{Z}$ s.t. $a = 2c, b = 2d$.

$$\begin{aligned} a + b &= 2c + 2d \\ &= 2(c + d) \end{aligned}$$

$c, d \in \mathbb{Z} \Rightarrow c + d \in \mathbb{Z}$
$\therefore a + b$ is even. $\square$

Example. Prove that if a, b are perfect squares, then ab is a perfect square. ($x \in \mathbb{Z}$ is a perfect square if $x = y^2$ for some $y \in \mathbb{Z}$.)

Example. Prove that if a, b are perfect squares, then ab is a perfect square. ($x \in \mathbb{Z}$ is a perfect square if $x = y^2$ for some $y \in \mathbb{Z}$.)

Proof.

$a = c^2, b = d^2$ for some $c, d \in \mathbb{Z}$

$$\begin{aligned} ab &= c^2 d^2 \\ &= (cd)^2 \end{aligned}$$

$c, d \in \mathbb{Z} \Rightarrow cd \in \mathbb{Z}$
$\therefore ab$ is a perfect square. □

Example. Prove that $\forall\, x \in \mathbb{R}, -x^2 + 2x + 1 \leq 2$.

Example. Prove that $\forall\, x \in \mathbb{R}, -x^2 + 2x + 1 \leq 2$.

Proof.

$$\begin{aligned} -x^2 + 2x + 1 \leq 2 &\Leftrightarrow -x^2 + 2x - 1 \leq 0 \\ &\Leftrightarrow x^2 - 2x + 1 \geq 0 \\ &\Leftrightarrow (x-1)^2 \geq 0 \qquad \text{(tautology)} \end{aligned}$$

$\therefore -x^2 + 2x + 1 \leq 2\ \forall\, x \in \mathbb{R}$ □

Generalised Proof II: Proof by Contradiction

Exercise. Prove that $p \to q \equiv \sim q \to \sim p$.

To prove $p \to q$, one may instead prove $\sim q \to \sim p$. That is, assume that the negation of the conclusion is true and show that one of the assumptions (or some other well-known truth) is false.

Example. Prove "$\forall\, n \in \mathbb{N}$, if n^2 is even, then n is even" by contradiction.

Example. Prove "$\forall\, n \in \mathbb{N}$, if n^2 is even, then n is even" by contradiction.

Proof.

$p(n)$: n^2 is even, $q(n)$: n is even

$\forall\, n \in \mathbb{N}, p(n) \to q(n) \equiv \forall\, n \in \mathbb{N}, \sim q(n) \to \sim p(n)$

Example. Prove "$\forall\, n \in \mathbb{N}$, if n^2 is even, then n is even" by contradiction.

Proof.

$p(n)$: n^2 is even, $q(n)$: n is even

$\forall\, n \in \mathbb{N}, p(n) \to q(n) \equiv \forall\, n \in \mathbb{N}, \sim q(n) \to \sim p(n)$

So we assume that n is odd and show that n^2 must be odd.

Example. Prove "$\forall\, n \in \mathbb{N}$, if n^2 is even, then n is even" by contradiction.

Proof.

$p(n)$: n^2 is even, $q(n)$: n is even
$\forall\, n \in \mathbb{N}, p(n) \to q(n) \equiv \forall\, n \in \mathbb{N}, \sim q(n) \to \sim p(n)$

So we assume that n is odd and show that n^2 must be odd.

Let n be odd.

$$n^2 = n \cdot n = (\text{odd})(\text{odd}) = \text{odd} \quad \text{(prop. of multiplication)}$$

$\therefore n$ odd $\Rightarrow n^2$ odd

$\therefore n^2$ even $\Rightarrow n$ even

Example. Prove that $y \in \mathbb{R} \setminus \mathbb{Q} \rightarrow y + 7 \in \mathbb{R} \setminus \mathbb{Q}$.

Example. Prove that $y \in \mathbb{R} \setminus \mathbb{Q} \rightarrow y + 7 \in \mathbb{R} \setminus \mathbb{Q}$.

Proof.

Let $y + 7 \in \mathbb{Q}$. Then $\exists\ a, b \in \mathbb{Z}, b \neq 0$ s.t. $y + 7 = \frac{a}{b}$.

Example. Prove that $y \in \mathbb{R} \setminus \mathbb{Q} \rightarrow y + 7 \in \mathbb{R} \setminus \mathbb{Q}$.

Proof.

Let $y + 7 \in \mathbb{Q}$. Then $\exists\ a, b \in \mathbb{Z}, b \neq 0$ s.t. $y + 7 = \frac{a}{b}$.

$$\begin{aligned} y &= \frac{a}{b} - 7 \\ &= \frac{a}{b} - \frac{7b}{b} \\ &= \frac{a - 7b}{b} \in \mathbb{Q} \qquad (\textit{contradiction}) \end{aligned}$$

Example. Prove that $y \in \mathbb{R} \setminus \mathbb{Q} \rightarrow y + 7 \in \mathbb{R} \setminus \mathbb{Q}$.

Proof.

Let $y + 7 \in \mathbb{Q}$. Then $\exists\ a, b \in \mathbb{Z}, b \neq 0$ s.t. $y + 7 = \frac{a}{b}$.

$$\begin{aligned} y &= \frac{a}{b} - 7 \\ &= \frac{a}{b} - \frac{7b}{b} \\ &= \frac{a - 7b}{b} \in \mathbb{Q} \qquad (\textit{contradiction}) \end{aligned}$$

$\therefore\ y + 7 \in \mathbb{R} \setminus \mathbb{Q}$ $\square$

Generalised Proof III: Proof by Cases

How do we prove "if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$"?

Generalised Proof III: Proof by Cases

How do we prove "if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$"? We need to split the problem into cases, proving the conclusion first if $x \neq 0$, then if $y \neq 0$. Any statement of the form $(p \vee q) \rightarrow r$ can be done this way, because of the logical equivalence

$$(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$$

Generalised Proof III: Proof by Cases

How do we prove "if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$"? We need to split the problem into cases, proving the conclusion first if $x \neq 0$, then if $y \neq 0$. Any statement of the form $(p \vee q) \to r$ can be done this way, because of the logical equivalence

$$(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$$

Proof.

Case 1. Let $x \neq 0$. Then $x^2 > 0$ and $y^2 \geq 0$. Hence, $x^2 + y^2 > 0$.

Case 2. Let $y \neq 0$. Then $x^2 \geq 0$ and $y^2 > 0$. Hence, $x^2 + y^2 > 0$.

$\therefore$ if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$. $\square$

Example. Prove that $\forall\ m \in \mathbb{N}, m^2 + m + 1$ is odd.

Example. Prove that $\forall\ m \in \mathbb{N}, m^2 + m + 1$ is odd.

Proof.

Case 1. Let m be even. Then m^2 is even.
$\Rightarrow m^2 + m$ is even
$\Rightarrow m^2 + m + 1$ is odd

Example. Prove that $\forall\ m \in \mathbb{N}, m^2 + m + 1$ is odd.

Proof.

Case 1. Let m be even. Then m^2 is even.
$\Rightarrow m^2 + m$ is even
$\Rightarrow m^2 + m + 1$ is odd

Case 2. Let m be odd. Then m^2 is odd.
$\Rightarrow m^2 + m$ is even
$\Rightarrow m^2 + m + 1$ is odd

Example. Prove that $\forall\, m \in \mathbb{N}, m^2 + m + 1$ is odd.

Proof.

Case 1. Let m be even. Then m^2 is even.
$\Rightarrow m^2 + m$ is even
$\Rightarrow m^2 + m + 1$ is odd

Case 2. Let m be odd. Then m^2 is odd.
$\Rightarrow m^2 + m$ is even
$\Rightarrow m^2 + m + 1$ is odd

$\therefore\ \forall\, m \in \mathbb{N}, m^2 + m + 1$ is odd. $\square$

Chapter 2:

Numbers

A *set* is a collection of objects called *elements*. We write $x \in S$ to mean that element x is in set S. A set is *nonempty* if it has at least one element. The *empty set* is denoted by $\varnothing$.

A *set* is a collection of objects called *elements*. We write $x \in S$ to mean that element x is in set S. A set is *nonempty* if it has at least one element. The *empty set* is denoted by $\varnothing$.

A *subset* of S is a set T with the property that $x \in T \Rightarrow x \in S$. We write $T \subseteq S$. Every element of T is an element of S. Trivially, $S \subseteq S$ and $\varnothing \subseteq S$.

Numbers

A *set* is a collection of objects called *elements*. We write $x \in S$ to mean that element x is in set S. A set is *nonempty* if it has at least one element. The *empty set* is denoted by $\varnothing$.

A *subset* of S is a set T with the property that $x \in T \Rightarrow x \in S$. We write $T \subseteq S$. Every element of T is an element of S. Trivially, $S \subseteq S$ and $\varnothing \subseteq S$.

The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ is useful for counting and for ordering. The order symbols are $<, \leq, >, \geq$.

Set Algebra

- An *operation* on a set S is a rule for combining elements of S.
- A *binary operation* combines pairs of elements to produce another.
- A binary operation $*$ is *closed* if $x, y \in S \Rightarrow x * y \in S$.
- Four common operations on numbers are $+, -, \cdot$ and $/$.

Set Algebra

- An *operation* on a set S is a rule for combining elements of S.
- A *binary operation* combines pairs of elements to produce another.
- A binary operation $*$ is *closed* if $x, y \in S \Rightarrow x * y \in S$.
- Four common operations on numbers are $+, -, \cdot$ and $/$.

Example. Are $+, -, \cdot, /$ closed on $\mathbb{N}$? Prove or disprove.

An element $e \in S$ is called an *identity* if

$$e * x = x \text{ and } x * e = x \ \forall \ x \in S.$$

Example. Does $\mathbb{N}$ have an identity under $+$? Under $\cdot$?

An element $e \in S$ is called an *identity* if

$$e * x = x \text{ and } x * e = x \; \forall \; x \in S.$$

Example. Does $\mathbb{N}$ have an identity under $+$? Under $\cdot$?

If $\exists$ e identity of S, an element $x \in S$ is called *invertible* when $\exists \; y \in S$ s.t.

$$x * y = e \text{ and } y * x = e.$$

Then y is called the inverse of x and vice versa.

Example. What are the invertible elements of $\mathbb{N}$ under $+$, $\cdot$?

- A binary operation $*$ on S is *commutative* if

$$x * y = y * x \ \forall \ x, y \in S.$$

- A binary operation $*$ on S is *associative* if

$$(x * y) * z = x * (y * z) \ \forall \ x, y, z \in S.$$

- The operations $+, \ \cdot$ are commutative and associative on $\mathbb{N}$.

Example. rock – paper – scissors

Let $M = \{r, p, s\}$ and consider the binary operation $*$ that gives the winner of the game:

Example. rock – paper – scissors

Let $M = \{r, p, s\}$ and consider the binary operation $*$ that gives the winner of the game:

$$r * p = p * r = p \quad \text{(paper beats rock)}$$
$$r * s = s * r = r \quad \text{(rock beats scissors)}$$
$$p * s = s * p = s \quad \text{(scissors beats paper)}$$

Example. rock – paper – scissors

Let $M = \{r, p, s\}$ and consider the binary operation $*$ that gives the winner of the game:

$r * p = p * r = p$	(paper beats rock)
$r * s = s * r = r$	(rock beats scissors)
$p * s = s * p = s$	(scissors beats paper)
$p * p = p, r * r = r, s * s = s$	(ties)

Example. rock – paper – scissors

Let $M = \{r, p, s\}$ and consider the binary operation $*$ that gives the winner of the game:

$r * p = p * r = p$	(paper beats rock)
$r * s = s * r = r$	(rock beats scissors)
$p * s = s * p = s$	(scissors beats paper)
$p * p = p, r * r = r, s * s = s$	(ties)

We see by the above that $*$ is commutative. Is it associative?

A binary operation $\cdot$ on a set S is *distributive* over another binary operation $+$ if for all $a, b, c \in S$ we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

For example, multiplication is distributive over addition on $\mathbb{N}$.

A binary operation $\cdot$ on a set S is *distributive* over another binary operation $+$ if for all $a, b, c \in S$ we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

For example, multiplication is distributive over addition on $\mathbb{N}$.

Exercise. Prove that addition is not distributive over multiplication on $\mathbb{N}$.

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$[8(a+b)] + 2a =$$

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$[8(a+b)] + 2a = (8a + 8b) + 2a \quad \text{(distributive)}$$
$$= $$

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$\begin{aligned}
[8(a+b)] + 2a &= (8a + 8b) + 2a && \text{(distributive)} \\
&= (8b + 8a) + 2a && \text{(commutative)} \\
&= &&
\end{aligned}$$

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$\begin{aligned}
[8(a+b)] + 2a &= (8a + 8b) + 2a && \text{(distributive)} \\
&= (8b + 8a) + 2a && \text{(commutative)} \\
&= 8b + (8a + 2a) && \text{(associative)} \\
&= &&
\end{aligned}$$

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$\begin{aligned}
[8(a+b)]+2a &= (8a+8b)+2a && \text{(distributive)}\\
&= (8b+8a)+2a && \text{(commutative)}\\
&= 8b+(8a+2a) && \text{(associative)}\\
&= 8b+[(8+2)a] && \text{(distributive)}\\
&= &&
\end{aligned}$$

Example. Let $a, b \in \mathbb{N}$. Simplify the following expression, giving a reason for each step.

$$\begin{aligned}
[8(a+b)] + 2a &= (8a + 8b) + 2a && \text{(distributive)} \\
&= (8b + 8a) + 2a && \text{(commutative)} \\
&= 8b + (8a + 2a) && \text{(associative)} \\
&= 8b + [(8 + 2)a] && \text{(distributive)} \\
&= 8b + 10a && \text{(addition of numbers)}
\end{aligned}$$

A set S with order $\leq$ is called *well-ordered* if every nonempty subset of S has at least one smallest element. That is,

$$\varnothing \neq T \subseteq S \Rightarrow \exists\, s_0 \in T \text{ s.t. } \leq s \,\forall\, s \in T.$$

A set S with order $\leq$ is called *well-ordered* if every nonempty subset of S has at least one smallest element. That is,

$$\varnothing \neq T \subseteq S \Rightarrow \exists\, s_0 \in T \text{ s.t. } \leq s \,\forall\, s \in T.$$

Example. The set $\mathbb{N}$ with the usual order $\leq$ is well-ordered.

The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ can be constructed from $\mathbb{N}$. It is the set of differences of all pairs of natural numbers:

$$\mathbb{Z} = \{m - n\} \; \forall \; m, n \in \mathbb{N} \, .$$

The order $\leq$ on $\mathbb{N}$ extends to $\mathbb{Z}$.

The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ can be constructed from $\mathbb{N}$. It is the set of differences of all pairs of natural numbers:

$$\mathbb{Z} = \{m - n\} \; \forall \; m, n \in \mathbb{N}\,.$$

The order $\leq$ on $\mathbb{N}$ extends to $\mathbb{Z}$.

Example.

(a) Are $+, -, \cdot, /$ closed on $\mathbb{Z}$?

(b) Does $\mathbb{Z}$ have identities under $+$ and $\cdot$?

(c) What are the invertible elements of $\mathbb{Z}$ under $+$ and $\cdot$?

On $\mathbb{Z}$, $+$ and $\cdot$ are commutative and associative, but $-$ and $/$ are not. However, if we define $a - b = a + (-b)$ and $\frac{a}{b} = a \cdot \frac{1}{b}$, then we have commutativity and associativity.

On $\mathbb{Z}$, $+$ and $\cdot$ are commutative and associative, but $-$ and $/$ are not. However, if we define $a - b = a + (-b)$ and $\frac{a}{b} = a \cdot \frac{1}{b}$, then we have commutativity and associativity.

$$a - b \neq b - a, \text{ but } a + (-b) = -b + a$$

$$\frac{a}{b} \neq \frac{b}{a}, \text{ but } a \cdot \frac{1}{b} = \frac{1}{b} \cdot a$$

On $\mathbb{Z}$, $+$ and $\cdot$ are commutative and associative, but $-$ and $/$ are not. However, if we define $a - b = a + (-b)$ and $\frac{a}{b} = a \cdot \frac{1}{b}$, then we have commutativity and associativity.

$$a - b \neq b - a, \text{ but } a + (-b) = -b + a$$
$$\frac{a}{b} \neq \frac{b}{a}, \text{ but } a \cdot \frac{1}{b} = \frac{1}{b} \cdot a$$

Multiplication is distributive over addition and subtraction on $\mathbb{Z}$.

$$a \cdot (b \pm c) = (a \cdot b) \pm (a \cdot c)$$
$$(a \pm b) \cdot c = (a \cdot c) \pm (b \cdot c)$$

Example. Is $\mathbb{Z}$ well-ordered?

Example. Is $\mathbb{Z}$ well-ordered?

- $m \in \mathbb{Z}$ is *even* if $\exists\ k \in \mathbb{Z}$ s.t. $m = 2k$.
- $m \in \mathbb{Z}$ is *odd* if $\exists\ k \in \mathbb{Z}$ s.t. $m = 2k + 1$.
- $m \in \mathbb{N} \setminus \{1\}$ is *prime* if $m = rs,\ r, s \in \mathbb{N} \Rightarrow r = 1$ or $s = 1$.
- $m \in \mathbb{N} \setminus \{1\}$ is *composite* if m is not prime.

The set of rationals $\mathbb{Q}$ is the set of numbers q that can be written $q = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$. We can construct $\mathbb{Q}$ from $\mathbb{Z}$ as the set of quotients

$$\mathbb{Q} = \left\{ \frac{a}{b} \right\} \ \forall \ a, b \in \mathbb{Z}, b \neq 0.$$

Dedekind cuts

To construct the set of real numbers $\mathbb{R}$ is a much more difficult task. We will use $\mathbb{Q}$ and the Dedekind cuts. A Dedekind cut of $\mathbb{Q}$ is a pair of subsets (A, B) of $\mathbb{Q}$ that satisfy the following.

1. A and B are nonempty.
2. $A \cup B = \mathbb{Q}$
3. A is closed downwards: if $q \in A$ and $r < q$, then $r \in A$.
4. B is closed upwards: if $q \in B$ and $r > q$, then $r \in B$.
5. A contains no greatest element: $\forall\, q \in A\ \exists\, r \in A$ s.t. $q < r$.

Given $q \in \mathbb{Q}$, we can form a Dedekind cut (A, B) where

$$A = \{x \in \mathbb{Q} : x < q\}, \qquad B = \{x \in \mathbb{Q} : x \geq q\}.$$

This is the Dedekind cut identification of all rational numbers $q \in \mathbb{Q}$.

Given $q \in \mathbb{Q}$, we can form a Dedekind cut (A, B) where

$$A = \{x \in \mathbb{Q} : x < q\}, \qquad B = \{x \in \mathbb{Q} : x \geq q\}.$$

This is the Dedekind cut identification of all rational numbers $q \in \mathbb{Q}$. But we can make such cuts at irrational numbers as well. An irrational number is a number that cannot be written as $\frac{a}{b}, a, b \in \mathbb{Z}$. One example is $\sqrt{2}$.

Exercise. Prove that $\sqrt{2} \notin \mathbb{Q}$.

Given $q \in \mathbb{Q}$, we can form a Dedekind cut (A, B) where

$$A = \{x \in \mathbb{Q} : x < q\}, \qquad B = \{x \in \mathbb{Q} : x \geq q\}.$$

This is the Dedekind cut identification of all rational numbers $q \in \mathbb{Q}$. But we can make such cuts at irrational numbers as well. An irrational number is a number that cannot be written as $\frac{a}{b}, a, b \in \mathbb{Z}$. One example is $\sqrt{2}$.

Exercise. Prove that $\sqrt{2} \notin \mathbb{Q}$.

The following Dedekind cut defines $\sqrt{2}$.

$$A = \{x : x < 0 \text{ or } x^2 < 2\}, \qquad B = \{x : x > 0 \text{ and } x^2 \geq 2\}$$

The numbers defined by all Dedekind cuts of $\mathbb{Q}$ make up the set of real numbers $\mathbb{R}$. The usual order $\leq$ on $\mathbb{R}$ is inherited from $\mathbb{Q}$.

The numbers defined by all Dedekind cuts of $\mathbb{Q}$ make up the set of real numbers $\mathbb{R}$. The usual order $\leq$ on $\mathbb{R}$ is inherited from $\mathbb{Q}$.

Example.

(a) Which of $+, -, \cdot, /$ are closed on $\mathbb{R}$?

(b) Does $\mathbb{R}$ have identities under $+, \cdot$?

(c) What are the invertible elements in $\mathbb{R}$ under $+, \cdot$?

The numbers defined by all Dedekind cuts of $\mathbb{Q}$ make up the set of real numbers $\mathbb{R}$. The usual order $\leq$ on $\mathbb{R}$ is inherited from $\mathbb{Q}$.

Example.

(a) Which of $+, -, \cdot, /$ are closed on $\mathbb{R}$?

(b) Does $\mathbb{R}$ have identities under $+, \cdot$?

(c) What are the invertible elements in $\mathbb{R}$ under $+, \cdot$?

As in $\mathbb{Q}$, the operations $+, \cdot$ are commutative and associative in $\mathbb{R}$ and $-, /$ are not, unless we define them as we did in $\mathbb{Q}$.

Mathematical Induction

Recall the induction principle: If $\operatorname{dom} p = \mathbb{N}$ such that

(a) $p(1)$ is true and

(b) $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$.

Exercise. Prove the induction principle (hint: by contradiction).

Example.

1. Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2} \ \forall \ n \in \mathbb{N}$.
2. Prove that $n^3 > 2n - 2 \ \forall \ n \in \mathbb{N}$.
3. Prove that $(n + 1)! \geq 2^n \ \forall \ n \in \mathbb{N}$.
4. Prove that $6|(3n^2 + 3n) \ \forall \ n \in \mathbb{N}$.

Proof.

1. (a) $1 = \frac{1(1+1)}{2}$

Proof.

1. (a) $1 = \frac{1(1+1)}{2}$

(b) Suppose $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$, show $1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}$.

Proof.

1. (a) $1 = \frac{1(1+1)}{2}$

(b) Suppose $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$, show $1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}$.

$$\begin{aligned} 1 + \cdots + (k+1) &= (1 + \cdots + k) + (k+1) \\ &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k^2 + k}{2} + \frac{2k+2}{2} = \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

□

Proof.

1. (a) $1^3 > 2(1) - 2 \Leftrightarrow 1 > 0$

Proof.

1. (a) $1^3 > 2(1) - 2 \Leftrightarrow 1 > 0$
(b) Suppose $k^3 > 2k - 2$, show $(k+1)^3 > 2(k+1) - 2 = 2k$.

Proof.

1. (a) $1^3 > 2(1) - 2 \Leftrightarrow 1 > 0$
(b) Suppose $k^3 > 2k - 2$, show $(k+1)^3 > 2(k+1) - 2 = 2k$.

$$\begin{aligned}(k+1)^3 &= k^3 + 3k^2 + 3k + 1 \\ &> (2k-2) + 3k^2 + 3k + 1 \\ &= 3k^2 + 5k - 1 \\ &= 2k + (3k^2 + 3k - 1) \\ &> 2k\end{aligned}$$

□

Proof.

3. (a) $(1+1)! \geq 2^1 \Leftrightarrow 2 \geq 2$

Proof.

3. (a) $(1+1)! \geq 2^1 \Leftrightarrow 2 \geq 2$
(b) Suppose $(k+1)! \geq 2^k$, show$(k+2)! \geq 2^{k+1}$.

Proof.

3. (a) $(1+1)! \geq 2^1 \Leftrightarrow 2 \geq 2$
(b) Suppose $(k+1)! \geq 2^k$, show$(k+2)! \geq 2^{k+1}$.

$$\begin{aligned}(k+2)! &= (k+1)!(k+2) \\ &\geq 2^k(k+2) \\ &= 2^k k + 2^{k+1} \\ &> 2^{k+1}\end{aligned}$$

□

Proof.

4. (a) $6|(3 \cdot 1^2 + 3 \cdot 1) \Leftrightarrow 6|6$

Proof.

4. (a) $6|(3 \cdot 1^2 + 3 \cdot 1) \Leftrightarrow 6|6$
(b) Suppose $6|(3k^2 + 3k)$, show $6|[3(k+1)^2 + 3(k+1)]$.

Proof.

4. (a) $6|(3 \cdot 1^2 + 3 \cdot 1) \Leftrightarrow 6|6$
(b) Suppose $6|(3k^2 + 3k)$, show $6|[3(k+1)^2 + 3(k+1)]$.

$$\begin{aligned} 3(k+1)^2 + 3(k+1) &= 3(k^2 + 2k + 1) + 3k + 3 \\ &= (3k^2 + 3k) + 6k + 6 \\ &= 6\left(\frac{3k^2 + 3k}{6} + k + 1\right) \\ &= 6m \text{ for some } m \in \mathbb{N} \end{aligned}$$

□

Sigma Notation

We use capital sigma Σ to shorten the notation of long sums:

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + a_3 + \cdots + a_k$$

Sigma Notation

We use capital sigma Σ to shorten the notation of long sums:

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + a_3 + \cdots + a_k$$

Example. Expand. (a) $\sum_{i=2}^{6} 2i^2$ (b) $\sum_{j=1}^{10} 2$

Sigma Notation

We use capital sigma Σ to shorten the notation of long sums:

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + a_3 + \cdots + a_k$$

Example. Expand. (a) $\sum_{i=2}^{6} 2i^2$ (b) $\sum_{j=1}^{10} 2$

Example. Simplify.
(a) $1 + 3 + 5 + \cdots + 13$
(b) $4 + 9 + 16 + \cdots + m^2$

By the laws of addition, we have the following properties.

$$\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=M}^{n} b_i \tag{1}$$

$$\sum_{i=m}^{n} ka_i = k\sum_{i=m}^{n} a_i \tag{2}$$

Generalised Mathematical Induction

Let $a \in \mathbb{N}$ and let $p(n)$ be defined for all $n \in \mathbb{N}, n \geq a$. If

(a) $p(a)$ is true and

(b) for all $k \in \mathbb{N}, k \geq a$, $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$, $n \geq a$.

Generalised Mathematical Induction

Let $a \in \mathbb{N}$ and let $p(n)$ be defined for all $n \in \mathbb{N}, n \geq a$. If

(a) $p(a)$ is true and

(b) for all $k \in \mathbb{N}, k \geq a$, $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$, $n \geq a$.

Example. Is $2^n > 2n + 1 \ \forall \ n \in \mathbb{N}$?

Generalised Mathematical Induction

Let $a \in \mathbb{N}$ and let $p(n)$ be defined for all $n \in \mathbb{N}, n \geq a$. If

(a) $p(a)$ is true and

(b) for all $k \in \mathbb{N}, k \geq a$, $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$, $n \geq a$.

Example. Is $2^n > 2n + 1 \ \forall \ n \in \mathbb{N}$?

$2^1 > 2 \cdot 1 + 1 \Leftrightarrow 2 > 3$ NO

Generalised Mathematical Induction

Let $a \in \mathbb{N}$ and let $p(n)$ be defined for all $n \in \mathbb{N}, n \geq a$. If

(a) $p(a)$ is true and

(b) for all $k \in \mathbb{N}, k \geq a$, $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$, $n \geq a$.

Example. Is $2^n > 2n+1 \ \forall \ n \in \mathbb{N}$?

$2^1 > 2 \cdot 1 + 1 \Leftrightarrow 2 > 3$ NO

Example. Prove that $2^n > 2n+1 \ \forall \ n \in \mathbb{N}, \ n \geq 3$.

Proof.

(a) $2^3 > 2 \cdot 3 + 1 \Leftrightarrow 8 > 7$

Proof.

(a) $2^3 > 2 \cdot 3 + 1 \Leftrightarrow 8 > 7$

(b) Suppose $2^k > 2k + 1,\ k \geq 3$. Show $2^{k+1} > 2(k + 1) + 1$.

Proof.

(a) $2^3 > 2 \cdot 3 + 1 \Leftrightarrow 8 > 7$

(b) Suppose $2^k > 2k + 1,\ k \geq 3$. Show $2^{k+1} > 2(k+1) + 1$.

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k > 2(2k+1) = 4k + 2 \\ &= 2(k+1) + 2k \\ &\geq 2(k+1) + 6 \\ &> 2(k+1) + 1 \end{aligned}$$

□

Example. Prove that $\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall \ n \geq 2, \ n \in \mathbb{N}$.

Example. Prove that $\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall\ n \geq 2,\ n \in \mathbb{N}$.

Proof.

(a) $\sum_{i=1}^{2-1} \frac{i}{i+1} < \frac{n^2}{n+1} \Leftrightarrow \frac{1}{1+1} < \frac{2^2}{2+1} \Leftrightarrow \frac{1}{2} < \frac{4}{3}$

Example. Prove that $\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall\ n \geq 2,\ n \in \mathbb{N}$.

Proof.

(a) $\sum_{i=1}^{2-1} \frac{i}{i+1} < \frac{n^2}{n+1} \Leftrightarrow \frac{1}{1+1} < \frac{2^2}{2+1} \Leftrightarrow \frac{1}{2} < \frac{4}{3}$

(b) Suppose $\sum_{i=1}^{k-1} \frac{i}{i+1} < \frac{k^2}{k+1}$. Show $\sum_{i=1}^{k} \frac{i}{i+1} < \frac{(k+1)^2}{k+2}$.

Example. Prove that $\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall\ n \geq 2,\ n \in \mathbb{N}$.

Proof.

(a) $\sum_{i=1}^{2-1} \frac{i}{i+1} < \frac{n^2}{n+1} \Leftrightarrow \frac{1}{1+1} < \frac{2^2}{2+1} \Leftrightarrow \frac{1}{2} < \frac{4}{3}$

(b) Suppose $\sum_{i=1}^{k-1} \frac{i}{i+1} < \frac{k^2}{k+1}$. Show $\sum_{i=1}^{k} \frac{i}{i+1} < \frac{(k+1)^2}{k+2}$.

$$\sum_{i=1}^{k} \frac{i}{i+1} = \sum_{i=1}^{k-1} \frac{i}{i+1} + \frac{k}{k+1}$$

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

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

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

□

Recursive Sequences

A sequence of numbers $a_1, a_2, a_3, \ldots$ is defined *recursively* if each a_n for $n \geq n_0$ is defined in terms of some or all of $a_1, a_2, \ldots, a_{n_0}$.

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \geq 3$. Find a_3 and a_4.

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \geq 3$. Find a_3 and a_4.

Example. The Fibonacci numbers constitute the famous sequence $1, 1, 2, 3, 5, 8, 13, \ldots$ defined by

$$f_1 = f_2 = 1,\ f_n = f_{n-1} + f_{n-2}\ \forall\ n \geq 3.$$

Can we show that $f_n < 2^n\ \forall\ n \in \mathbb{N}$?

Strong Mathematical Induction

Let $p(n)$ be defined for all $n \in \mathbb{N}$ and let $a \in \mathbb{N}$. If

(a) $p(1), p(2), \ldots, p(a)$ are true and

(b) for all $k \in \mathbb{N}, k \geq a$, $p(k)$ true $\Rightarrow p(k+1)$ true,

then $p(n)$ is true for all $n \in \mathbb{N}$.

Example. For the Fibonacci sequence $f_1 = f_2 = 1$, $f_n = f_{n-1} + f_{n=2}\ \forall\ n \geq 3$, prove that $f_n < 2^n\ \forall\ n \in \mathbb{N}$.

Example. For the Fibonacci sequence $f_1 = f_2 = 1$, $f_n = f_{n-1} + f_{n=2}\ \forall\ n \geq 3$, prove that $f_n < 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $f_1 = 1 < 2^1 = 2$; $f_2 = 1 < 2^2 = 4$; $f_3 = 2 < 2^3 = 8$ (by hand until the first recursion).

Example. For the Fibonacci sequence $f_1 = f_2 = 1$, $f_n = f_{n-1} + f_{n=2}\ \forall\ n \geq 3$, prove that $f_n < 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $f_1 = 1 < 2^1 = 2$; $f_2 = 1 < 2^2 = 4$; $f_3 = 2 < 2^3 = 8$ (by hand until the first recursion).

(b) Suppose for $k \geq 3$ that $f_1 < 2^1$, $f_2 < 2^2$, ..., $f_k < 2^k$. Show $f_{k+1} < 2^{k+1}$.

Example. For the Fibonacci sequence $f_1 = f_2 = 1$, $f_n = f_{n-1} + f_{n=2}\ \forall\ n \geq 3$, prove that $f_n < 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $f_1 = 1 < 2^1 = 2$; $f_2 = 1 < 2^2 = 4$; $f_3 = 2 < 2^3 = 8$ (by hand until the first recursion).

(b) Suppose for $k \geq 3$ that $f_1 < 2^1$, $f_2 < 2^2$, ..., $f_k < 2^k$. Show $f_{k+1} < 2^{k+1}$.

$$f_{k+1} = f_k + f_{k-1} < 2^k + 2^{k-1} < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$ □

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \in \mathbb{N}$.
Prove that $a_n = 2^n\ \forall\ n \in \mathbb{N}$.

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \in \mathbb{N}$.
Prove that $a_n = 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $a_1 = 2^1$, $a_2 = 2^2$, $a_3 = 5 \cdot 4 - 6 \cdot 2 = 8 = 2^3$

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \in \mathbb{N}$. Prove that $a_n = 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $a_1 = 2^1$, $a_2 = 2^2$, $a_3 = 5 \cdot 4 - 6 \cdot 2 = 8 = 2^3$

(b) Suppose for $k \geq 3$, $a_i = 2^i$ for $i = 1, 2, \ldots, k$. Prove $a_{k+1} = 2^{k+1}$.

Example. Let $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \in \mathbb{N}$. Prove that $a_n = 2^n\ \forall\ n \in \mathbb{N}$.

Proof.

(a) $a_1 = 2^1$, $a_2 = 2^2$, $a_3 = 5 \cdot 4 - 6 \cdot 2 = 8 = 2^3$

(b) Suppose for $k \geq 3$, $a_i = 2^i$ for $i = 1, 2, \ldots, k$. Prove $a_{k+1} = 2^{k+1}$.

$$\begin{aligned} a_{k+1} &= 5a_k - 6a_{k-1} = 5 \cdot 2^k - 6 \cdot 2^{k-1} \\ &= 5 \cdot 2^k - 3 \cdot 2^k = 2 \cdot 2^k = 2^{k+1} \end{aligned}$$

□

Number Theory

Let $n, d \in \mathbb{Z}$, $d \neq 0$. We say that n is *divisible* by d if $n = dk$ for some $k \in \mathbb{Z}$. We write $d|n$ and call d a *divisor* of n and n a *multiple* of d. If d does not divide n, we write $d \nmid n$.

Number Theory

Let $n, d \in \mathbb{Z}$, $d \neq 0$. We say that n is *divisible* by d if $n = dk$ for some $k \in \mathbb{Z}$. We write $d|n$ and call d a *divisor* of n and n a *multiple* of d. If d does not divide n, we write $d \nmid n$.

Transitivity of Divisibility: If $a, b, c \in \mathbb{Z}$ s.t. $a|b \wedge b|c$, then $a|c$.

Number Theory

Let $n, d \in \mathbb{Z}$, $d \neq 0$. We say that n is *divisible* by d if $n = dk$ for some $k \in \mathbb{Z}$. We write $d|n$ and call d a *divisor* of n and n a *multiple* of d. If d does not divide n, we write $d \nmid n$.

Transitivity of Divisibility: If $a, b, c \in \mathbb{Z}$ s.t. $a|b \wedge b|c$, then $a|c$.

Proof.

$$a|b \Rightarrow \exists d \in \mathbb{Z} \text{ s.t. } b = ad$$
$$b|c \Rightarrow \exists e \in \mathbb{Z} \text{ s.t. } c = be$$
$$\Rightarrow c = be = (ad)e = a(de),\ de \in \mathbb{Z}$$
$$\therefore a|c$$

□

Divisibility by Primes: Every $n \in \mathbb{N} \setminus \{1\}$ is divisible by some prime number.

Divisibility by Primes: Every $n \in \mathbb{N} \setminus \{1\}$ is divisible by some prime number.

Proof.

Strong induction. (a) $2|2$

Divisibility by Primes: Every $n \in \mathbb{N} \setminus \{1\}$ is divisible by some prime number.

Proof.

Strong induction. (a) $2|2$

(b)For $k > 2$, suppose every integer m s.t. $1 < m \leq k$ is divisible by a prime. Show that $k + 1$ is divisible by a prime.

Divisibility by Primes: Every $n \in \mathbb{N} \setminus \{1\}$ is divisible by some prime number.

Proof.

Strong induction. (a) $2|2$

(b)For $k > 2$, suppose every integer m s.t. $1 < m \leq k$ is divisible by a prime. Show that $k + 1$ is divisible by a prime.

Case 1: Let $k + 1$ be prime. Then $(k + 1)|(k + 1)$

Divisibility by Primes: Every $n \in \mathbb{N} \setminus \{1\}$ is divisible by some prime number.

Proof.

Strong induction. (a) $2|2$

(b)For $k > 2$, suppose every integer m s.t. $1 < m \leq k$ is divisible by a prime. Show that $k+1$ is divisible by a prime.

Case 1: Let $k+1$ be prime. Then $(k+1)|(k+1)$

Case 2: Let $k+1$ be composite. Then $k+1 = ab$ for some $a, b \in \mathbb{N} \setminus \{1\},\ a, b < k+1$. By hypothesis, $\exists\ c$ prime s.t. $c|a$. Then by transitivity,

$c|a \wedge a|(k+1) \Rightarrow c|(k+1)$. □

Theorem: There are infinitely many prime numbers.

Theorem: There are infinitely many prime numbers.

Proof (by contradiction).

Suppose there is a finite number of primes, $p_1, p_2, \ldots, p_n$. Let $p = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Clearly p is larger than all the primes, so p is not equal to any of the primes.

Theorem: There are infinitely many prime numbers.

Proof (by contradiction).

Suppose there is a finite number of primes, $p_1, p_2, \ldots, p_n$. Let $p = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Clearly p is larger than all the primes, so p is not equal to any of the primes. Hence, p is divisible by a prime. Without loss of generality (WLOG), let $p_1 | p$. Then

$$\frac{p}{p_1} = \frac{p_1 p_2 \cdots p_n + 1}{p_1} = p_2 p_3 \cdots p_n + \frac{1}{p_1} \notin \mathbb{Z}.$$

This is a contradiction. Therefore, there is an infinite number of primes. □

Quotient-Remainder Theorem

Let $n \in \mathbb{Z}, d \in \mathbb{N}$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

Quotient-Remainder Theorem

Let $n \in \mathbb{Z}, d \in \mathbb{N}$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

Example. Find $q, r,$ s.t. $n = dq + r, 0 \leq r < d$.

1. $n = 54, d = 4$
2. $n = -32, d = 7$
3. $n = 42, d = 70$
4. $n = 121, d = 11$

Fundamental Theorem of Arithmetic

Every $a \in \mathbb{N} \setminus \{1\}$ can be factored uniquely in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $k \in \mathbb{N}, \alpha_i \in \mathbb{N} \ \forall \ i$ and p_i is prime $\forall \ i$.

Fundamental Theorem of Arithmetic

Every $a \in \mathbb{N} \setminus \{1\}$ can be factored uniquely in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $k \in \mathbb{N}, \alpha_i \in \mathbb{N}\ \forall\ i$ and p_i is prime $\forall\ i$.

Example. (a) $48 = 2^4 \cdot 3$ (b) $4665 = 5 \cdot 7^2 \cdot 19$

Fundamental Theorem of Arithmetic

Every $a \in \mathbb{N} \setminus \{1\}$ can be factored uniquely in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $k \in \mathbb{N}, \alpha_i \in \mathbb{N}\ \forall\ i$ and p_i is prime $\forall\ i$.

Example. (a) $48 = 2^4 \cdot 3$ (b) $4665 = 5 \cdot 7^2 \cdot 19$

The proof of the theorem requires the following lemma.

Euclid's Lemma: Let p be prime, $a, b \in \mathbb{N}$. If $p|ab$, then $p|a \vee p|b$.

Fundamental Theorem of Arithmetic

Every $a \in \mathbb{N} \setminus \{1\}$ can be factored uniquely in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $k \in \mathbb{N}, \alpha_i \in \mathbb{N}\ \forall\ i$ and p_i is prime $\forall\ i$.

Example. (a) $48 = 2^4 \cdot 3$ (b) $4665 = 5 \cdot 7^2 \cdot 19$

The proof of the theorem requires the following lemma.

Euclid's Lemma: Let p be prime, $a, b \in \mathbb{N}$. If $p|ab$, then $p|a \vee p|b$.

Example. $5|100$ and $100 = 25 \cdot 4$, so either $5|25$ or $5|4$ (the former is true).

Proof (Fundamental Theorem - Part 1).

First, show that every $a \in \mathbb{N}$ is either prime or a product of primes, by strong induction.

Proof (Fundamental Theorem - Part 1).

First, show that every $a \in \mathbb{N}$ is either prime or a product of primes, by strong induction.

(a) 2 is prime.

Proof (Fundamental Theorem - Part 1).

First, show that every $a \in \mathbb{N}$ is either prime or a product of primes, by strong induction.

(a) 2 is prime.

Suppose $2, 3, \ldots, k$ are all either primes or products of primes. Show that $k + 1$ is either prime or a product of primes.

Proof (Fundamental Theorem - Part 1).

First, show that every $a \in \mathbb{N}$ is either prime or a product of primes, by strong induction.

(a) 2 is prime.

Suppose $2, 3, \ldots, k$ are all either primes or products of primes. Show that $k+1$ is either prime or a product of primes.

If $k+1$ is prime, there is nothing more to prove. If not, then it is composite: $\exists\, b, c \in \mathbb{Z}$ s.t. $1 < b \leq c < k+1 \wedge k+1 = bc$. By hypothesis, $b = p_1 p_2 \cdots p_j$ and $c = q_1 q_2 \cdots q_m$ are products of primes.

Proof (Fundamental Theorem - Part 1).

First, show that every $a \in \mathbb{N}$ is either prime or a product of primes, by strong induction.

(a) 2 is prime.

Suppose $2, 3, \ldots, k$ are all either primes or products of primes. Show that $k+1$ is either prime or a product of primes.

If $k+1$ is prime, there is nothing more to prove. If not, then it is composite: $\exists\, b, c \in \mathbb{Z}$ s.t. $1 < b \leq c < k+1 \wedge k+1 = bc$. By hypothesis, $b = p_1 p_2 \cdots p_j$ and $c = q_1 q_2 \cdots q_m$ are products of primes.

Then $k+1 = bc = p_1 p_2 \cdots p_j q_1 q_2 \cdots q_m$ is a product of primes.

Therefore, every $a \in \mathbb{N} \setminus \{1\}$ is either a prime or a product of primes. □

Proof (Fundamental Theorem - Part 2).

Now show uniqueness. Suppose a is two different products:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Proof (Fundamental Theorem - Part 2).

Now show uniqueness. Suppose a is two different products:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Since $p_1 | a$, $p_1 | q_i$ for some i. WLOG, let $p_1 | q_1$. Since q_1 is prime, $p_1 = q_1$ and

$$\frac{a}{p_1} = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

Proof (Fundamental Theorem - Part 2).

Now show uniqueness. Suppose a is two different products:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Since $p_1 | a$, $p_1 | q_i$ for some i. WLOG, let $p_1 | q_1$. Since q_1 is prime, $p_1 = q_1$ and

$$\frac{a}{p_1} = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

By the same logic, WLOG $p_2 | q_2$ and

$$\frac{a}{p_1 p_2} = p_3 p_4 \cdots p_m = q_3 q_4 \cdots q_n.$$

Proof (Fundamental Theorem - Part 2).

Now show uniqueness. Suppose a is two different products:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Since $p_1 | a$, $p_1 | q_i$ for some i. WLOG, let $p_1 | q_1$. Since q_1 is prime, $p_1 = q_1$ and

$$\frac{a}{p_1} = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

By the same logic, WLOG $p_2 | q_2$ and

$$\frac{a}{p_1 p_2} = p_3 p_4 \cdots p_m = q_3 q_4 \cdots q_n.$$

Continuing like this, we find $m \leq n$ and $p_i = q_i \; \forall \; i \in \{1, 2, \ldots, m\}$. The same argument with p and q reversed gives $n \leq m$ and $q_i = p_i \; \forall \; i \in \{1, 2, \ldots, n\}$.

Proof (Fundamental Theorem - Part 2).

Now show uniqueness. Suppose a is two different products:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Since $p_1 | a$, $p_1 | q_i$ for some i. WLOG, let $p_1 | q_1$. Since q_1 is prime, $p_1 = q_1$ and

$$\frac{a}{p_1} = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

By the same logic, WLOG $p_2 | q_2$ and

$$\frac{a}{p_1 p_2} = p_3 p_4 \cdots p_m = q_3 q_4 \cdots q_n.$$

Continuing like this, we find $m \leq n$ and $p_i = q_i \; \forall \; i \in \{1, 2, \ldots, m\}$. The same argument with p and q reversed gives $n \leq m$ and $q_i = p_i \; \forall \; i \in \{1, 2, \ldots, n\}$.

Therefore, $m = n$ and the two factorisations are the same. □

Example. Find the prime factorisations.

1. 924
2. 1300
3. 2722
4. 50,193

Example. Find the prime factorisations.

1. 924
2. 1300
3. 2722
4. 50,193

1. $924 = 2 \cdot 462 = 2^2 \cdot 231 = 2^2 \cdot 3 \cdot 77 = 2^2 \cdot 3 \cdot 7 \cdot 11$

Example. Find the prime factorisations.

1. 924
2. 1300
3. 2722
4. 50,193

1. $924 = 2 \cdot 462 = 2^2 \cdot 231 = 2^2 \cdot 3 \cdot 77 = 2^2 \cdot 3 \cdot 7 \cdot 11$
2. $1300 = 2 \cdot 650 = 2^2 \cdot 325 = 2^2 \cdot 5 \cdot 65 = 2^2 \cdot 5^2 \cdot 13$

Example. Find the prime factorisations.

1. 924
2. 1300
3. 2722
4. 50,193

1. $924 = 2 \cdot 462 = 2^2 \cdot 231 = 2^2 \cdot 3 \cdot 77 = 2^2 \cdot 3 \cdot 7 \cdot 11$
2. $1300 = 2 \cdot 650 = 2^2 \cdot 325 = 2^2 \cdot 5 \cdot 65 = 2^2 \cdot 5^2 \cdot 13$
3. $2722 = 2 \cdot 1361$

Example. Find the prime factorisations.

1. 924
2. 1300
3. 2722
4. 50,193

1. $924 = 2 \cdot 462 = 2^2 \cdot 231 = 2^2 \cdot 3 \cdot 77 = 2^2 \cdot 3 \cdot 7 \cdot 11$
2. $1300 = 2 \cdot 650 = 2^2 \cdot 325 = 2^2 \cdot 5 \cdot 65 = 2^2 \cdot 5^2 \cdot 13$
3. $2722 = 2 \cdot 1361$
4. $50,193 = 3 \cdot 16,731 = 3^2 \cdot 5577 = 3^3 \cdot 1859 = 3^3 \cdot 11 \cdot 169 = 3^3 \cdot 11 \cdot 13^2$

Definition

*Let $a, b \in \mathbb{Z}, b \neq 0$. The **greatest common divisor (GCD)** of a and b, denoted by $\gcd(a, b)$, is the number $c \in \mathbb{N}$ such that*

(a) *$c|a$ and $c|b$;*

(b) *if $d|a$ and $d|b$, then $d \leq c$.*

Definition

*Let $a, b \in \mathbb{Z}, b \neq 0$. The **greatest common divisor (GCD)** of a and b, denoted by $\gcd(a, b)$, is the number $c \in \mathbb{N}$ such that*

(a) *$c|a$ and $c|b$;*

(b) *if $d|a$ and $d|b$, then $d \leq c$.*

Example. $\gcd(18, 12) = 6$, since $6|18$ and $6|12$ and there is no bigger integer that divides them both.

Note that
$\gcd(18, 12) = \gcd(-18, 12) = \gcd(18, -12) = \gcd(-18, -12)$.

Prime factorisations can be used to find GCDs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\gcd(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \min\{\alpha_i, \beta_i\}$.

Prime factorisations can be used to find GCDs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\gcd(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \min\{\alpha_i, \beta_i\}$.

Example. Given $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have

$$\gcd(3220, 1155) = 5 \cdot 7 = 35.$$

Prime factorisations can be used to find GCDs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\gcd(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \min\{\alpha_i, \beta_i\}$.

Example. Given $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have

$$\gcd(3220, 1155) = 5 \cdot 7 = 35.$$

Example. Find $\gcd(35100, 6975)$.

Definition

*Let $a, b \in \mathbb{Z}, b \neq 0$. The **least common multiple (LCM)** of a and b, denoted by $\operatorname{lcm}(a, b)$, is the number $c \in \mathbb{N}$ such that*

(a) *$a|c$ and $b|c$;*

(b) *if $a|d$ and $b|d$, then $c \leq d$.*

Definition

*Let $a, b \in \mathbb{Z}, b \neq 0$. The **least common multiple (LCM)** of a and b, denoted by $\text{lcm}(a, b)$, is the number $c \in \mathbb{N}$ such that*

(a) *$a|c$ and $b|c$;*

(b) *if $a|d$ and $b|d$, then $c \leq d$.*

Example. (a) $\text{lcm}(12, 4) = 12$ (b) $\text{lcm}(18, 15) = 90$

Prime factorisations can be used to find LCMs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\text{lcm}(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Prime factorisations can be used to find LCMs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\operatorname{lcm}(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Example. Given $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have

$$\operatorname{lcm}(3220, 1155) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 106260.$$

Prime factorisations can be used to find LCMs. If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

(some α_i, β_j can be zero), then

$$\operatorname{lcm}(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Example. Given $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have

$$\operatorname{lcm}(3220, 1155) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 106260.$$

Example. Find $\operatorname{lcm}(31500, 6975)$.
Example. Find $\gcd(268944, 198466)$.

The Euclidean algorithm

The Euclidean algorithm is a process for finding GCDs. It works because if the quotient-remainder theorem and the following two lemmas.

Lemma

For all $r \in \mathbb{N}$, $\gcd(r, 0) = r$.

Exercise. Prove it.

The Euclidean algorithm

The Euclidean algorithm is a process for finding GCDs. It works because if the quotient-remainder theorem and the following two lemmas.

Lemma

For all $r \in \mathbb{N}$, $\gcd(r, 0) = r$.

Exercise. Prove it.

Lemma

Let $a, b \in \mathbb{Z}, b \neq 0, q, r \in \mathbb{N}$ s.t. $a = bq + r$. *Then*

$$\gcd(a, b) = \gcd(b, r).$$

Proof (Part 1).

Let $D = \{d \in \mathbb{Z} : d|a, d|b\}$, $\overline{D} = \{d \in \mathbb{Z} : d|b, d|r\}$. We show that $D = \overline{D}$.

Proof (Part 1).

Let $D = \{d \in \mathbb{Z} : d|a, d|b\}$, $\overline{D} = \{d \in \mathbb{Z} : d|b, d|r\}$. We show that $D = \overline{D}$.

($\subseteq$): Let $x \in D$. Then $x|a$ and $x|b$. We have

$$\begin{aligned} a &= bq + r \\ a - bq &= r \\ \frac{a - bq}{x} &= \frac{r}{x} \\ \frac{a}{x} - \frac{bq}{x} &= \frac{r}{x}. \end{aligned}$$

Proof (Part 1).

Let $D = \{d \in \mathbb{Z} : d|a, d|b\}$, $\overline{D} = \{d \in \mathbb{Z} : d|b, d|r\}$. We show that $D = \overline{D}$.

($\subseteq$): Let $x \in D$. Then $x|a$ and $x|b$. We have

$$\begin{aligned} a &= bq + r \\ a - bq &= r \\ \frac{a - bq}{x} &= \frac{r}{x} \\ \frac{a}{x} - \frac{bq}{x} &= \frac{r}{x}. \end{aligned}$$

Since $\frac{a}{x}$ and $\frac{bq}{x}$ are integers, $\frac{r}{x}$ is too, so $x|r$. Hence, $x \in \overline{D}$ and we have $D \subseteq \overline{D}$. □

Proof (Part 2).

($\supseteq$): Let $x \in \overline{D}$. Then $x|b$ and $x|r$. We have

$$a = bq + r$$

$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}$$

Proof (Part 2).

($\supseteq$): Let $x \in \overline{D}$. Then $x|b$ and $x|r$. We have

$$a = bq + r$$
$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}$$

Since $\frac{bq}{x}$ and $\frac{r}{x}$ are integers, $\frac{a}{x}$ is too, so $x|a$. Hence, $x \in D$ and we have $\overline{D} \subseteq D$, so $D = \overline{D}$.

Proof (Part 2).

($\supseteq$): Let $x \in \overline{D}$. Then $x|b$ and $x|r$. We have

$$a = bq + r$$
$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}$$

Since $\frac{bq}{x}$ and $\frac{r}{x}$ are integers, $\frac{a}{x}$ is too, so $x|a$. Hence, $x \in D$ and we have $\overline{D} \subseteq D$, so $D = \overline{D}$.

So every common divisor of a, b is also a common divisor of b, r and vice versa.

$$\therefore \gcd(a, b) = \max_{d \in D} d = \max_{d \in \overline{D}} d = \gcd(b, r). \qquad \square$$

Euclidean algorithm:

1. Let $a > b \geq 0$.
2. Check if $b = 0$. If so, $\gcd(a, b) = a$ (lemma).
3. If $b \neq 0$, use quotient-remainder theorem to find q, r. Then $\gcd(a, b) = \gcd(b, r)$ (lemma).
4. Set $a = b$, $b = r$ and go to Step 2.

This algorithm will terminate with $r = 0$, since each remainder is smaller than the previous one.

Example. Find $\gcd(2772, 2310)$.

Example. Find $\gcd(2772, 2310)$.

$$2772 = 2310 \cdot 1 + 462$$

Example. Find $\gcd(2772, 2310)$.

$$2772 = 2310 \cdot 1 + 462$$
$$2310 = 462 \cdot 5 + 0$$

Example. Find $\gcd(2772, 2310)$.

$$2772 = 2310 \cdot 1 + 462$$
$$2310 = 462 \cdot 5 + 0$$

$\therefore \gcd(2772, 2310) = 462.$

Example. Find $\gcd(-243, 223)$.

Example. Find $\gcd(-243, 223)$.

$$243 = 223 \cdot 1 + 20 \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$

Example. Find $\gcd(-243, 223)$.

$$243 = 223 \cdot 1 + 20 \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$
$$223 = 20 \cdot 11 + 3$$

Example. Find $\gcd(-243, 223)$.

$$243 = 223 \cdot 1 + 20 \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$
$$223 = 20 \cdot 11 + 3$$
$$20 = 3 \cdot 6 + 2$$

Example. Find $\gcd(-243, 223)$.

$$243 = 223 \cdot 1 + 20 \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$
$$223 = 20 \cdot 11 + 3$$
$$20 = 3 \cdot 6 + 2$$
$$3 = 2 \cdot 1 + 1$$

Example. Find $\gcd(-243, 223)$.

$$243 = 223 \cdot 1 + 20 \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$
$$223 = 20 \cdot 11 + 3$$
$$20 = 3 \cdot 6 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Example. Find $\gcd(-243, 223)$.

$$\begin{aligned} 243 &= 223 \cdot 1 + 20 \qquad (\gcd(a,b) = \gcd(|a|,|b|)) \\ 223 &= 20 \cdot 11 + 3 \\ 20 &= 3 \cdot 6 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

$\therefore \gcd(-243, 223) = 1.$

Example. Find $\gcd(-243, 223)$.

$$\begin{aligned} 243 &= 223 \cdot 1 + 20 \\ 223 &= 20 \cdot 11 + 3 \\ 20 &= 3 \cdot 6 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \qquad (\gcd(a, b) = \gcd(|a|, |b|))$$

$\therefore \gcd(-243, 223) = 1.$

Definition

*Ingeters a, b are called **coprime** if $\gcd(a, b) = 1$.*

Exercise. True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Exercise. True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Theorem (Bézout's Identity)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then $d = \gcd(a, b)$ exists, as do $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Exercise. True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Theorem (Bézout's Identity)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then $d = \gcd(a, b)$ exists, as do $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Corollary

If a and b are coprime, then there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

Exercise. True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Theorem (Bézout's Identity)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then $d = \gcd(a, b)$ exists, as do $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Corollary

If a and b are coprime, then there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

To fiind m, n, use the Euclidean algorithm in reverse.

Example. Find m, n such that $\gcd(330, 156) = 330m + 156n$.

Example. Find m, n such that $\gcd(330, 156) = 330m + 156n$.

$$330 = 156 \cdot 2 + 18 \tag{1}$$
$$156 = 18 \cdot 8 + 12 \tag{2}$$
$$18 = 12 \cdot 1 + 6 \tag{3}$$
$$12 = 6 \cdot 2 + 0 \Rightarrow \gcd(330, 156) = 6$$

Example. Find m, n such that $\gcd(330, 156) = 330m + 156n$.

$$330 = 156 \cdot 2 + 18 \tag{1}$$
$$156 = 18 \cdot 8 + 12 \tag{2}$$
$$18 = 12 \cdot 1 + 6 \tag{3}$$
$$12 = 6 \cdot 2 + 0 \Rightarrow \gcd(330, 156) = 6$$

Now starting with (3), isolate the GCD and use each previous line to substitute.

Example. Find m, n such that $\gcd(330, 156) = 330m + 156n$.

$$330 = 156 \cdot 2 + 18 \quad (1)$$
$$156 = 18 \cdot 8 + 12 \quad (2)$$
$$18 = 12 \cdot 1 + 6 \quad (3)$$
$$12 = 6 \cdot 2 + 0 \Rightarrow \gcd(330, 156) = 6$$

Now starting with (3), isolate the GCD and use each previous line to substitute.

(3) $18 = 12 \cdot 1 + 6 \Rightarrow 6 = 18 - 12$

(2) $12 = 156 - 18 \cdot 8 \Rightarrow 6 = 18 - (156 - 18 \cdot 8) = -156 + 18 \cdot 9$

(1) $18 = 330 - 156 \cdot 2 \Rightarrow 6 = -156 + (330 - 156 \cdot 2)9 = 330 \cdot 9 - 156 \cdot 19$

Example. Find m, n such that $\gcd(330, 156) = 330m + 156n$.

$$330 = 156 \cdot 2 + 18 \quad (1)$$
$$156 = 18 \cdot 8 + 12 \quad (2)$$
$$18 = 12 \cdot 1 + 6 \quad (3)$$
$$12 = 6 \cdot 2 + 0 \Rightarrow \gcd(330, 156) = 6$$

Now starting with (3), isolate the GCD and use each previous line to substitute.

(3) $18 = 12 \cdot 1 + 6 \Rightarrow 6 = 18 - 12$

(2) $12 = 156 - 18 \cdot 8 \Rightarrow 6 = 18 - (156 - 18 \cdot 8) = -156 + 18 \cdot 9$

(1) $18 = 330 - 156 \cdot 2 \Rightarrow 6 = -156 + (330 - 156 \cdot 2)9 = 330 \cdot 9 - 156 \cdot 19$

$\therefore m = 9, n = -19$

Example. Find m, n such that $243m + 223n = 1$.

Example. Find m, n such that $243m + 223n = 1$.

$$\begin{aligned} 243 &= 223 \cdot 1 + 20 \\ 223 &= 20 \cdot 11 + 3 \\ 20 &= 3 \cdot 6 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

Example. Find m, n such that $243m + 223n = 1$.

$$\begin{aligned} 243 &= 223 \cdot 1 + 20 \\ 223 &= 20 \cdot 11 + 3 \\ 20 &= 3 \cdot 6 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (20 - 3 \cdot 6) = -20 + 3 \cdot 7 \\ &= -20 + (223 - 20 \cdot 11)7 = 223 \cdot 7 - 20 \cdot 78 \\ &= 223 \cdot 7 - (243 - 223)78 = -243 \cdot 78 + 223 \cdot 85 \end{aligned}$$

Example. Find m, n such that $243m + 223n = 1$.

$$\begin{aligned} 243 &= 223 \cdot 1 + 20 \\ 223 &= 20 \cdot 11 + 3 \\ 20 &= 3 \cdot 6 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (20 - 3 \cdot 6) = -20 + 3 \cdot 7 \\ &= -20 + (223 - 20 \cdot 11)7 = 223 \cdot 7 - 20 \cdot 78 \\ &= 223 \cdot 7 - (243 - 223)78 = -243 \cdot 78 + 223 \cdot 85 \end{aligned}$$

$\therefore n = -78, n = 85$

The Pigeonhole Principle. Let $k, n \in \mathbb{N}, k < n$. If n pigeons fly into k pigeonholes, then some pigeonhole contains at least two pigeons.

The Pigeonhole Principle. Let $k, n \in \mathbb{N}, k < n$. If n pigeons fly into k pigeonholes, then some pigeonhole contains at least two pigeons.

Proof.

Suppose that each pigeonhole contains at most one pigeon. Then the total number of pigeons is at most $\sum_{i=1}^{k} 1 = k < n$, a contradiction. Therefore, there exists a pigeonhole that contains more than one pigeon. □

Example.

1. You have a drawer full of socks of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?

Example.

1. You have a drawer full of socks of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?

   4. The first 3 could possibly be all 3 different colours, but the fourth will match one of those (or else there's a previous pair).

Example.

1. You have a drawer full of socks of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?

   4. The first 3 could possibly be all 3 different colours, but the fourth will match one of those (or else there's a previous pair).

2. In a room of 367 people (allowing for a leap year), at least 2 of them share a birthday.

Example.

1. You have a drawer full of socks of 3 different colours. How many socks must you pick at random to be sure you have a matching pair?

   4. The first 3 could possibly be all 3 different colours, but the fourth will match one of those (or else there's a previous pair).

2. In a room of 367 people (allowing for a leap year), at least 2 of them share a birthday.
3. Humans have a maximum of about 500,000 hairs. Is it guaranteed that 2 residents of Wollongong have exactly the same number of hairs? How about 2 residents of Sydney?

Example. In a group of 700 people, must there be two whose first names have the same first and last letters?

Example. In a group of 700 people, must there be two whose first names have the same first and last letters?

Yes. At most 26 people can have different first letters and at most 26 people can have different last letters. So at most $26 \cdot 26 = 676$ people can have different either first or last letters.

Example. In a group of 700 people, must there be two whose first names have the same first and last letters?

Yes. At most 26 people can have different first letters and at most 26 people can have different last letters. So at most $26 \cdot 26 = 676$ people can have different either first or last letters.

Problems of this sort involve figuring out how to form the pigeonholes properly (how to partition the set).

Example. 5 different numbers are selected from the set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Show that two of the selected numbers sum to 9.

Example. 5 different numbers are selected from the set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Show that two of the selected numbers sum to 9.

Partition the set into pairs that sum to 9 (the pigeonholes):

$$S = \{1, 8\} \cup \{2, 7\} \cup \{3, 6\}, \cup \{4, 5\}.$$

Example. 5 different numbers are selected from the set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Show that two of the selected numbers sum to 9.

Partition the set into pairs that sum to 9 (the pigeonholes):

$$S = \{1, 8\} \cup \{2, 7\} \cup \{3, 6\}, \cup \{4, 5\}.$$

There are 4 subsets, so it's possible to select 4 numbers from S such that only one of them belongs to each subset. Choosing 5 numbers, by the pigeonhole principle, results in 2 chosen numbers belonging to the same subset.

Example. A restaurant serves 3 different salads, 6 different mains and 4 different desserts. How many people must eat there to ensure that at least 2 of them have the same meal?

Example. A restaurant serves 3 different salads, 6 different mains and 4 different desserts. How many people must eat there to ensure that at least 2 of them have the same meal?

There are $3 \cdot 6 \cdot 4 = 72$ different meals (this is combinatorics, more on this later), so there must be at least 73 people.

Generalised Pigeonhole Principle: If n pigeons fly into k pigeonholes and $n > km$ for some $m \in \mathbb{N}$, then some pigeonhole contains at least $m + 1$ pigeons.

Generalised Pigeonhole Principle: If n pigeons fly into k pigeonholes and $n > km$ for some $m \in \mathbb{N}$, then some pigeonhole contains at least $m + 1$ pigeons.

Example. Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.

Generalised Pigeonhole Principle: If n pigeons fly into k pigeonholes and $n > km$ for some $m \in \mathbb{N}$, then some pigeonhole contains at least $m + 1$ pigeons.

Example. Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.

85 pigeons (people), 26 pigeonholes (letters in the alphabet), $85 = 26 \cdot 3 + 7$. So $85 > 26 \cdot 3$ and some pigeonhole contains at least $m + 1 = 4$ pigeons.

Generalised Pigeonhole Principle: If n pigeons fly into k pigeonholes and $n > km$ for some $m \in \mathbb{N}$, then some pigeonhole contains at least $m + 1$ pigeons.

Example. Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.

85 pigeons (people), 26 pigeonholes (letters in the alphabet), $85 = 26 \cdot 3 + 7$. So $85 > 26 \cdot 3$ and some pigeonhole contains at least $m + 1 = 4$ pigeons.

Exercise. Find the minimum number of students needed in a class to be sure 3 of them were born in the same month.

Example. We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

Example. We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

Assume only 2 classes have 5 or more people and show a contradiction.

Example. We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

Assume only 2 classes have 5 or more people and show a contradiction.

The best case is that those 2 classes are full (leaving the fewest possible people for the other classes), 15 students each. Then 40 people remain, for 9 classes.

Example. We want to assign 70 students to 11 classes so that no class has more than 15 people. Show that there must be at least 3 classes with 5 or more people.

Assume only 2 classes have 5 or more people and show a contradiction.

The best case is that those 2 classes are full (leaving the fewest possible people for the other classes), 15 students each. Then 40 people remain, for 9 classes. Since $40 = 9 \cdot 4 + 4$, we have $m = 4$ and we know that at least 1 of the 9 classes has 5 or more people in it.

Chapter 3:

Modular Arithmetic

Modular Arithmetic

Definition

Let $n \in \mathbb{N}, a \in \mathbb{Z}$. We define by $a \pmod{n}$ the remainder when a is divided by n.

Modular Arithmetic

Definition

Let $n \in \mathbb{N}, a \in \mathbb{Z}$. We define by $a \pmod{n}$ the remainder when a is divided by n.

Example.

$$14 \pmod{4} = 2 \qquad \text{(since } \tfrac{14}{4} = 3 \text{ with remainder 2)}$$

Modular Arithmetic

Definition

Let $n \in \mathbb{N}, a \in \mathbb{Z}$. We define by $a \pmod{n}$ the remainder when a is divided by n.

Example.

$$14 \pmod{4} = 2 \qquad \text{(since } \tfrac{14}{4} = 3 \text{ with remainder 2)}$$

$$18 \pmod{3} = 0$$

Modular Arithmetic

Definition

Let $n \in \mathbb{N}, a \in \mathbb{Z}$. We define by $a \pmod{n}$ the remainder when a is divided by n.

Example.

$$14 \pmod 4 = 2 \qquad \text{(since } \tfrac{14}{4} = 3 \text{ with remainder 2)}$$
$$18 \pmod 3 = 0$$
$$-8 \pmod 6 = 4$$

Modular Arithmetic

Definition

Let $n \in \mathbb{N}, a \in \mathbb{Z}$. We define by $a \pmod{n}$ the remainder when a is divided by n.

Example.

$$14 \pmod 4 = 2 \qquad \text{(since } \tfrac{14}{4} = 3 \text{ with remainder 2)}$$
$$18 \pmod 3 = 0$$
$$-8 \pmod 6 = 4$$
$$10 \pmod 1 = 0$$

Definition

*a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a-b)$. Equivalently, $a \equiv b \pmod{n}$ iff*

$$a \pmod{n} = b \pmod{n}.$$

Definition

*a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a-b)$. Equivalently, $a \equiv b \pmod{n}$ iff*

$$a \pmod{n} = b \pmod{n}.$$

Example. True or false?
(a) $154 \equiv 56 \pmod{11}$
(b) $7 \equiv -9 \pmod{8}$

Definition

*a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a-b)$. Equivalently, $a \equiv b \pmod{n}$ iff*

$$a \pmod{n} = b \pmod{n}.$$

Example. True or false?
(a) $154 \equiv 56 \pmod{11}$
(b) $7 \equiv -9 \pmod{8}$

(a) $11|(154-56) \Leftrightarrow 11|98$. False.

Definition

*a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a-b)$. Equivalently, $a \equiv b \pmod{n}$ iff*

$$a \pmod{n} = b \pmod{n}.$$

Example. True or false?
(a) $154 \equiv 56 \pmod{11}$
(b) $7 \equiv -9 \pmod{8}$

(a) $11|(154-56) \Leftrightarrow 11|98$. False.
(b) $8|(7-(-9)) \Leftrightarrow 8|16$. True.

Example. Find x such that $12 \equiv x \pmod{5}$.

Example. Find x such that $12 \equiv x \pmod 5$.

We need $5|(12 - x)$, so $x \in \{\ldots, -8, -3, 2, 7, 12, \ldots\}$.

Example. Find x such that $12 \equiv x \pmod 5$.

We need $5|(12 - x)$, so $x \in \{\ldots, -8, -3, 2, 7, 12, \ldots\}$.

Example. If $m \equiv 0 \pmod 2$, what can be said about m?

Example. Find x such that $12 \equiv x \pmod 5$.

We need $5|(12 - x)$, so $x \in \{\ldots, -8, -3, 2, 7, 12, \ldots\}$.

Example. If $m \equiv 0 \pmod 2$, what can be said about m?

m is an even number.

Theorem (Congruence Arithmetic)

Let $n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$. *If* $a \equiv c \pmod{n}$ *and* $b \equiv d \pmod{n}$, *then*

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n} \; \forall \; m \in \mathbb{N}$

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

(1) $a + b = (np + c) + (nq + d) = n(p + q) + c + d$

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

(1) $a + b = (np + c) + (nq + d) = n(p + q) + c + d$
$(a + b) \pmod{n} \equiv [n(p + q) + c + d] \pmod{n} \equiv (c + d) \pmod{n}$

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

(1) $a + b = (np + c) + (nq + d) = n(p + q) + c + d$
$(a + b) \pmod{n} \equiv [n(p + q) + c + d] \pmod{n} \equiv (c + d) \pmod{n}$

(2) Similarly, $(a - b) \pmod{n} \equiv (c - d) \pmod{n}$

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

(1) $a + b = (np + c) + (nq + d) = n(p + q) + c + d$
$(a + b) \pmod{n} \equiv [n(p + q) + c + d] \pmod{n} \equiv (c + d) \pmod{n}$

(2) Similarly, $(a - b) \pmod{n} \equiv (c - d) \pmod{n}$

(3) $ab = (np + c)(nq + d) = n^2pq + npd + nqc + cd$
$= n(npq + pd + qc) + cd$

Proof.

We have $a - c = np$ and $b - d = nq$ for some $p, q \in \mathbb{Z}$.

(1) $a + b = (np + c) + (nq + d) = n(p + q) + c + d$
$(a + b) \pmod{n} \equiv [n(p + q) + c + d] \pmod{n} \equiv (c + d) \pmod{n}$

(2) Similarly, $(a - b) \pmod{n} \equiv (c - d) \pmod{n}$

(3) $ab = (np + c)(nq + d) = n^2pq + npd + nqc + cd$
$= n(npq + pd + qc) + cd$

$ab \pmod{n} \equiv cd \pmod{n}$ □

Proof.

(4) Induction.

(a) $m = 1$: $a^1 \equiv c^1 \pmod{n}$ TRUE

Proof.

(4) Induction.

(a) $m = 1$: $a^1 \equiv c^1 \pmod{n}$ TRUE

(b) Suppose $a^k \equiv c^k \pmod{n}$ and prove $a^{k+1} \equiv c^{k+1} \pmod{n}$.

Proof.

(4) Induction.

(a) $m = 1$: $a^1 \equiv c^1 \pmod{n}$ TRUE

(b) Suppose $a^k \equiv c^k \pmod{n}$ and prove $a^{k+1} \equiv c^{k+1} \pmod{n}$.

$a^{k+1} = a^k \cdot a$ and $c^{k+1} = c^k \cdot c$, so by (3), $a^k \cdot a \equiv c^k \cdot c \pmod{n}$.

Proof.

(4) Induction.

(a) $m = 1$: $a^1 \equiv c^1 \pmod{n}$ TRUE

(b) Suppose $a^k \equiv c^k \pmod{n}$ and prove $a^{k+1} \equiv c^{k+1} \pmod{n}$.

$a^{k+1} = a^k \cdot a$ and $c^{k+1} = c^k \cdot c$, so by (3), $a^k \cdot a \equiv c^k \cdot c \pmod{n}$.

$\Rightarrow a^{k+1} \equiv c^{k+1} \pmod{n}$

Proof.

(4) Induction.

(a) $m = 1$: $a^1 \equiv c^1 \pmod{n}$ TRUE

(b) Suppose $a^k \equiv c^k \pmod{n}$ and prove $a^{k+1} \equiv c^{k+1} \pmod{n}$.

$a^{k+1} = a^k \cdot a$ and $c^{k+1} = c^k \cdot c$, so by (3), $a^k \cdot a \equiv c^k \cdot c \pmod{n}$.

$\Rightarrow a^{k+1} \equiv c^{k+1} \pmod{n}$

$\therefore a^m \equiv c^m \pmod{n} \; \forall \; m \in \mathbb{N}$ □

Example.

1. Given $2064 = 1715 + 349$, find $2064 \pmod{17}$.
2. Given $713064 = 803 \cdot 888$, find $713064 \pmod{8}$.
3. Find x such that $3^9 \equiv x \pmod{5}$.

Example.

1. Given $2064 = 1715 + 349$, find $2064 \pmod{17}$.
2. Given $713064 = 803 \cdot 888$, find $713064 \pmod{8}$.
3. Find x such that $3^9 \equiv x \pmod{5}$.

(1)$1715 \equiv 15 \pmod{17}$ and $349 \equiv 9 \pmod{17}$
$\Rightarrow 2064 = (1715 + 349) \equiv (15 + 9) \pmod{17} = 7 \pmod{17}$

(2) $803 \equiv 3 \pmod 8$ and $888 \equiv 0 \pmod 8$
$\Rightarrow 803 \cdot 888 \equiv 3 \cdot 0 \pmod 8 \equiv 0 \pmod 8$

(2) $803 \equiv 3 \pmod 8$ and $888 \equiv 0 \pmod 8$
$\Rightarrow 803 \cdot 888 \equiv 3 \cdot 0 \pmod 8 \equiv 0 \pmod 8$

(3) $3^9 = 3^4 \cdot 3^4 \cdot 3 = 81 \cdot 81 \cdot 3$ and $81 \equiv 1 \pmod 5$
$\Rightarrow 3^9 \equiv 1 \cdot 1 \cdot 3 \pmod 5 \equiv 3 \pmod 5$

(2) $803 \equiv 3 \pmod 8$ and $888 \equiv 0 \pmod 8$
$\Rightarrow 803 \cdot 888 \equiv 3 \cdot 0 \pmod 8 \equiv 0 \pmod 8$

(3) $3^9 = 3^4 \cdot 3^4 \cdot 3 = 81 \cdot 81 \cdot 3$ and $81 \equiv 1 \pmod 5$
$\Rightarrow 3^9 \equiv 1 \cdot 1 \cdot 3 \pmod 5 \equiv 3 \pmod 5$

Exercise. Find the remainder when 7^6 is divided by 16.

Theorem (Cancellation Law)

Let $n, a, b, c \in \mathbb{Z}$. *If* $\gcd(a, n) = 1$ *and* $ab \equiv ac \pmod{n}$, *then* $b \equiv c \pmod{n}$.

Theorem (Cancellation Law)

Let $n, a, b, c \in \mathbb{Z}$. If $\gcd(a, n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Example. Let $n = 5, a = 6, b = 8, c = 13$. Then $\gcd(a, n) = 1$ and $ab = 48 \equiv 3 \pmod{5} \equiv 78 = ac$.
$\Rightarrow 8 \equiv 13 \pmod{5}$ (Verify that both equal $3 \pmod{5}$.)

Theorem (Cancellation Law)

Let $n, a, b, c \in \mathbb{Z}$. If $\gcd(a, n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Example. Let $n = 5, a = 6, b = 8, c = 13$. Then $\gcd(a, n) = 1$ and $ab = 48 \equiv 3 \pmod{5} \equiv 78 = ac$.
$\Rightarrow 8 \equiv 13 \pmod{5}$ (Verify that both equal $3 \pmod{5}$.)

Example. Let $n = 4, a = 6, b = 8, c = 10$. Then $ab = 48 \equiv 0 \pmod{4} \equiv 60 = ac$, but $b \not\equiv c \pmod{4}$. This is because $\gcd(4, 6) \neq 1$.

Proof.

$$ab \equiv ac \pmod{n}$$
$$\Rightarrow (ab - ac) \equiv 0 \pmod{n}$$
$$a(b-c) \equiv 0 \pmod{n} \Rightarrow a(b-c) = kn \text{ for some } k \in \mathbb{Z}$$

But a and n are coprime, so the multiple of n on the LHS must be $(b - c)$.

Proof.

$$ab \equiv ac \pmod{n}$$
$$\Rightarrow (ab - ac) \equiv 0 \pmod{n}$$
$$a(b-c) \equiv 0 \pmod{n} \Rightarrow a(b-c) = kn \text{ for some } k \in \mathbb{Z}$$

But a and n are coprime, so the multiple of n on the LHS must be $(b - c)$. Hence,

$$(b-c) \equiv 0 \pmod{n}$$
$$b \equiv c \pmod{n}$$

Example. Given $10904 \equiv 32 \pmod{9}$, find the smallest $x \in \mathbb{N}$ such that $x \equiv 1363 \pmod{9}$.

Example. Given $10904 \equiv 32 \pmod 9$, find the smallest $x \in \mathbb{N}$ such that $x \equiv 1363 \pmod 9$.

Note that $10904 = 1363 \cdot 8$.

$$
\begin{aligned}
1363 \cdot 8 &\equiv 4 \cdot 8 \pmod 9 \\
1363 &\equiv 4 \pmod 9 && \text{(since 8 and 9 are coprime)} \\
x &= 4
\end{aligned}
$$

Congruence Classes

The quotient-remainder theorem gives us the following.

Fact

Let $n \in \mathbb{Z}$. Every $x \in \mathbb{Z}$ is congruent modulo n to exactly one element in $\{0, 1, 2, \ldots, n-1\}$.

Congruence Classes

The quotient-remainder theorem gives us the following.

Fact

Let $n \in \mathbb{Z}$. Every $x \in \mathbb{Z}$ is congruent modulo n to exactly one element in $\{0, 1, 2, \ldots, n-1\}$.

This allows us to group integers according to their remainders after dividing by n.

Definition

*Let $n \in \mathbb{N}$. The **congruence class (residue)** of $a \in \mathbb{Z}$ modulo n is the set $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$.*

Example. Write the congruence classes for $n = 4$. How many of them are there?

Example. Write the congruence classes for $n = 4$. How many of them are there?

Theorem

Let $n \in \mathbb{N}$. There are exactly n distinct congruence classes modulo n;

$$[0], [1], \ldots, [n-1]$$

Proof.

Let $0 \leq a < b < n$, $a, b \in \mathbb{N}$. Then $b - a \in \mathbb{N}$ and $b - a < n$. Thus, $n \not| (b - a)$, so $b \not\equiv a \pmod{n}$. No two of $0, 1, \ldots, n-1$ are congruent and we have that $[0], [1], \ldots, [n-1]$ are all distinct residues. Let $x \in \mathbb{Z}$. By QRT, $x = nq + r, 0 \leq r < n$.

Proof.

Let $0 \leq a < b < n$, $a, b \in \mathbb{N}$. Then $b - a \in \mathbb{N}$ and $b - a < n$. Thus, $n \not| (b - a)$, so $b \not\equiv a \pmod{n}$. No two of $0, 1, \ldots, n-1$ are congruent and we have that $[0], [1], \ldots, [n-1]$ are all distinct residues. Let $x \in \mathbb{Z}$. By QRT, $x = nq + r, 0 \leq r < n$. So $r \in \{0, 1, \ldots, n-1\}$ and $x - r = nq \Rightarrow x \equiv r \pmod{n}$.

Proof.

Let $0 \leq a < b < n$, $a, b \in \mathbb{N}$. Then $b - a \in \mathbb{N}$ and $b - a < n$. Thus, $n \not| (b - a)$, so $b \not\equiv a \pmod{n}$. No two of $0, 1, \ldots, n-1$ are congruent and we have that $[0], [1], \ldots, [n-1]$ are all distinct residues. Let $x \in \mathbb{Z}$. By QRT, $x = nq + r, 0 \leq r < n$. So $r \in \{0, 1, \ldots, n-1\}$ and $x - r = nq \Rightarrow x \equiv r \pmod{n}$.

Therefore, every $x \in \mathbb{Z}$ is in one class. □

Definition

Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Definition

Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Definition

Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Example. $\mathbb{Z}_3 = \{[0], [1], [2]\}$, so in $\mathbb{Z}_3$ we have

$$[4] = [1]; [-1] = [2]; [30] = [0], \text{etc.}$$

Definition

Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Example. $\mathbb{Z}_3 = \{[0], [1], [2]\}$, so in $\mathbb{Z}_3$ we have

$$[4] = [1]; [-1] = [2]; [30] = [0], \text{etc.}$$

Example. In $\mathbb{Z}_n$,

$$[0] \cup [1] \cup \cdots \cup [n-1] = ?$$
$$[0] \cap [1] \cap \cdots \cap [n-1] = ?$$

Operations on $\mathbb{Z}_n$

We want to define addition and multiplication on $\mathbb{Z}_n$. Since different numbers can give the same residues, we must be careful with the definitions.

Operations on $\mathbb{Z}_n$

We want to define addition and multiplication on $\mathbb{Z}_n$. Since different numbers can give the same residues, we must be careful with the definitions.

Theorem

Let $n \in \mathbb{N}$. The operation $+$

$$[a] + [b] = [a + b]$$

is well-defined addition on $\mathbb{Z}_n$. That is, if $[a] = [c]$ and $[b] = [d]$, then $[a + b] = [c + d]$.

Operations on $\mathbb{Z}_n$

We want to define addition and multiplication on $\mathbb{Z}_n$. Since different numbers can give the same residues, we must be careful with the definitions.

Theorem

Let $n \in \mathbb{N}$. The operation $+$

$$[a] + [b] = [a + b]$$

is well-defined addition on $\mathbb{Z}_n$. That is, if $[a] = [c]$ and $[b] = [d]$, then $[a + b] = [c + d]$. Similarly, the operation $\cdot$

$$[a] \cdot [b] = [ab]$$

is well-defined multiplication on $\mathbb{Z}_n$. That is, if $[a] = [c]$ and $[b] = [d]$, then $[ab] = [cd]$.

Proof.

$$[a] = [c] \Rightarrow a \equiv c \pmod{n} \Rightarrow \exists\, k_1 \in \mathbb{Z} \text{ s.t. } a = c + k_1 n$$
$$[b] = [d] \Rightarrow b \equiv d \pmod{n} \Rightarrow \exists\, k_2 \in \mathbb{Z} \text{ s.t. } b = d + k_2 n$$
$$a + b = (c + k_1 n) + (d + k_2 n) = c + d + n(k_1 + k_2)$$
$$\Rightarrow (a + b) \equiv (c + d) \pmod{n} \Rightarrow [a + b] = [c + d]$$

Proof.

$$[a] = [c] \Rightarrow a \equiv c \pmod{n} \Rightarrow \exists\, k_1 \in \mathbb{Z} \text{ s.t. } a = c + k_1 n$$
$$[b] = [d] \Rightarrow b \equiv d \pmod{n} \Rightarrow \exists\, k_2 \in \mathbb{Z} \text{ s.t. } b = d + k_2 n$$
$$a + b = (c + k_1 n) + (d + k_2 n) = c + d + n(k_1 + k_2)$$
$$\Rightarrow (a + b) \equiv (c + d) \pmod{n} \Rightarrow [a + b] = [c + d]$$
$$ab = (c + k_1 n)(d + k_2 n) = cd + n(k_2 c + k_1 d + n k_1 k_2)$$
$$\Rightarrow ab \equiv cd \pmod{n} \Rightarrow [ab] = [cd]$$

Example. Write addition and multiplication tables for $\mathbb{Z}_3$.

$+$	[0]	[1]	[2]
[0]			
[1]			
[2]			

$\cdot$	[0]	[1]	[2]
[0]			
[1]			
[2]			

Properties of $\mathbb{Z}_n$

1. $+$ and $\cdot$ are closed binary operators
2. $+$ and $\cdot$ are commutative and associative
3. $\cdot$ is distributive over $+$
4. Identities are [0] under $+$, [1] under $\cdot$
5. Additive inverse of $[x]$ is $[n - x]$
6. Multiplicative inverses exist only for $\gcd(x, n) = 1$

Theorem

If a and n are coprime, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$. We call b the multiplicative inverse of a modulo n; it is unique and we write

$$b = a^{-1} \pmod{n}.$$

Proof.

Consider the set $\{0, a, 2a, 3a, \ldots, (n-1)a\}$. If we can show that these are all distinct modulo n, then exactly one of them is equivalent to 1 $\pmod{n}$.

Proof.

Consider the set $\{0, a, 2a, 3a, \ldots, (n-1)a\}$. If we can show that these are all distinct modulo n, then exactly one of them is equivalent to 1 $(\text{mod } n)$.

Suppose the contrary:
$\exists\, c, d \in \mathbb{N} \cup \{0\}, c, d < n, c \neq d \text{ s.t. } ca \equiv da \pmod{n}$.

Proof.

Consider the set $\{0, a, 2a, 3a, \ldots, (n-1)a\}$. If we can show that these are all distinct modulo n, then exactly one of them is equivalent to 1 $(\text{mod } n)$.

Suppose the contrary:
$\exists\, c, d \in \mathbb{N} \cup \{0\}, c, d < n, c \neq d$ s.t. $ca \equiv da \pmod{n}$. Then $(c-d)a \equiv 0 \pmod{n}$, so $\exists\, k \in \mathbb{Z}$ s.t. $(c-d)a = kn$.

Proof.

Consider the set $\{0, a, 2a, 3a, \ldots, (n-1)a\}$. If we can show that these are all distinct modulo n, then exactly one of them is equivalent to 1 $\pmod{n}$.

Suppose the contrary:
$\exists\ c, d \in \mathbb{N} \cup \{0\}, c, d < n, c \neq d$ s.t. $ca \equiv da \pmod{n}$. Then $(c-d)a \equiv 0 \pmod{n}$, so $\exists\ k \in \mathbb{Z}$ s.t. $(c-d)a = kn$. But a and n are coprime, so $n|(c-d)$. This is a contradiction, since c and d are distinct nonnegative integers less than n. $\square$

Example. Find the multiplicative inverse of 43 modulo 60.

Example. Find the multiplicative inverse of 43 modulo 60.

We need $x \in \mathbb{N}$ such that $43x \equiv 1 \pmod{60}$. Notice that $43x$ must have last digit 1, since 60 is a multiple of 10.

Example. Find the multiplicative inverse of 43 modulo 60.

We need $x \in \mathbb{N}$ such that $43x \equiv 1 \pmod{60}$. Notice that $43x$ must have last digit 1, since 60 is a multiple of 10. Any x such that $43x$ ends in 1 has last digit 7. The possibilities are $7, 17, 27, 37, 47, 57$.

Example. Find the multiplicative inverse of 43 modulo 60.

We need $x \in \mathbb{N}$ such that $43x \equiv 1 \pmod{60}$. Notice that $43x$ must have last digit 1, since 60 is a multiple of 10. Any x such that $43x$ ends in 1 has last digit 7. The possibilities are $7, 17, 27, 37, 47, 57$.

$$43 \cdot 7 = 301 \equiv 1 \pmod{60}$$

$$\therefore\ 43^{-1} \pmod{60} = 7$$

Example. Find $3^{-1} \pmod{40}$

Example. Find $3^{-1} \pmod{40}$

By the same reasoning as above, the possibilities are $7, 17, 27, 37$.

Example. Find $3^{-1} \pmod{40}$

By the same reasoning as above, the possibilities are $7, 17, 27, 37$.

$$\begin{aligned} 3 \cdot 7 &= 21 \equiv 21 \pmod{40} \\ 3 \cdot 17 &= 51 \equiv 11 \pmod{40} \\ 3 \cdot 27 &= 81 \equiv 1 \pmod{40} \end{aligned}$$

$$\therefore 3^{-1} \pmod{40} = 27$$

Application: cryptography

Cryptography is the study of methods for sending secret messages. There are many techniques for encryption and decryption, one of which is *public key cryptography*. The method uses big prime numbers and modular arithmetic.

Application: cryptography

Cryptography is the study of methods for sending secret messages. There are many techniques for encryption and decryption, one of which is *public key cryptography*. The method uses big prime numbers and modular arithmetic.

RSA Public Key

1. Choose 2 large primes p and q.
2. Choose $e \in \mathbb{Z}$ that is coprime with $(p-1)(q-1)$.
3. Find $d \in \mathbb{Z}$ s.t. $ed \equiv 1 \pmod{(p-1)(q-1)}$.
4. The public key is (e, pq). This is available to everyone for encryption.
5. The private key is (d, pq). This is available only to those who the sender wants to be able to decrypt.

Encryption step. Let the message to be encrypted be $M \in \mathbb{Z}$, $0 \leq M < pq$ (a computer uses binary code for everything, so encrypting integers is sufficient). The encrypted message is

$$C = M^e \pmod{pq}$$

Encryption step. Let the message to be encrypted be $M \in \mathbb{Z}$, $0 \leq M < pq$ (a computer uses binary code for everything, so encrypting integers is sufficient). The encrypted message is

$$C = M^e \pmod{pq}$$

Decryption step. M is recovered by

$$M = C^d \pmod{pq}$$

Encryption step. Let the message to be encrypted be $M \in \mathbb{Z}$, $0 \leq M < pq$ (a computer uses binary code for everything, so encrypting integers is sufficient). The encrypted message is

$$C = M^e \pmod{pq}$$

Decryption step. M is recovered by

$$M = C^d \pmod{pq}$$

p and q are several hundred digits long each, making it impossible for a computer to find the factors $(p-1)(q-1)$ in reasonable time.

Example. Let $A = 1, B = 2, \cdots, Z = 26$, public key $(3, 55)$. Encrypt and decrypt the message “HEY”.

Example. Let $A = 1, B = 2, \cdots, Z = 26$, public key $(3, 55)$. Encrypt and decrypt the message "HEY".

$pq = 55 \Rightarrow p = 5, q = 11$. I choose $e = 3$, which is coprime with $(5 - 1)(11 - 1) = 40$. The unencrypted message is 8 5 25.

Example. Let $A = 1, B = 2, \cdots, Z = 26$, public key $(3, 55)$. Encrypt and decrypt the message "HEY".

$pq = 55 \Rightarrow p = 5, q = 11$. I choose $e = 3$, which is coprime with $(5-1)(11-1) = 40$. The unencrypted message is 8 5 25.

$$8^3 = 64 \cdot 8 \equiv 9 \cdot 8 \pmod{55} = 72 \pmod{55} = 17$$

$$5^3 = 125 \equiv 15$$

$$25^3 = 125 \cdot 125 \equiv 15 \cdot 15 \pmod{55} = 5$$

The encrypted message is 17 15 5.

From a previous example, $3^{-1} \pmod{40} = 27$.

From a previous example, $3^{-1} \pmod{40} = 27$.

$$17^{27} = 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^{6} \cdot 14 \cdot 17$$

From a previous example, $3^{-1} \pmod{40} = 27$.

$$\begin{aligned} 17^{27} &= 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^{6} \cdot 14 \cdot 17 \\ &= 196^{6} \cdot 238 \equiv 31^{6} \cdot 18 \pmod{55} = 961^{3} \cdot 18 \end{aligned}$$

From a previous example, $3^{-1} \pmod{40} = 27$.

$$\begin{aligned} 17^{27} &= 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^{6} \cdot 14 \cdot 17 \\ &= 196^{6} \cdot 238 \equiv 31^{6} \cdot 18 \pmod{55} = 961^{3} \cdot 18 \\ &\equiv 26^{3} \cdot 18 \pmod{55} = 676 \cdot 468 \equiv 16 \cdot 28 \pmod{55} \end{aligned}$$

From a previous example, $3^{-1} \pmod{40} = 27$.

$$\begin{aligned} 17^{27} &= 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^6 \cdot 14 \cdot 17 \\ &= 196^6 \cdot 238 \equiv 31^6 \cdot 18 \pmod{55} = 961^3 \cdot 18 \\ &\equiv 26^3 \cdot 18 \pmod{55} = 676 \cdot 468 \equiv 16 \cdot 28 \pmod{55} \\ &= 448 \equiv 8 \pmod{55} \end{aligned}$$

From a previous example, $3^{-1} \pmod{40} = 27$.

$$\begin{aligned} 17^{27} &= 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^6 \cdot 14 \cdot 17 \\ &= 196^6 \cdot 238 \equiv 31^6 \cdot 18 \pmod{55} = 961^3 \cdot 18 \\ &\equiv 26^3 \cdot 18 \pmod{55} = 676 \cdot 468 \equiv 16 \cdot 28 \pmod{55} \\ &= 448 \equiv 8 \pmod{55} \end{aligned}$$

So the decrypted 17 is 8, the original “H”. Similarly, $15 \to 5$ and $5 \to 25$.

From a previous example, $3^{-1} \pmod{40} = 27$.

$$\begin{aligned} 17^{27} &= 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^6 \cdot 14 \cdot 17 \\ &= 196^6 \cdot 238 \equiv 31^6 \cdot 18 \pmod{55} = 961^3 \cdot 18 \\ &\equiv 26^3 \cdot 18 \pmod{55} = 676 \cdot 468 \equiv 16 \cdot 28 \pmod{55} \\ &= 448 \equiv 8 \pmod{55} \end{aligned}$$

So the decrypted 17 is 8, the original "H". Similarly, $15 \to 5$ and $5 \to 25$.

Exercise. Decrypt the message 76 70 14 with public key $(11, 91)$.

Chapter 4:

Set Theory

A “set” is a loosely-defined collection of items called *elements*. Sets are completely determined by their elements, i.e. two sets with exactly the same elements are the same set. The order in which elements are listed is irrelevant, as are repeated elements.

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

A “set” is a loosely-defined collection of items called *elements*. Sets are completely determined by their elements, i.e. two sets with exactly the same elements are the same set. The order in which elements are listed is irrelevant, as are repeated elements.

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

The collection of all people in this room is a set.

The collection of your favourite songs is a set.

The collection of all real numbers is a set.

Sets come from a *universe* of elements U. For example, the set of even numbers comes from the universe $\mathbb{Z}$. Sets can be contained in other sets and can be finite or infinite.

$$\{1, 2, 3\}; \{\text{Susan, Robert}\}; \{0, \{0\}, 1, \{0, 1\}\}; \{2, 4, 6, \ldots\}$$

Sets come from a *universe* of elements U. For example, the set of even numbers comes from the universe $\mathbb{Z}$. Sets can be contained in other sets and can be finite or infinite.

$$\{1,2,3\}; \{\text{Susan, Robert}\}; \{0,\{0\},1,\{0,1\}\}; \{2,4,6,\ldots\}$$

Some important sets of numbers are

$$\mathbb{N} = \{1,2,3,\ldots\} \qquad \text{(natural)}$$
$$\mathbb{Z} = \{\ldots,-2,-1,0,1,1,\ldots\} \qquad \text{(integer)}$$
$$\mathbb{Q} = \left\{\frac{a}{b} : a,b \in \mathbb{Z}, b \neq 0\right\} \qquad \text{(rational)}$$
$$\mathbb{R} = \text{real numbers} \qquad \text{(rational and irrational)}$$

A set can be defined by a property of elements of a bigger set. Given a set S, define a set T by

$$T = \{x \in S : p(x)\},$$

all the elements of S that satisfy p.

A set can be defined by a property of elements of a bigger set. Given a set S, define a set T by

$$T = \{x \in S : p(x)\},$$

all the elements of S that satisfy p.

Example. The set $\{x \in \mathbb{R} : -2 < x \leq 5\}$ is the set of all real numbers between -2 and 5, not including -2. It is an *interval*, which can also be denoted $(-2, 5]$.

A set can be defined by a property of elements of a bigger set. Given a set S, define a set T by

$$T = \{x \in S : p(x)\},$$

all the elements of S that satisfy p.

Example. The set $\{x \in \mathbb{R} : -2 < x \leq 5\}$ is the set of all real numbers between -2 and 5, not including -2. It is an *interval*, which can also be denoted $(-2, 5]$.

Example. The set $\{x \in \mathbb{Z} : -2 < x \leq 5\}$ can be rewritten how?

A set can be defined by a property of elements of a bigger set. Given a set S, define a set T by

$$T = \{x \in S : p(x)\},$$

all the elements of S that satisfy p.

Example. The set $\{x \in \mathbb{R} : -2 < x \leq 5\}$ is the set of all real numbers between -2 and 5, not including -2. It is an *interval*, which can also be denoted $(-2, 5]$.

Example. The set $\{x \in \mathbb{Z} : -2 < x \leq 5\}$ can be rewritten how?

Example. The set $\{x \in \mathbb{R} : x^3 = x\}$ can be rewritten how?

The *empty set* $\varnothing$ is the set with no elements in it. It can be written in different ways:

$$\{x \in \mathbb{N} : x \neq x\}; \{x \in \mathbb{R} : 3 < x < 2\}$$

The *empty set* $\varnothing$ is the set with no elements in it. It can be written in different ways:

$$\{x \in \mathbb{N} : x \neq x\}; \{x \in \mathbb{R} : 3 < x < 2\}$$

A set is *finite* if $\exists\ n \in \mathbb{N}$ such that there is a one-to-one correspondence with the set $\{1, 2, \ldots, n\}$. For a set S of this size, we write $|S| = n$ and say that S has *cardinality* n. Note that $|\varnothing| = 0$. A set that is not finite is said to be *infinite*.

Definition

*Let A and B be sets. We say A is a **subset** of B, written $A \subseteq B$, iff every element of A is also an element of B.*

$$A \subseteq B \Leftrightarrow \forall\, x \in U, x \in A \Rightarrow x \in B$$

*Then B is called a **superset** of A.*

We also say that A is contained in B and that B contains A. If at least one element of A is not in B, then A is not a subset of B.

$$A \not\subseteq B \Leftrightarrow \exists\, x \in U \text{ s.t. } x \in A \wedge x \notin B$$

Example. Decide true or false.

1. $\{1,2\} \subseteq \{1,2,3\}$
2. $\{0,2\} \subseteq \{1,2,3\}$
3. $-1 \in \{x \in \mathbb{N} : x^2 = 1\}$
4. $\{1\} \in \{x \in \mathbb{N} : x^2 = 1\}$
5. $A \subseteq A$ for all sets A
6. $\varnothing \subseteq A$ for all sets A

Definition

*A subset $a \subseteq B$ is **proper** if $\exists\ x \in B$ $\texttt{s.t.}$ $x \notin A$. We can (but don't have to) write $A \subset B$ or $A \subsetneq B$.*

For example, $\{1\} \subseteq \{1,2\}$ and $\{1,2\} \subseteq \{1,2\}$, but $2 \in \{1,2\}$ and $2 \notin \{1\}$, so $\{1\} \subset \{1,2\}$ ($\{1\}$ is a proper subset of $\{1,2\}$).

Definition

*A subset $a \subseteq B$ is **proper** if $\exists\ x \in B$ $\mathtt{s.t.}$ $x \notin A$. We can (but don't have to) write $A \subset B$ or $A \subsetneq B$.*

For example, $\{1\} \subseteq \{1,2\}$ and $\{1,2\} \subseteq \{1,2\}$, but $2 \in \{1,2\}$ and $2 \notin \{1\}$, so $\{1\} \subset \{1,2\}$ ($\{1\}$ is a proper subset of $\{1,2\}$).

Example. Order the sets $\mathbb{R}, \mathbb{N}, \mathbb{Q}$ and $\mathbb{Z}$ in terms of subsets. Are any of them proper subsets?

Example. Let $A = \{1, 2, 3\}$. Decide true or false.

(a) $a \subset A$
(b) $\varnothing \in A$
(c) $\varnothing \subseteq A$
(d) $\{\varnothing\} \subseteq A$
(e) $2 \in A$
(f) $\{2\} \in A$
(g) $2 \subseteq A$
(h) $\{2\} \subseteq A$
(i) $\{2\} \subseteq \{\{1\}, \{2\}\}$
(j) $\{2\} \in \{\{1\}, \{2\}\}$

Definition

*Let A and B be sets. We say that A **equals** B, written $A = B$, iff A contains B and B contains A.*

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

To prove that two sets are equal, prove both contentions.

Example. Prove that $A = \{n \in \mathbb{N} : n \text{ is even}\}$ and $B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$ are equal.

Proof.

($\subseteq$) Let $n \in A$. Then $n = 2k$ for some $k \in \mathbb{N}$.

Example. Prove that $A = \{n \in \mathbb{N} : n \text{ is even}\}$ and $B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$ are equal.

Proof.

($\subseteq$) Let $n \in A$. Then $n = 2k$ for some $k \in \mathbb{N}$.

$n^2 = (2k)^2 = 2(2k^2) \Rightarrow n^2$ is even $\Rightarrow n \in B$. $\therefore A \subseteq B$.

Example. Prove that $A = \{n \in \mathbb{N} : n \text{ is even}\}$ and $B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$ are equal.

Proof.

($\subseteq$) Let $n \in A$. Then $n = 2k$ for some $k \in \mathbb{N}$.

$n^2 = (2k)^2 = 2(2k^2) \Rightarrow n^2$ is even $\Rightarrow n \in B$. $\therefore A \subseteq B$.

($\supseteq$) Let $n \in B$. Suppose that n is odd: $n = 2k + 1$ for some $k \in \mathbb{N}$. Then $n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$ is odd, a contradiction. Hence, n is even and $n \in A$. $\therefore B \subseteq A$.

Example. Prove that $A = \{n \in \mathbb{N} : n \text{ is even}\}$ and $B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$ are equal.

Proof.

($\subseteq$) Let $n \in A$. Then $n = 2k$ for some $k \in \mathbb{N}$.

$n^2 = (2k)^2 = 2(2k^2) \Rightarrow n^2$ is even $\Rightarrow n \in B$. $\therefore A \subseteq B$.

($\supseteq$) Let $n \in B$. Suppose that n is odd: $n = 2k + 1$ for some $k \in \mathbb{N}$. Then $n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$ is odd, a contradiction. Hence, n is even and $n \in A$. $\therefore B \subseteq A$.

$$\therefore A = B$$

Example. Define

$$A = \{n \in \mathbb{Z} : n = 2p, p \in \mathbb{Z}\}$$
$$B = \{n \in \mathbb{Z} : n \text{ is even}\}$$
$$C = \{n \in \mathbb{Z} : n = 2q - 2, q \in \mathbb{Z}\}$$
$$D = \{k \in \mathbb{Z} : k = 3r + 1, r \in \mathbb{Z}\}$$

(a) Is $A = B$? (b) Is $A = D$? (c) Is $A = C$?

Operations on Sets. Let A, B be subsets of a universe U.

1. The *union* of A and B, written $A \cup B$, is the set of all elements that are in A or in B.

$$A \cup B = \{x \in U : x \in A \vee x \in B\}$$

2. The *intersection* of A and B, written $A \cap B$, is the set of all elements that are in A and in B.

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}$$

3. The *complement* of A, written $\overline{A}$ or A', is the set of all elements that are not in A.

$$\overline{A} = \{x \in U : x \notin A\}$$

4. The *difference* $B - A$ or $B \setminus A$ is the set of all elements that are in B and not in A.

$$B - A = \{x \in U : x \in B \wedge x \notin A\}$$

The *power set* of U, denoted by $P(U)$, is the set of all subsets of U.

Example. Let $A = \{1, 2, 3\}$. Then

$$P(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$$

If $|A| = n$, then $|P(A)| = 2^n$.

The operations of set theory are equivalent to their counterpart connectives in logic theory.

Set Operation		Logic Connective	
$\setminus$	complement	$\sim$	negation
$\cup$	union	$\vee$	or
$\cap$	intersection	$\wedge$	and
$\subseteq$	subset	$\Rightarrow$	conditional
$=$	equality	$\Leftrightarrow$	biconditional

Example. Let $U = \mathbb{Z}$. Write down $\overline{A}$ for the following.

1. $A = \{1, 2, 3\}$
2. $A = \{x \in \mathbb{Z} : x \text{ is even}\}$
3. $A = \{x \in \mathbb{Z} : x > 0 \vee x < 0\}$

Example. Let $U = \mathbb{Z}$. Write down $\overline{A}$ for the following.

1. $A = \{1, 2, 3\}$
2. $A = \{x \in \mathbb{Z} : x \text{ is even}\}$
3. $A = \{x \in \mathbb{Z} : x > 0 \vee x < 0\}$

Example. Let $U = \mathbb{R}$. Write down $A \cup B$ and $A \cap B$ for the following.

1. $A = \{1\}$, $B = \{2\}$
2. A is the set of even integers, B is the set of odd integers.
3. $A = \{x \in \mathbb{R} : 0 \leq x \leq 2\}$, $B = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Proof.

$[(A \to C) \wedge (B \to C)] \underset{F}{\to} [(A \vee B) \to C]$

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Proof.

$[(A \to C) \wedge (B \to C)] \underset{F}{\to} [(A \vee B) \to C]$

$(A \to C) \underset{T}{\wedge} (B \to C)$ and $(A \vee B) \underset{F}{\to} C$

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Proof.

$[(A \to C) \wedge (B \to C)] \underset{F}{\to} [(A \vee B) \to C]$

$(A \to C) \underset{T}{\wedge} (B \to C)$ and $(A \vee B) \underset{F}{\to} C$

$A \underset{T}{\to} C$ and $B \underset{T}{\to} C$ and $A \underset{T}{\vee} B$ and $\underset{F}{C}$

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Proof.

$[(A \to C) \wedge (B \to C)] \underset{F}{\to} [(A \vee B) \to C]$

$(A \to C) \underset{T}{\wedge} (B \to C)$ and $(A \vee B) \underset{F}{\to} C$

$A \underset{T}{\to} C$ and $B \underset{T}{\to} C$ and $A \underset{T}{\vee} B$ and $\underset{F}{C}$

$\underset{F}{A}$ and $\underset{F}{B}$ and $A \underset{T}{\vee} B$ Contradiction!

Example. Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$. Use a truth table, or suppose the main connective is false and try to show a contradiction.

Proof.

$[(A \to C) \wedge (B \to C)] \underset{F}{\to} [(A \vee B) \to C]$

$(A \to C) \underset{T}{\wedge} (B \to C)$ and $(A \vee B) \underset{F}{\to} C$

$A \underset{T}{\to} C$ and $B \underset{T}{\to} C$ and $A \underset{T}{\vee} B$ and $\underset{F}{C}$

$\underset{F}{A}$ and $\underset{F}{B}$ and $A \underset{T}{\vee} B$ Contradiction!

$\therefore (A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$ $\square$

Exercise. Prove or disprove $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cap B \subseteq C$

Example. Let $U = \mathbb{R}$, $A = \{1, 2, 3\}$, $B = \{2\}$, $C = \{2, 3, 4\}$, $D = [0, 1]$.

(a) $A - C =$
(b)$B - C =$
(c) $D - B =$
(d) $D - A =$
(e) $A - D =$

Definition

*The sets A and B are **disjoint** if $A \cap B = \varnothing$.*

Definition

*The sets A and B are **disjoint** if $A \cap B = \varnothing$.*

Example. Let $U = \mathbb{R}$. Write down some sets that are disjoint to the following.

(a) $\{x \in \mathbb{Z} : x \text{ is even}\}$

(b) $\{x \in \mathbb{R} : x^2 - 5x + 6 \geq 0\}$

(c) $\mathbb{Q}$

Definition

*The sets A and B are **disjoint** if $A \cap B = \varnothing$.*

Example. Let $U = \mathbb{R}$. Write down some sets that are disjoint to the following.

(a) $\{x \in \mathbb{Z} : x \text{ is even}\}$

(b) $\{x \in \mathbb{R} : x^2 - 5x + 6 \geq 0\}$

(c) $\mathbb{Q}$

Definition (Addition Rule)

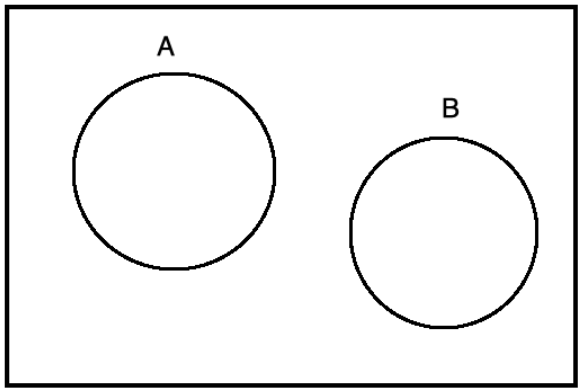
Let A, B be finite, disjoint sets. Then $A \cup B$ is finite and $|A \cup B| = |A| + |B|$.

Venn Diagrams

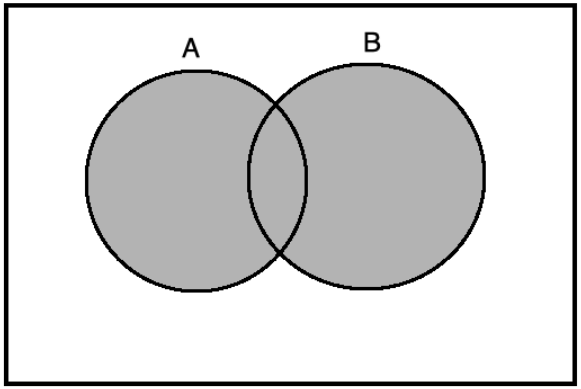
If we represent sets as regions in the plane, then the relationships among sets can be represented by drawings called Venn diagrams.

Venn Diagrams

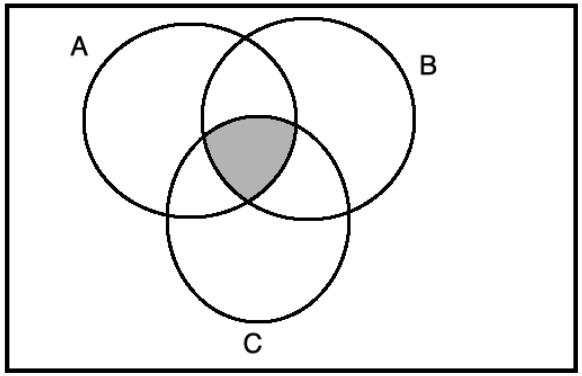
If we represent sets as regions in the plane, then the relationships among sets can be represented by drawings called Venn diagrams.



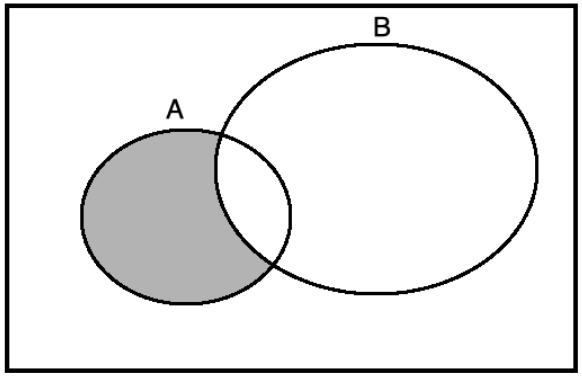
2 disjoint sets



Union of sets



Intersection of sets



Difference of sets

Algebra of Sets

There are many rules that govern set theory and the relationships among sets. All of the following can be proved using the definitions we have seen so far.

Algebra of Sets

There are many rules that govern set theory and the relationships among sets. All of the following can be proved using the definitions we have seen so far.

Theorem. Let U be a set and A, B, C be elements of $P(U)$.

(1) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$
$A \subseteq A \cup B$; $B \subseteq A \cup B$
$A \cap B \subseteq A$; $A \cap B \subseteq B$

Algebra of Sets

There are many rules that govern set theory and the relationships among sets. All of the following can be proved using the definitions we have seen so far.

Theorem. Let U be a set and A, B, C be elements of $P(U)$.

(1) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$
$A \subseteq A \cup B$; $B \subseteq A \cup B$
$A \cap B \subseteq A$; $A \cap B \subseteq B$

(2) $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$
$A \subseteq B \Leftrightarrow A \cup B = B$
$A \subseteq B \Leftrightarrow A \cap B = A$

Algebra of Sets

There are many rules that govern set theory and the relationships among sets. All of the following can be proved using the definitions we have seen so far.

Theorem. Let U be a set and A, B, C be elements of $P(U)$.

(1) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$
$A \subseteq A \cup B$; $B \subseteq A \cup B$
$A \cap B \subseteq A$; $A \cap B \subseteq B$

(2) $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$
$A \subseteq B \Leftrightarrow A \cup B = B$
$A \subseteq B \Leftrightarrow A \cap B = A$

(3) $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
$A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$

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

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

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

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

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

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

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

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

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

(7) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$

(8) $\overline{(\overline{A})} = A$

$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$

$A - B = A \cap \overline{B}$

$\overline{U} = \varnothing; \overline{\varnothing} = U$

(8) $\overline{(\overline{A})} = A$
$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$
$A - B = A \cap \overline{B}$
$\overline{U} = \varnothing; \overline{\varnothing} = U$

(9) $A \cap U = A; A \cup \varnothing = A$
$A \cap \varnothing = \varnothing; A \cup U = U$
$A \cap \overline{A} = \varnothing; A \cup \overline{A} = U$

(8) $\overline{(\overline{A})} = A$
$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$
$A - B = A \cap \overline{B}$
$\overline{U} = \varnothing; \overline{\varnothing} = U$

(9) $A \cap U = A; A \cup \varnothing = A$
$A \cap \varnothing = \varnothing; A \cup U = U$
$A \cap \overline{A} = \varnothing; A \cup \overline{A} = U$

(10) $(A \subseteq C \wedge B \subseteq C) \Leftrightarrow (A \cup B) \subseteq C$
$(A \subseteq B \wedge A \subseteq C) \Leftrightarrow A \subset (B \cap C)$

(8) $\overline{(\overline{A})} = A$
$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$
$A - B = A \cap \overline{B}$
$\overline{U} = \varnothing; \overline{\varnothing} = U$

(9) $A \cap U = A; A \cup \varnothing = A$
$A \cap \varnothing = \varnothing; A \cup U = U$
$A \cap \overline{A} = \varnothing; A \cup \overline{A} = U$

(10) $(A \subseteq C \wedge B \subseteq C) \Leftrightarrow (A \cup B) \subseteq C$
$(A \subseteq B \wedge A \subseteq C) \Leftrightarrow A \subset (B \cap C)$

Exercise. Prove them all!

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$.

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$.

$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \in \overline{A} \wedge x \in \overline{B} \Rightarrow x \in \overline{A} \cap \overline{B}$

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$.
$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \in \overline{A} \wedge x \in \overline{B} \Rightarrow x \in \overline{A} \cap \overline{B}$

($\supseteq$) Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A} \wedge x \in \overline{B}$.

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$.

$$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \in \overline{A} \wedge x \in \overline{B} \Rightarrow x \in \overline{A} \cap \overline{B}$$

($\supseteq$) Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A} \wedge x \in \overline{B}$.

$$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \notin A \cup B \Rightarrow x \in \overline{A \cup B}$$

Example. Prove De Morgan's Laws (7): $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$.

$$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \in \overline{A} \wedge x \in \overline{B} \Rightarrow x \in \overline{A} \cap \overline{B}$$

($\supseteq$) Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A} \wedge x \in \overline{B}$.

$$\Rightarrow x \notin A \wedge x \notin B \Rightarrow x \notin A \cup B \Rightarrow x \in \overline{A \cup B}$$

$\therefore \overline{A \cup B} = \overline{A} \cap \overline{B}$ $\square$

Example. Prove (2): $A \subseteq B \Leftrightarrow A \cup B = B$.

Example. Prove (2): $A \subseteq B \Leftrightarrow A \cup B = B$.

Proof (Part 1).

($\Rightarrow$) Let $A \subseteq B$.

($\subseteq$) Let $x \in A \cup B$. Then $x \in A \vee x \in B$.

Since $A \subseteq B$, if $x \in A$, then $x \in B$.

$\Rightarrow x \in B$

$\therefore A \cup B \subseteq B$.

Example. Prove (2): $A \subseteq B \Leftrightarrow A \cup B = B$.

Proof (Part 1).

($\Rightarrow$) Let $A \subseteq B$.

($\subseteq$) Let $x \in A \cup B$. Then $x \in A \vee x \in B$.
Since $A \subseteq B$, if $x \in A$, then $x \in B$.
$\Rightarrow x \in B$
$\therefore A \cup B \subseteq B$.

($\supseteq$) Let $x \in B$. Then $x \in A \cup B$.
$\therefore B \subseteq A \cup B$

Example. Prove (2): $A \subseteq B \Leftrightarrow A \cup B = B$.

Proof (Part 1).

($\Rightarrow$) Let $A \subseteq B$.

($\subseteq$) Let $x \in A \cup B$. Then $x \in A \vee x \in B$.

Since $A \subseteq B$, if $x \in A$, then $x \in B$.

$\Rightarrow x \in B$

$\therefore A \cup B \subseteq B$.

($\supseteq$) Let $x \in B$. Then $x \in A \cup B$.

$\therefore B \subseteq A \cup B$

$\therefore A \subseteq B \Rightarrow A \cup B = B$. $\square$

Proof (part 2).

($\Leftarrow$) Let $A \cup B = B$.

Let $x \in A$. Then $x \in A \cup B$. But $A \cup B = B$, so $x \in B$.

Proof (part 2).

($\Leftarrow$) Let $A \cup B = B$.

Let $x \in A$. Then $x \in A \cup B$. But $A \cup B = B$, so $x \in B$.

$\Rightarrow A \subseteq B$

$\therefore A \cup B = B \Rightarrow A \subseteq B$

Proof (part 2).

($\Leftarrow$) Let $A \cup B = B$.

Let $x \in A$. Then $x \in A \cup B$. But $A \cup B = B$, so $x \in B$.

$\Rightarrow A \subseteq B$

$\therefore A \cup B = B \Rightarrow A \subseteq B$

$\therefore A \subseteq B \Leftrightarrow A \cup B = B$ $\square$

Example. Prove that the difference operator is not associative: $A - (B - C) \neq (A - B) - C$.

Example. Prove that the difference operator is not associative: $A - (B - C) \neq (A - B) - C$.

Proof.

$A - (B - C) = A - (B \cap \overline{C}) = A \cap \overline{B \cap \overline{C}} = A \cap (\overline{B} \cup C) = (A \cap \overline{B}) \cup (A \cap C)$

Example. Prove that the difference operator is not associative: $A - (B - C) \neq (A - B) - C$.

Proof.

$A - (B - C) = A - (B \cap \overline{C}) = A \cap \overline{B \cap \overline{C}} = A \cap (\overline{B} \cup C) =$
$(A \cap \overline{B}) \cup (A \cap C)$
$(A - B) - C = (A \cap \overline{B}) - C = A \cap \overline{B} \cap \overline{C}$

Example. Prove that the difference operator is not associative: $A - (B - C) \neq (A - B) - C$.

Proof.

$A - (B - C) = A - (B \cap \overline{C}) = A \cap \overline{B \cap \overline{C}} = A \cap (\overline{B} \cup C) = (A \cap \overline{B}) \cup (A \cap C)$

$(A - B) - C = (A \cap \overline{B}) - C = A \cap \overline{B} \cap \overline{C}$

Let $x \in A \cap C$. Then $x \in A - (B - C)$ and, since $x \in C$, we have $x \notin \overline{C}$. Hence, $x \notin (A - B) - C$. □

Definition

The sets $A_1, A_2, \ldots, A_k$ *are* ***pairwise disjoint*** *if*

$A_i \cap A_j = \varnothing \ \forall \ i, j \in \{1, 2, \ldots, k\}, i \neq j.$

Definition

*The sets $A_1, A_2, \ldots, A_k$ are **pairwise disjoint** if*

$A_i \cap A_j = \varnothing \ \forall \ i, j \in \{1, 2, \ldots, k\}, i \neq j.$

Theorem (Extension of Addition Rule)

Let $A_1, A_2, \ldots, A_k$ be finite, pairwise disjoint sets. Then $A_1 \cup A_2 \cup \cdots \cup A_k$ is finite and
$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$

Chapter 5:

Combinatorics

Sequences and Words

A *sequence* is an ordered list of objects, with repetitions of the same object allowed (as opposed to a set). The objects of a sequence are called *terms*. A sequence may be finite

$$(1, 2, 3, 4); (a, b, \ldots, z);$$

or infinite

$$(2, 4, 6, \ldots); \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots\right).$$

Sequences and Words

A *sequence* is an ordered list of objects, with repetitions of the same object allowed (as opposed to a set). The objects of a sequence are called *terms*. A sequence may be finite

$$(1, 2, 3, 4); (a, b, \ldots, z);$$

or infinite

$$(2, 4, 6, \ldots); \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots\right).$$

The order matters; $(1, 2, 3)$ is a different sequence than $(3, 2, 1)$.

A sequence is also called a *word* in the alphabet U. The sequence $(t_1, t_2, \ldots, t_k)$ is equivalent to the word $t_1 t_2 \cdots t_k$.

A sequence is also called a *word* in the alphabet U. The sequence $(t_1, t_2, \ldots, t_k)$ is equivalent to the word $t_1 t_2 \cdots t_k$.

Theorem (Multiplication Rule)

Let S denote the number of distinct sequences $(t_1, t_2, \ldots, t_k)$ with n_i possible values for each t_i. Then

$$S = n_1 n_2 \cdots n_k.$$

A sequence is also called a *word* in the alphabet U. The sequence $(t_1, t_2, \ldots, t_k)$ is equivalent to the word $t_1 t_2 \cdots t_k$.

Theorem (Multiplication Rule)

Let S denote the number of distinct sequences $(t_1, t_2, \ldots, t_k)$ with n_i possible values for each t_i. Then

$$S = n_1 n_2 \cdots n_k.$$

Corollary

Let $|A| = n$. Then there are n^k sequences of length k in A.

Example. How many 3-letter words can be formed with the English alphabet?

Example. How many 3-letter words can be formed with the English alphabet?

$26 \cdot 26 \cdot 26 = 17576$. The words are $AAA, AAB, \ldots, ZZZ$.

Example. How many 3-letter words can be formed with the English alphabet?

$26 \cdot 26 \cdot 26 = 17576$. The words are $AAA, AAB, \ldots, ZZZ$.

Permutations

A sequence in which all terms are distinct is called a permutation. If $|S| = n$, a sequence of length $k \leq n$ of all distinct terms is called a *permutation of n objects taken k at a time*. If $k = n$, we just say a permutation of n objects.

Example. Let $s = \{1, 2, 3, 4, 5, 6\}$. The following words in S are permutations of 6 objects taken 3 at a time.

$$s_1 = 146, \quad s_2 = 324, \quad s_3 = 531$$

The following words in S are permutations of 6 objects.

$$s_4 = 123456, \quad s_5 = 132645, \quad s_6 = 651324$$

Example. Let $s = \{1, 2, 3, 4, 5, 6\}$. The following words in S are permutations of 6 objects taken 3 at a time.

$$s_1 = 146, \quad s_2 = 324, \quad s_3 = 531$$

The following words in S are permutations of 6 objects.

$$s_4 = 123456, \quad s_5 = 132645, \quad s_6 = 651324$$

There are $P_k^n = \frac{n!}{(n-k)!}$ permutations of n objects taken k at a time.

Notice that

$$\frac{n!}{(n-k)!} = \frac{1 \cdot 2 \cdot \ldots \cdot n}{1 \cdot 2 \cdot \ldots \cdot (n-k)} = n(n-1)\cdots(n-k+1).$$

This has a shorter notation called *falling factorial* $n^{\underline{k}}$, which is also used for $k > n$. In that case, $n^{\underline{k}} = 0$.

Notice that

$$\frac{n!}{(n-k)!} = \frac{1 \cdot 2 \cdot \ldots \cdot n}{1 \cdot 2 \cdot \ldots \cdot (n-k)} = n(n-1)\cdots(n-k+1).$$

This has a shorter notation called *falling factorial* $n^{\underline{k}}$, which is also used for $k > n$. In that case, $n^{\underline{k}} = 0$.

Example. Let $n = 7, k = 10$. Then

$$n^{\underline{k}} = 7^{\underline{10}} = 7 \cdot 6 \cdot \ldots \cdot 1 \cdot 0 \cdot (-1) \cdot (-2) = 0.$$

Theorem

For all $n, k \in \mathbb{N}$, there are $n^{\underline{k}}$ permutations of n objects taken k at a time.

Theorem

For all $n, k \in \mathbb{N}$, there are $n^{\underline{k}}$ permutations of n objects taken k at a time.

Proof.

If $k > n$, there is no way to permute n objects k at a time, so the answer is zero.

$$n^{\underline{k}} = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 \cdot 0 \cdot (-1) \cdot \ldots \cdot (n-k+1) = 0$$

Theorem

For all $n, k \in \mathbb{N}$, there are $n^{\underline{k}}$ permutations of n objects taken k at a time.

Proof.

If $k > n$, there is no way to permute n objects k at a time, so the answer is zero.

$$n^{\underline{k}} = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 \cdot 0 \cdot (-1) \cdot \ldots \cdot (n-k+1) = 0$$

If $k \leq n$, there are n choices for the first element, then $n-1$ choices for the second, etc. The total is

$$n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = n^{\underline{k}} = \frac{n!}{(n-k)!} = P_k^n.$$

Counting Strategies

Consider the problem, “how many sequences satisfy a certain set of properties?”

Counting Strategies

Consider the problem, “how many sequences satisfy a certain set of properties?” We use counting strategy to answer this question methodically. For a sequence of length k, use k empty slots.

$$\underline{\quad} \quad \underline{\quad} \quad \underline{\quad} \quad \cdots \quad \underline{\quad}$$
$$1 \quad 2 \quad 3 \quad \cdots \quad k$$

Counting Strategies

Consider the problem, “how many sequences satisfy a certain set of properties?” We use counting strategy to answer this question methodically. For a sequence of length k, use k empty slots.

$$\underline{\quad} \quad \underline{\quad} \quad \underline{\quad} \quad \cdots \quad \underline{\quad}$$
$$1 \quad 2 \quad 3 \quad \cdots \quad k$$

Fill them one at a time with the number of possible values for each term, given the restrictions of the properties. If there are n_1 choices for position 1, n_2 for position 2, etc., then the multiplication rule says there are $n_1 n_2 \cdots n_k$ possible distinct sequences.

Example. There are 2 highways from Brisbane to Sydney and 3 highways from Sydney to Adelaide. How many different round trips are there from Brisbane to Adelaide through Sydney? How many are there without taking the same highway twice?

Example. There are 2 highways from Brisbane to Sydney and 3 highways from Sydney to Adelaide. How many different round trips are there from Brisbane to Adelaide through Sydney? How many are there without taking the same highway twice?

First question: $\overline{B-S}\ \overline{S-A}\ \overline{A-S}\ \overline{S-B}$

Example. There are 2 highways from Brisbane to Sydney and 3 highways from Sydney to Adelaide. How many different round trips are there from Brisbane to Adelaide through Sydney? How many are there without taking the same highway twice?

First question: $\overline{B-S}\ \overline{S-A}\ \overline{A-S}\ \overline{S-B}$

Second question: $\overline{B-S}\ \overline{S-A}\ \overline{A-S}\ \overline{S-B}$

You don't necesarily have to start with the first position. Start where it's most convenient.

Example. How many 5-digit odd numbers with no repeated digits are there?

_____ _____ _____ _____ _____

You don't necesarily have to start with the first position. Start where it's most convenient.

Example. How many 5-digit odd numbers with no repeated digits are there?

_____ _____ _____ _____ _____

Hint: There's a big restriction on digit 5 and a smaller one on digit 1, so start with those.

Sometimes we need to break up a problem into subproblems.

Example. How many 5-digit even numbers with no repeated digits are there?

_____ _____ _____ _____ _____

Sometimes we need to break up a problem into subproblems.

Example. How many 5-digit even numbers with no repeated digits are there?

_____ _____ _____ _____ _____

We have the same restriction on digit 5, but the restriction on digit 1 is different if digit 5 is zero.

For a required adjacency, treat the adjacency as a single object, then multiply by the number of arrangements of the adjacency.

Example. Three single people and a married couple are to be seated in a row of chairs. In how many ways can this be done such that the spouses sit together?

For a required adjacency, treat the adjacency as a single object, then multiply by the number of arrangements of the adjacency.

Example. Three single people and a married couple are to be seated in a row of chairs. In how many ways can this be done such that the spouses sit together?

For a forbidden adjacency, calculate it as a required adjacency, then subtract from the total possible arrangements.

Example. In how many ways can you arrange a cow, a goat, a fox and a chicken in a row so that the fox and the chicken are not next to each other?

Binomial Coefficients

Recall the power set of X: $P(X) = \{A : A \subseteq X\}$.

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

Binomial Coefficients

Recall the power set of X: $P(X) = \{A : A \subseteq X\}$.

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

Another notation for $P(X)$ is 2^X. This is because of the following.

Theorem

Let $|X| = n \in \mathbb{N} \cup \{0\}$. Then X has 2^n subsets, i.e. $|P(X)| = 2^{|X|}$.

Proof (induction).

(a) Let $n = 0$. Then $X = \varnothing$ and $P(X) = \varnothing$, so $|P(X)| = 1 = 2^0$.

Proof (induction).

(a) Let $n = 0$. Then $X = \varnothing$ and $P(X) = \varnothing$, so $|P(X)| = 1 = 2^0$.

(b) Let $k \in \mathbb{N}$, suppose $|X| = k$ and $|P(X)| = 2^k$. Define

$$Y = X \cup \{y\} = \{x_1, x_2, \ldots, x_k, y\}.$$

The subsets of Y are those that contain y and those that do not.

Proof (induction).

(a) Let $n = 0$. Then $X = \varnothing$ and $P(X) = \varnothing$, so $|P(X)| = 1 = 2^0$.

(b) Let $k \in \mathbb{N}$, suppose $|X| = k$ and $|P(X)| = 2^k$. Define

$$Y = X \cup \{y\} = \{x_1, x_2, \ldots, x_k, y\}.$$

The subsets of Y are those that contain y and those that do not.

- Those that do not contain y are exactly the subsets of X, of which there are 2^k.

Proof (induction).

(a) Let $n = 0$. Then $X = \varnothing$ and $P(X) = \varnothing$, so $|P(X)| = 1 = 2^0$.

(b) Let $k \in \mathbb{N}$, suppose $|X| = k$ and $|P(X)| = 2^k$. Define

$$Y = X \cup \{y\} = \{x_1, x_2, \ldots, x_k, y\}.$$

The subsets of Y are those that contain y and those that do not.

- Those that do not contain y are exactly the subsets of X, of which there are 2^k.
- Those that do contain y are of the form $Z \cup \{y\}$ where $Z \in P(X)$, so there are exactly 2^k of those as well.

Proof (induction).

(a) Let $n = 0$. Then $X = \varnothing$ and $P(X) = \varnothing$, so $|P(X)| = 1 = 2^0$.

(b) Let $k \in \mathbb{N}$, suppose $|X| = k$ and $|P(X)| = 2^k$. Define

$$Y = X \cup \{y\} = \{x_1, x_2, \ldots, x_k, y\}.$$

The subsets of Y are those that contain y and those that do not.

- Those that do not contain y are exactly the subsets of X, of which there are 2^k.
- Those that do contain y are of the form $Z \cup \{y\}$ where $Z \in P(X)$, so there are exactly 2^k of those as well.

Thus, $|Y| = 2^k + 2^k = 2^{k+1}$.

$\therefore |P(X)| = 2^{|X|}\ \forall X$ finite. □

Let $|X| = n \in \mathbb{N} \cup \{0\}$. For every $k \in \mathbb{N} \cup \{0\}$, we denote by $\binom{n}{k}$ the number of subsets of X with k elements.

$$\binom{n}{k} = |\{A : A \subseteq X \wedge |A| = k\}|$$

This is read "n choose k" and is the k^{th} *binomial coefficient* of order n. Some $\binom{n}{k}$ values are obvious:

- $\binom{n}{0} = 1$, since the only subset of cardinality 0 is $\varnothing$.
- $\binom{n}{n} = 1$, since X is the only subset of X with n elements.
- If $k > n$, then $\binom{n}{k} = 0$, as it is impossible to have a subset of X with cardinality larger than $|X|$.

Let $|X| = n \in \mathbb{N} \cup \{0\}$. For every $k \in \mathbb{N} \cup \{0\}$, we denote by $\binom{n}{k}$ the number of subsets of X with k elements.

$$\binom{n}{k} = |\{A : A \subseteq X \wedge |A| = k\}|$$

This is read "n choose k" and is the k^{th} *binomial coefficient* of order n. Some $\binom{n}{k}$ values are obvious:

- $\binom{n}{0} = 1$, since the only subset of cardinality 0 is $\varnothing$.
- $\binom{n}{n} = 1$, since X is the only subset of X with n elements.
- If $k > n$, then $\binom{n}{k} = 0$, as it is impossible to have a subset of X with cardinality larger than $|X|$.

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$, $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n^{\underline{k}}}{k!}$.

Proof.

For $k > n$, we have seen that $n^{\underline{k}} = 0$ and $\binom{n}{k} = 0$. Let $k \leq n$.

Proof.

For $k > n$, we have seen that $n^{\underline{k}} = 0$ and $\binom{n}{k} = 0$. Let $k \leq n$.

Recall that the number of permutations of n objects taken k at a time is $P_k^n = \frac{n!}{(n-k)!}$. This number can be obtained by taking all $\binom{n}{k}$ combinations of k elements and ordering the elements in each combination, which can be done in P_k^k ways.

Proof.

For $k > n$, we have seen that $n^{\underline{k}} = 0$ and $\binom{n}{k} = 0$. Let $k \leq n$.

Recall that the number of permutations of n objects taken k at a time is $P_k^n = \frac{n!}{(n-k)!}$. This number can be obtained by taking all $\binom{n}{k}$ combinations of k elements and ordering the elements in each combination, which can be done in P_k^k ways. Thus,

$$P_k^n = \binom{n}{k} P_k^k \Rightarrow \binom{n}{k} = \frac{P_k^n}{P_k^k} = \frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{k!(n-k)!} = \frac{n^{\underline{k}}}{k!}.$$

Proof.

For $k > n$, we have seen that $n^{\underline{k}} = 0$ and $\binom{n}{k} = 0$. Let $k \leq n$.

Recall that the number of permutations of n objects taken k at a time is $P_k^n = \frac{n!}{(n-k)!}$. This number can be obtained by taking all $\binom{n}{k}$ combinations of k elements and ordering the elements in each combination, which can be done in P_k^k ways. Thus,

$$P_k^n = \binom{n}{k} P_k^k \Rightarrow \binom{n}{k} = \frac{P_k^n}{P_k^k} = \frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{k!(n-k)!} = \frac{n^{\underline{k}}}{k!}.$$

□

The symbol $\binom{n}{k}$ is also denoted by C_k^n, the number of combinations of n objects taken k at a time.

Example. How many different poker hands are there?

Example. How many different poker hands are there?

There are 5 cards in a poker hand, order is not important and they are taken from a deck of 52 cards. So there are

$$\binom{52}{5} = \frac{52!}{5!47!} = 2,598,960.$$

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

Proof.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}$$

□

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

Proof.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}$$ □

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$,

(a) $\binom{n}{0} = 1$

(b) $\binom{0}{k} = 0$

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

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

Proof.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}$$ □

Theorem

For all $n, k \in \mathbb{N} \cup \{0\}$ s.t. $k \leq n$,

(a) $\binom{n}{0} = 1$

(b) $\binom{0}{k} = 0$

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

Exercise. Prove the above theorem.

The Binomial Theorem

In how many ways can 3 red marbles and 4 blue marbles be arranged in a row? (Or a more practical equivalent example: how many binary words with 3 zeros and 4 ones are there?)

The Binomial Theorem

In how many ways can 3 red marbles and 4 blue marbles be arranged in a row? (Or a more practical equivalent example: how many binary words with 3 zeros and 4 ones are there?)

The multiplication rule isn't very helpful here; there are too many cases. However, notice that once you choose positions for the red marbles, the placement of the blue ones is determined already.

So the question is how many way are there to choose 3 of 7 positions? We know the answer is $\binom{7}{3} = 35$. Similarly, if you choose 4 positions for the blue marbles first, there are $\binom{7}{4} = 35$ ways to do it. The answer is the same.

So the question is how many way are there to choose 3 of 7 positions? We know the answer is $\binom{7}{3} = 35$. Similarly, if you choose 4 positions for the blue marbles first, there are $\binom{7}{4} = 35$ ways to do it. The answer is the same.

Theorem

The number of words of length n consisting of n_1 letters of one sort and $n_2 = n - n_1$ letters of another sort is

$$\binom{n}{n_1} = \binom{n}{n_2} = \frac{(n_1 + n_2)!}{n_1! n_2!}.$$

Consider the binomial expansion

$$(x+y)^2 = xx + xy + yx + yy,$$

which is the sum of all words of length 2 in the alphabet $\{x, y\}$.

Consider the binomial expansion

$$(x+y)^2 = xx + xy + yx + yy,$$

which is the sum of all words of length 2 in the alphabet $\{x, y\}$. Similarly,

$$(x+y)^3 = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$

is the sum of all words of length 3 in the same alphabet.

Consider the binomial expansion

$$(x+y)^2 = xx + xy + yx + yy,$$

which is the sum of all words of length 2 in the alphabet $\{x, y\}$. Similarly,

$$(x+y)^3 = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$

is the sum of all words of length 3 in the same alphabet. Simplifying, we get the familiar formulae:

$$(x+y)^2 = x^2 + 2xy + y^2,$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

The binomial theorem below is a formula for the coefficients of binomial expansion to any power n.

Theorem

For all $n \in \mathbb{N} \cup \{0\}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

The binomial theorem below is a formula for the coefficients of binomial expansion to any power n.

Theorem

For all $n \in \mathbb{N} \cup \{0\}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof.

The case $n = 0$ is easily verified by hand. For $n \in \mathbb{N}$, the expansion of $(x+y)^n$ is the sum of all 2^n words of length n in the alphabet $\{x, y\}$. By the previous theorem, the number of such words that consist of k x's and $n-k$ y's is $\binom{n}{k}$. □

The theorem gives the expansion in ascending powers of x.

$$(x+y)^n = \binom{n}{0}y^n + \binom{n}{1}xy^{n-1} + \binom{n}{2}x^2y^{n-2} + \cdots + \binom{n}{n-1}x^{n-1}y + \binom{n}{n}x^n$$

The theorem gives the expansion in ascending powers of x.

$$(x+y)^n = \binom{n}{0}y^n + \binom{n}{1}xy^{n-1} + \binom{n}{2}x^2y^{n-2} + \cdots + \binom{n}{n-1}x^{n-1}y + \binom{n}{n}x^n$$

Equivalently, it can be written in reverse.

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

We can substitute values for x, y to obtain identities.

Example. Let $x = y = 1$. then the binomial theorem gives

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

We can substitute values for x, y to obtain identities.

Example. Let $x = y = 1$. then the binomial theorem gives

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Example. Let $x = -1, y = 1$, and n be odd. Then the binomial theorem gives

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots - \binom{n}{n} = 0$$

We can substitute values for x, y to obtain identities.

Example. Let $x = y = 1$. then the binomial theorem gives

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Example. Let $x = -1, y = 1$, and n be odd. Then the binomial theorem gives

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots - \binom{n}{n} = 0$$

$$\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{(n-1)} = \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n}$$

We can substitute values for x, y to obtain identities.

Example. Let $x = y = 1$. then the binomial theorem gives

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Example. Let $x = -1, y = 1$, and n be odd. Then the binomial theorem gives

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots - \binom{n}{n} = 0$$

$$\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{(n-1)} = \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n}$$

$$\sum_{k \text{ even}}^{n} \binom{n}{k} = \sum_{k \text{ odd}}^{n} \binom{n}{k}$$

Sometimes, a useful trick is to use the fact that $x = x \cdot 1$.

Example. Factorise $\sum_{k=0}^{n} \binom{n}{k} a^k$.

Sometimes, a useful trick is to use the fact that $x = x \cdot 1$.

Example. Factorise $\sum_{k=0}^{n} \binom{n}{k} a^k$.

$$\sum_{k=0}^{n} \binom{n}{k} a^k = \sum_{k=0}^{n} \binom{n}{k} a^k 1^{n-k} = (a+1)^n$$

Sometimes, a useful trick is to use the fact that $x = x \cdot 1$.

Example. Factorise $\sum_{k=0}^{n} \binom{n}{k} a^k$.

$$\sum_{k=0}^{n} \binom{n}{k} a^k = \sum_{k=0}^{n} \binom{n}{k} a^k 1^{n-k} = (a+1)^n$$

Example. Simplify $\sum_{k=1}^{17} (-1)^k \binom{17}{k} 13^{17-k}$.

Sometimes, a useful trick is to use the fact that $x = x \cdot 1$.

Example. Factorise $\sum_{k=0}^{n} \binom{n}{k} a^k$.

$$\sum_{k=0}^{n} \binom{n}{k} a^k = \sum_{k=0}^{n} \binom{n}{k} a^k 1^{n-k} = (a+1)^n$$

Example. Simplify $\sum_{k=1}^{17} (-1)^k \binom{17}{k} 13^{17-k}$.

$$\begin{aligned}\sum_{k=1}^{17} \binom{17}{k} 13^{17-k}(-1)^k &= \sum_{k=0}^{17} \binom{17}{k} 13^{17-k}(-1)^k - \binom{17}{0} 13^{17-0}(-1)^0 \\ &= (13-1)^{17} - 1 \cdot 13^{17} \cdot 1 \\ &= 12^{17} - 13^{17}\end{aligned}$$

Chapter 6:

Relations and Functions

Definition

Let A, B be sets, $a \in A$, $b \in B$. An ***ordered pair*** (a, b) *is a pair of elements with the property*

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Note. The open interval $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ uses the same notation, but context makes it clear.

Definition

*The **Cartesian product** of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

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

Definition

*The **Cartesian product** of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

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

Example. Let $A = B = \mathbb{R}$. What is $A \times B$?

Definition

*The **Cartesian product** of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

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

Example. Let $A = B = \mathbb{R}$. What is $A \times B$?

Example. Let $A = \{3\}$, $B = \{2, 3\}$. What is $A \times B$?

Definition

*The **Cartesian product** of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

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

Example. Let $A = B = \mathbb{R}$. What is $A \times B$?

Example. Let $A = \{3\}$, $B = \{2, 3\}$. What is $A \times B$?

Example. Let $A = \{x, y\}$, $B = \{1, 2, 3\}$, $C = \{\alpha, \beta\}$. What is $(A \times B) \times C$?

Definition

*The **Cartesian product** of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.*

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

Example. Let $A = B = \mathbb{R}$. What is $A \times B$?

Example. Let $A = \{3\}$, $B = \{2, 3\}$. What is $A \times B$?

Example. Let $A = \{x, y\}$, $B = \{1, 2, 3\}$, $C = \{\alpha, \beta\}$. What is $(A \times B) \times C$?

Example. Let $A = \{1, 2\}$, $B = \{\pi, e\}$. Is $A \times B = B \times A$?

Definition

*We say that R is a **(binary) relation** from A to B if R is a subset of $A \times B$. If $R \subseteq A \times A$, then R is called a relation on A. We say that a is **related** to b by R if $(a, b) \in R$. This is denoted by aRb.*

Definition

*We say that R is a **(binary) relation** from A to B if R is a subset of $A \times B$. If $R \subseteq A \times A$, then R is called a relation on A. We say that a is **related** to b by R if $(a, b) \in R$. This is denoted by aRb.*

Example. Let $X = \{0, 1, 2, 3\}$,
$R = \{(x, y) : \exists\, z \in \mathbb{N} \text{ s.t. } x + z = y\}$.

(a) What is a simpler expression for R (without using z)?

(b) List all the elements of R.

(c) Sketch $X \times X$ and circle the elements of R.

Example. Let R on $\mathbb{Z}\setminus\{0\}$ be given by

$$R = \{(x, y) : \exists\, z \in \mathbb{Z} \text{ s.t. } xz = y\}.$$

(a) Describe R.

(b) True or false?

- $(2, -4) \in R$
- $-3R0$
- $(3, 5) \in R$

Example. Let R on $\mathbb{Z}$ be given by

$$R = \{(m, n) : m - n \text{ is even}\}.$$

(a) Which are elements of R? $(0, 3), (-5, -6), (2, -11), (17, 1)$

(b) Prove that n odd $\Rightarrow nR1$.

Union and Intersection of Relations

Relations are sets, so the set operators can be applied.

Example. Let R_1, R_2 on $\mathbb{R}$ be given by

$$R_1 = \{(x, y) : x = y\}, \quad R_2 = \{(x, y) : x = -y\}.$$

Write expressions for $R_1 \cup R_2$ and $R_1 \cap R_2$.

Definition

*Let R be a relation from A to B. The **domain** of R and the **range** of R, denoted respectively by* $\operatorname{dom} R$ *and* $\operatorname{ran} R$*, are defined by*

$$\operatorname{dom} R = \{x \in A : \exists\, y \in B \text{ s.t. } xRy\},$$
$$\operatorname{ran} R = \{y \in B : \exists\, x \in A \text{ s.t. } xRy\}.$$

Note that $\operatorname{dom} R \subseteq A$ and $\operatorname{ran} R \subseteq B$.

Example. Let $A = \{0, 1, 2, 3\}$, $R = \{(0, 0), (0, 1), (0, 2), (3, 0)\}$. Find $\operatorname{dom} R$ and $\operatorname{ran} R$.

Example. Let $A = \{0, 1, 2, 3\}$, $R = \{(0, 0), (0, 1), (0, 2), (3, 0)\}$. Find $\operatorname{dom} R$ and $\operatorname{ran} R$.

Example. Find domain and range of R on $\mathbb{Z} \times \mathbb{Q}$, $R = \left\{(x, y) : x \neq 0 \wedge y = \frac{1}{x}\right\}$.

Example. Let $A = \{0, 1, 2, 3\}$, $R = \{(0, 0), (0, 1), (0, 2), (3, 0)\}$. Find $\operatorname{dom} R$ and $\operatorname{ran} R$.

Example. Find domain and range of R on $\mathbb{Z} \times \mathbb{Q}$, $R = \left\{(x, y) : x \neq 0 \wedge y = \frac{1}{x}\right\}$.

Example. Find domain and range of R on $\mathbb{Z}$, $R = \{(x, y) : xy \neq 0\}$.

Inverse Relations

If R is on $A \times B$, then a relation R^{-1} on $B \times A$ can be defined by interchanging the elements of every ordered pair of R.

Inverse Relations

If R is on $A \times B$, then a relation R^{-1} on $B \times A$ can be defined by interchanging the elements of every ordered pair of R.

Definition

*Let R be a relation on $A \times B$. The **inverse relation** of R is*

$$R^{-1} = \{(y, x) : (x, y) \in R\}.$$

Note that $\text{dom } R^{-1} = \text{ran } R$ and $\text{ran } R^{-1} = \text{dom } R$.

Example. Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $R = \{(a, 1), (b, 2), (c, 3), (a, 4)\}$. Find R^{-1}.

Example. Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $R = \{(a, 1), (b, 2), (c, 3), (a, 4)\}$. Find R^{-1}.

Example. Define R on $\mathbb{N}$ by $R = \{(x, y) : y = 2x\}$. Write 3 elements of R and 3 elements of R^{-1}. Write a definition of R^{-1}.

Example. Let $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $R = \{(a, 1), (b, 2), (c, 3), (a, 4)\}$. Find R^{-1}.

Example. Define R on $\mathbb{N}$ by $R = \{(x, y) : y = 2x\}$. Write 3 elements of R and 3 elements of R^{-1}. Write a definition of R^{-1}.

Example. The identity relation on $\mathbb{R}$ is $R = \{(x, x) : x \in \mathbb{R}\}$. What is R^{-1}?

Properties of Relations

Let R be a relation on A. Then

(a) R is **reflexive** on A iff $\forall\ x \in A$, $(x, x) \in R$;

Properties of Relations

Let R be a relation on A. Then

(a) R is **reflexive** on A iff $\forall\, x \in A$, $(x, x) \in R$;

(b) R is **symmetric** on A iff $\forall\, x, y \in A$, $(x, y) \in R \Rightarrow (y, x) \in R$;

Properties of Relations

Let R be a relation on A. Then

(a) R is **reflexive** on A iff $\forall\, x \in A$, $(x, x) \in R$;

(b) R is **symmetric** on A iff $\forall\, x, y \in A$, $(x, y) \in R \Rightarrow (y, x) \in R$;

(c) R is **transitive** on A iff $\forall\, x, y, z \in A$, $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$.

Example. Which properties do the following relations satisfy?

1. On $\mathbb{N}$, $R = \{(x, y) : x \text{ is a factor of } y\}$.
2. On $\mathbb{R}$, the identity relation.
3. On $\mathbb{Z}$, $R = \{(x, y) : x < y\}$.
4. On $\mathbb{R}$, $R = \{(x, y) : y = x^2\}$.
5. On the set P of all people in the world, $R = \{(x, y) : x \text{ is in the family of } y\}$.
6. On P, $R = \{(x, y) : x \text{ loves } y\}$.

Equivalence Relations

Definition

*Let R be a relation on A. Then R is an **equivalence relation** on A iff R is reflexive, symmetric and transitive on A.*

Equivalence Relations

Definition

*Let R be a relation on A. Then R is an **equivalence relation** on A iff R is reflexive, symmetric and transitive on A.*

Example. Prove or disprove that the identity relation on $\mathbb{R}$ is an equivalence relation.

Equivalence Relations

Definition

*Let R be a relation on A. Then R is an **equivalence relation** on A iff R is reflexive, symmetric and transitive on A.*

Example. Prove or disprove that the identity relation on $\mathbb{R}$ is an equivalence relation.

Example. On $\mathbb{Z}$, prove that $R = \{(a \equiv b \pmod{n})\}$ is an equivalence relation.

Equivalence Relations

Definition

*Let R be a relation on A. Then R is an **equivalence relation** on A iff R is reflexive, symmetric and transitive on A.*

Example. Prove or disprove that the identity relation on $\mathbb{R}$ is an equivalence relation.

Example. On $\mathbb{Z}$, prove that $R = \{(a \equiv b \pmod{n})\}$ is an equivalence relation.

Example. On $\mathbb{Z}$, prove that $R = \{(a, b) : ab = 0\}$ is not an equivalence relation.

Equivalence Classes

Definition

Let R be an equivalence relation on A. For each $a \in A$, the ***equivalence class*** *of a, denoted by $[a]$, is the set*

$$[a] = \{x \in A : xRa\}.$$

Equivalence Classes

Definition

Let R be an equivalence relation on A. For each $a \in A$, the ***equivalence class*** *of a, denoted by $[a]$, is the set*

$$[a] = \{x \in A : xRa\}.$$

Equivalence classes have the following properties.

(a) For any $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.

(b) All distinct equivalence classes form a partition of A: their union is A and the intersection of any two of them is empty.

Example. Let $A = \{0, 1, 2\}$,
$R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Find $[0], [1], [2]$.

Example. Let $A = \{0, 1, 2\}$,
$R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Find [0], [1], [2].

Example. What do the equivalence classes of the identity relation on $\mathbb{R}$ look like?

Example. Let $A = \{0, 1, 2\}$,
$R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Find $[0], [1], [2]$.

Example. What do the equivalence classes of the identity relation on $\mathbb{R}$ look like?

Example. Let R on $\mathbb{Z}$ be defined by $R = \{(a, b) : a \equiv b \pmod 3\}$. Find $[0], [1], [2]$.

Functions

Definition

*A relation F from A to B is a **function** from A to B iff*

1. $\text{dom } F = A$ *and*
2. *for each $x \in A$ there is at most one $y \in B$ such that $(x, y) \in F$.*

Functions

Definition

*A relation F from A to B is a **function** from A to B iff*

1. $\text{dom } F = A$ *and*
2. *for each $x \in A$ there is at most one $y \in B$ such that $(x, y) \in F$.*

A function f from A to B is denoted by $f : A \to B$. The equation $y = f(x)$ means $(x, y) \in f$, in which case y is the image of x under f.

Relations and Functions

Relations on $\mathbb{R}$ can be plotted by drawing all the points. Such relations are functions if they satisfy the vertical line test: every vertical line cuts the curve of the relation at most once.

Relations on $\mathbb{R}$ can be plotted by drawing all the points. Such relations are functions if they satisfy the vertical line test: every vertical line cuts the curve of the relation at most once.

Example. Sketch the relations and determine which are functions.

1. On $\mathbb{R}$, $R = \{(x, y) : y = x^2\}$
2. On $\mathbb{R}$, $R = \{(x, y) : x = y^2\}$
3. On $\mathbb{R}_+$, $R = \{(x, y) : x = y^2\}$
4. On $\mathbb{R}$, $R = \{(x, y) : y = \sqrt{x}\}$

Example. Which are functions?

1. The identity relation on $A = \{1, 5, 10\}$.
2. $A = \{2, 4, 6\}$, $B = \{1, 3, 5\}$, R on $A \times B$, $R = \{(x, y) : x + 1 = y\}$.
3. On $\mathbb{Z}$, $F = \{(x, y) : x + 1 = y\}$.
4. On $\mathbb{R}$, $R = \{(x, y) : y = 1\}$.

Definition

*Let $f : A \to B$ be a function. Then f is **injective (one-to-one)** iff for all $x_1, x_2 \in A$,*

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

That is, each element of the range is the image of only one element of the domain.

Note. An injective function satisfies the horizontal line test.

Example. Let $A = \{0, 1, 2, 3\}$, $f : P(A) \to \mathbb{N}$, $f(A_i)$ is the number of elements in A_i. Prove or disprove that f is injective.

Example. Let $A = \{0, 1, 2, 3\}$, $f : P(A) \to \mathbb{N}$, $f(A_i)$ is the number of elements in A_i. Prove or disprove that f is injective.

Example. Which are injective?

1. On $A = \{1, 2, 3\}$, $F = \{(1, 2), (2, 3), (3, 1)\}$.
2. On A, $G = \{(1, 2), (2, 1), (3, 1)\}$.
3. On $\mathbb{Z}$, $F = \{(x, y) : y = 2x\}$.
4. On $\mathbb{Z} \setminus \{0\} \times \mathbb{R}$, $F = \{(x, y) : y = \sqrt{x^2 - 1}\}$.

Definition

*A function $f : A \to B$ is **surjective (onto)** iff* $\operatorname{ran} f = B$. *That is, for all $y \in B$ there exists $x \in A$ such that $f(x) = y$.*

Definition

*A function $f : A \to B$ is **surjective (onto)** iff* $\operatorname{ran} f = B$. *That is, for all $y \in B$ there exists $x \in A$ such that $f(x) = y$.*

Example. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$. Which are surjective?

1. $f : A \to B$, $f = \{(1, a), (2, c), (3, c), (4, d), (5, d)\}$
2. $f : A \to B$, $f = \{(1, a), (2, b), (3, c), (4, d), (5, a)\}$
3. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 4x - 1$
4. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 4x - 1$

Theorem

*The **inverse** of a function f, written f^{-1}, is also a function iff f is injective and surjective (i.e. bijective).*

Theorem

*The **inverse** of a function f, written f^{-1}, is also a function iff f is injective and surjective (i.e. bijective).*

Example. Sketch $f : \mathbb{R}_+ \to \mathbb{R}$, $f = \{(x, y), y = x^2\}$. Find and sketch f^{-1}. Is f^{-1} a function?

Chapter 7:

Graph Theory

Many real-world problems concern objects and relations, eg. people with friendships, cities connected by highways, web pages linked to others, etc. Graph theory is the mathematical abstraction and analysis of these situations.

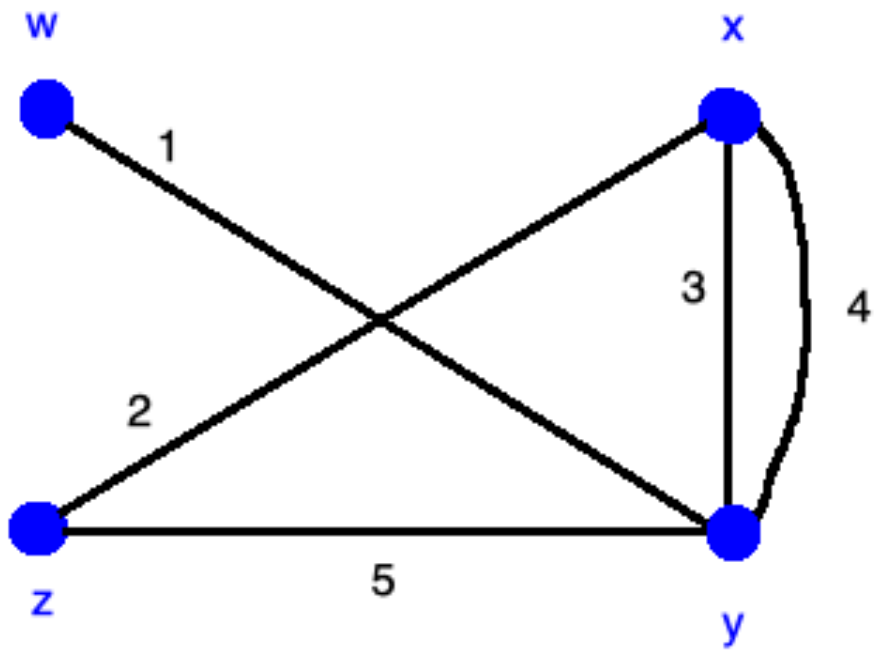
Many real-world problems concern objects and relations, eg. people with friendships, cities connected by highways, web pages linked to others, etc. Graph theory is the mathematical abstraction and analysis of these situations.

Definition

*A **graph** consists of a pair of finite sets: a nonempty set V of vertices and a set E of edges, where each edge is associated to a subset of V of either 1 or 2 vertices, called the endpoints of the edge.*

- An edge with just one endpoint is called a loop.
- Two edges with the same endpoints are called parallel edges.
- An edge is said to connect its endpoints and be incident on each endpoint.
- A vertex on which no edge is incident is called isolated.
- Two vertices connected by an edge are called adjacent.

Example. Write down V and E for the following graph. List any loops and parallel edges.



Example. Draw a graph that has 5 vertices including 1 isolated, 1 loop and 1 pair of parallel edges. Write down V and E.

Example. Draw a graph that has 5 vertices including 1 isolated, 1 loop and 1 pair of parallel edges. Write down V and E.

Definition

*A **simple graph** is a graph that does not have loops nor parallel edges.*

Example. Draw a graph that has 5 vertices including 1 isolated, 1 loop and 1 pair of parallel edges. Write down V and E.

Definition

*A **simple graph** is a graph that does not have loops nor parallel edges.*

Example. Draw a simple graph with $V = \{v_1, v_2, v_3, v_4\}$ and 2 edges, one of which has endpoints v_1 and v_2.

Definition

*A **complete graph** on n vertices, denoted by K_n, is a simple graph with n vertices whose edge set contains one edge for every pair of distinct vertices.*

Definition

*A **complete graph** on n vertices, denoted by K_n, is a simple graph with n vertices whose edge set contains one edge for every pair of distinct vertices.*

Example. Draw K_1, K_2, K_3, K_4 and K_5.

Definition

A simple graph is ***bipartite*** *if there exist* $U \subseteq V$ *and* $W \subseteq V$ *such that*

(a) $U \cup W = V$ *and* $U \cap W = \varnothing$;

(b) *every edge connects a vertex of* U *with a vertex of* W.

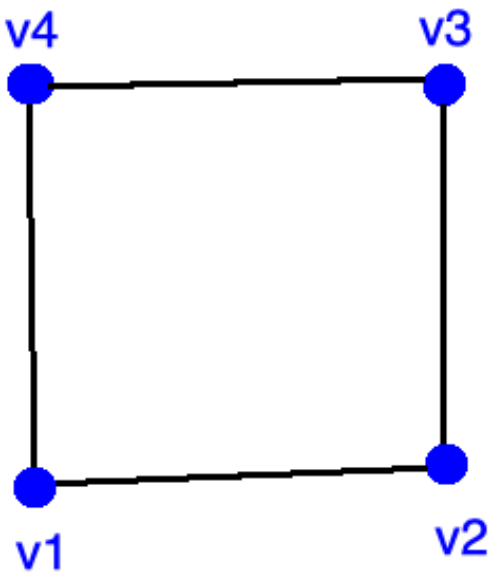
Definition

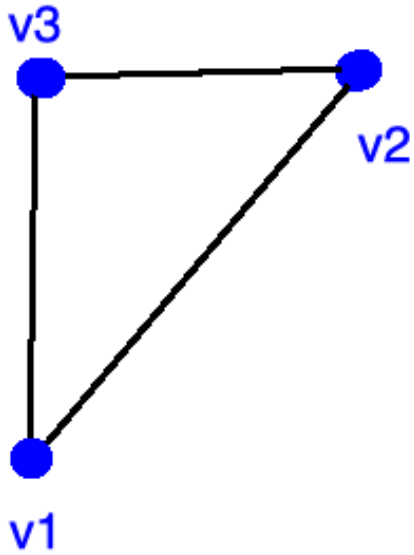
*A simple graph is **bipartite** if there exist $U \subseteq V$ and $W \subseteq V$ such that*

(a) $U \cup W = V$ *and* $U \cap W = \varnothing$;

(b) *every edge connects a vertex of U with a vertex of W.*

Example. Which are bipartite?





Definition

*A **complete bipartite graph** on (m, n) vertices, denoted by $K_{m,n}$, is a simple graph with $V = \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$ such that for all $1 \leq i, k \leq m$ and all $1 \leq j, l \leq n$ we have*

1. *an edge from each v_i to each w_j;*
2. *no edge from any v_i to any v_k;*
3. *no edge from any w_j to any w_l.*

Definition

*A **complete bipartite graph** on (m, n) vertices, denoted by $K_{m,n}$, is a simple graph with $V = \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$ such that for all $1 \leq i, k \leq m$ and all $1 \leq j, l \leq n$ we have*

1. *an edge from each v_i to each w_j;*
2. *no edge from any v_i to any v_k;*
3. *no edge from any w_j to any w_l.*

Example. Draw $K_{3,2}$ and $K_{3,3}$.

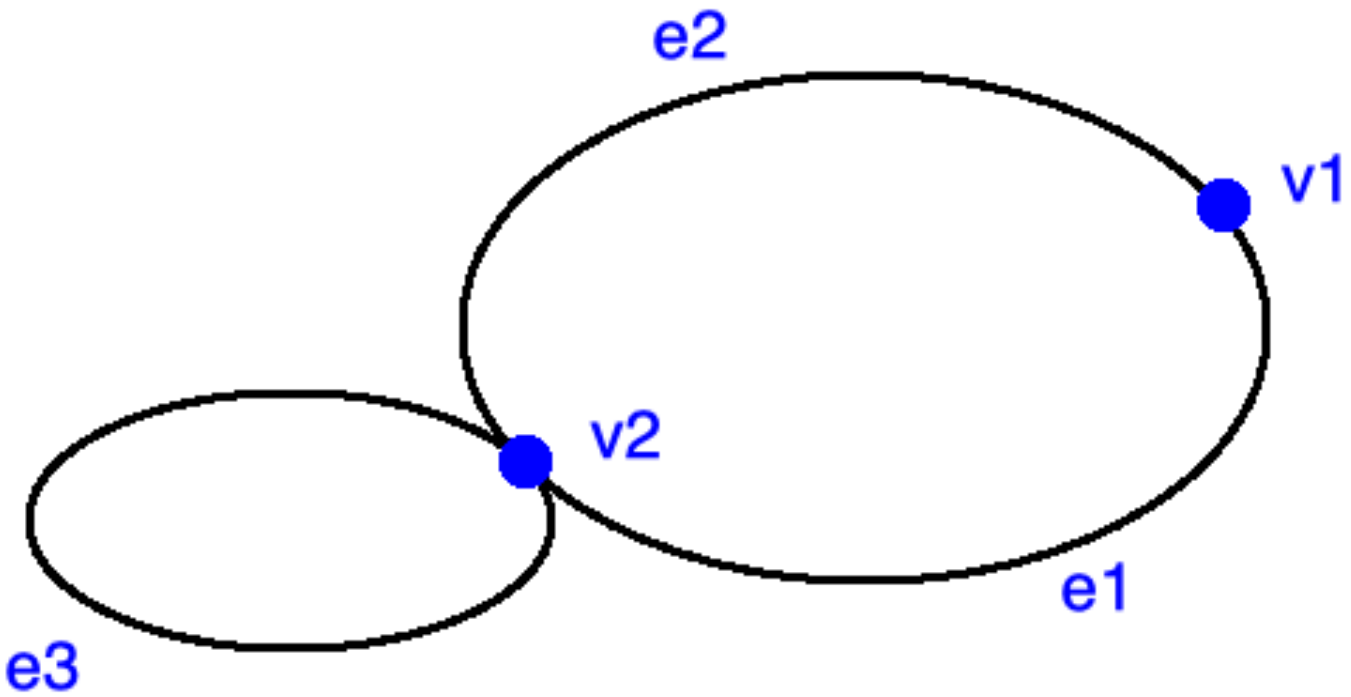
Definition

*A graph H is a **subgraph** of a graph G if every vertex in H is in G, every edge in H is in G and every edge in H has the same endpoints in G.*

Definition

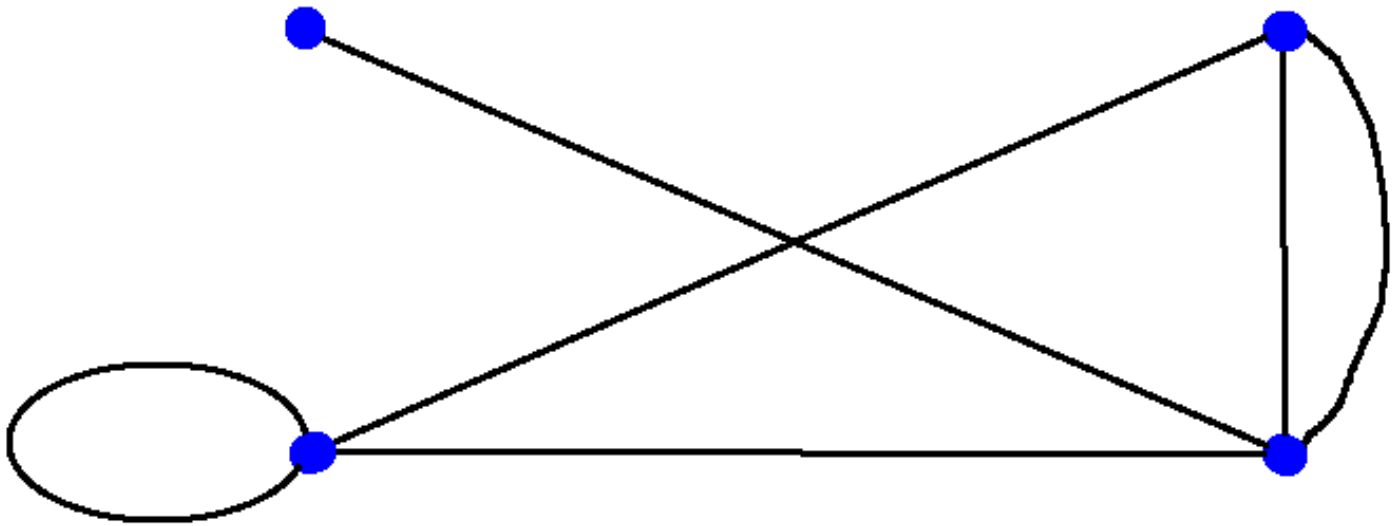
*A graph H is a **subgraph** of a graph G if every vertex in H is in G, every edge in H is in G and every edge in H has the same endpoints in G.*

Example. Draw all the subgraphs of the graph below.



Example. From the following graph, draw

1. two different simple subgraphs with 3 vertices;
2. a non-simple subgraph with 1 vertex;
3. a subgraph with no edges.



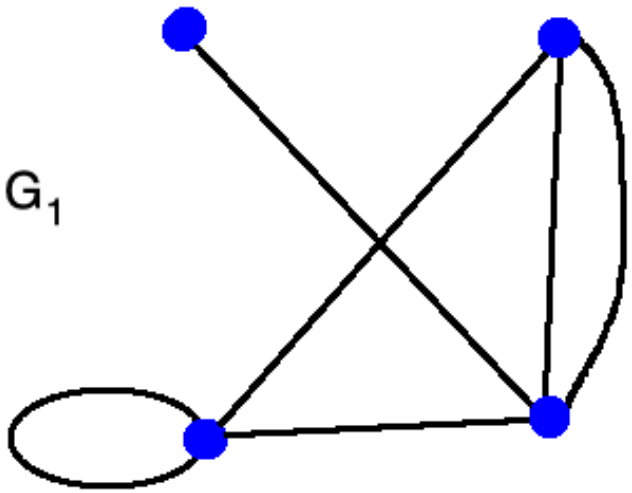
Definition

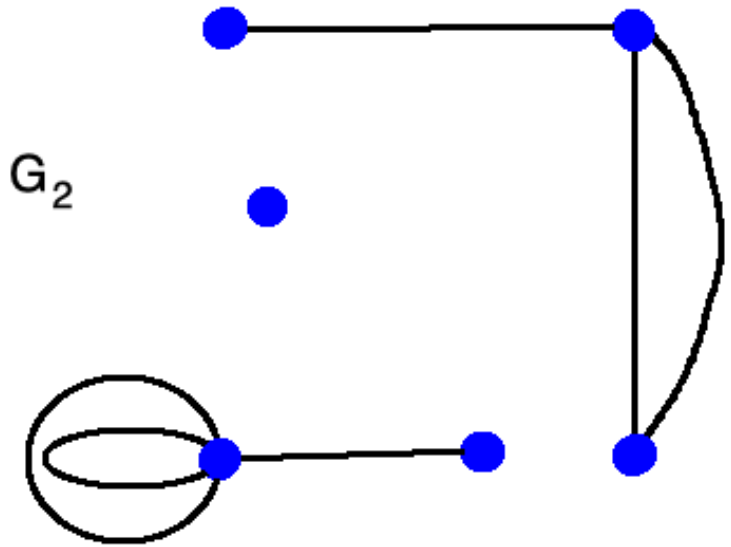
*Let $G = (V, E)$ be a graph, $v \in V$. The **degree** of v, denoted by $\delta(v)$, is the number of edges incident on v (with loops counted twice). The degree of G is the sum of degrees of all $v \in V$.*

Definition

*Let $G = (V, E)$ be a graph, $v \in V$. The **degree** of v, denoted by $\delta(v)$, is the number of edges incident on v (with loops counted twice). The degree of G is the sum of degrees of all $v \in V$.*

Example. Find the degrees of G_1 and G_2.





Example. Draw graphs with $|V| = 4$ and vertices of degrees

- 1,1,3,3;
- 1,1,2,3.

Example. Draw graphs with $|V| = 4$ and vertices of degrees

- 1,1,3,3;
- 1,1,2,3.

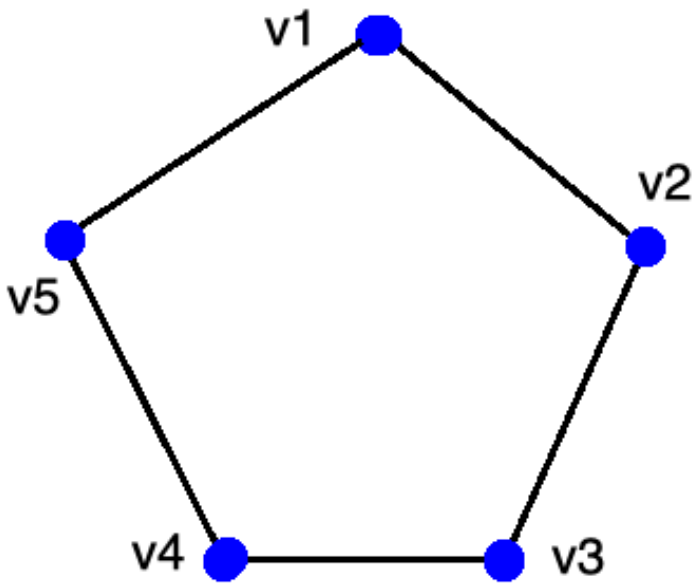
Theorem (The Handshake Theorem)

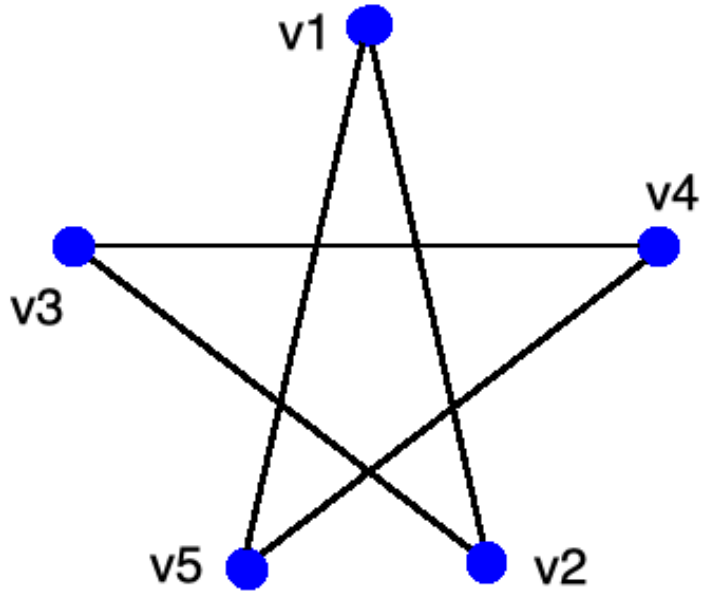
The degree of a graph is twice the number of its edges.

This holds because each edge has 2 endpoints. So the degree of a graph is always even. A graph with 4 vertices of degrees 1,1,2,3 is impossible.

Isomorphic Graphs

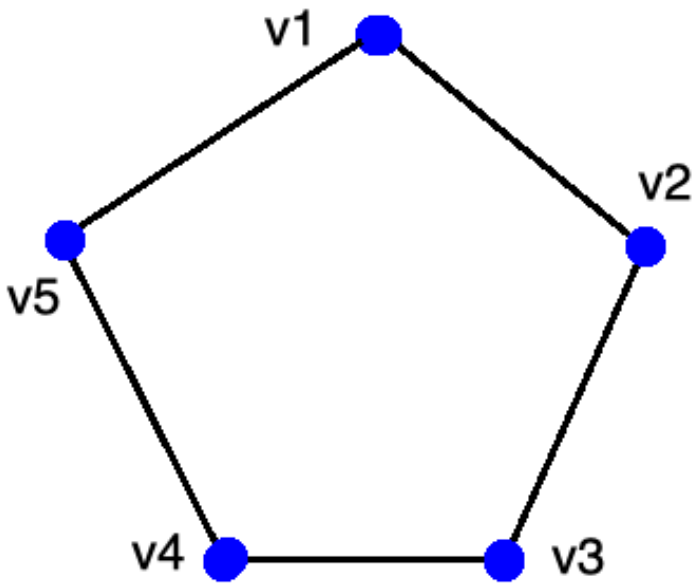
Is there a difference between these 2 graphs?

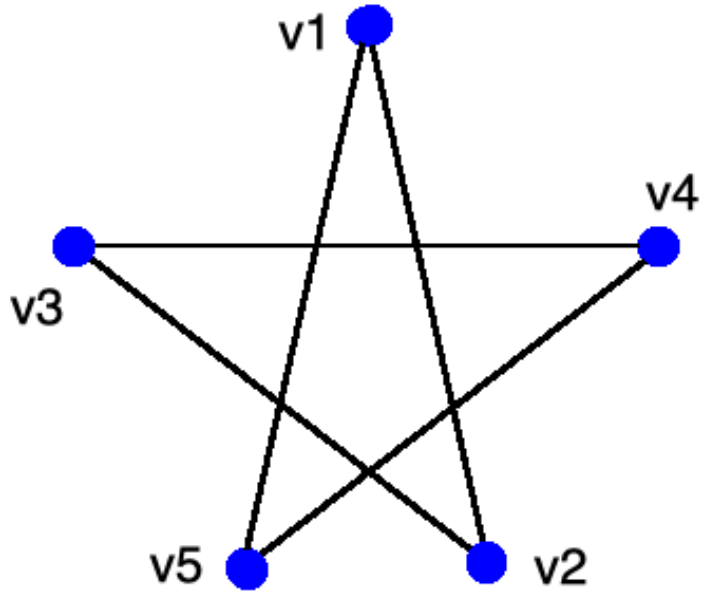




Isomorphic Graphs

Is there a difference between these 2 graphs?

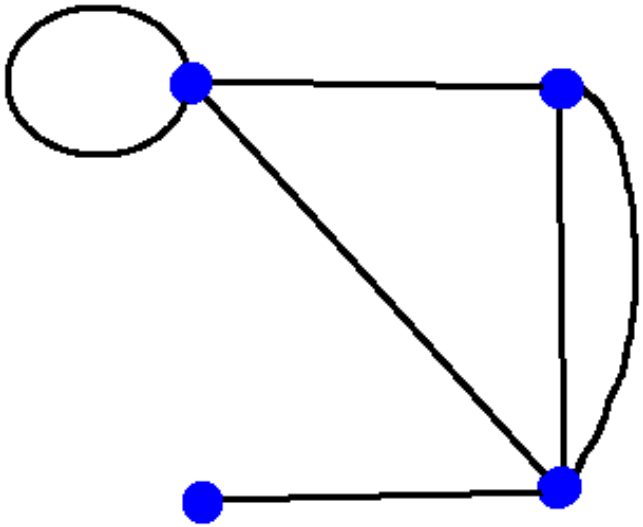


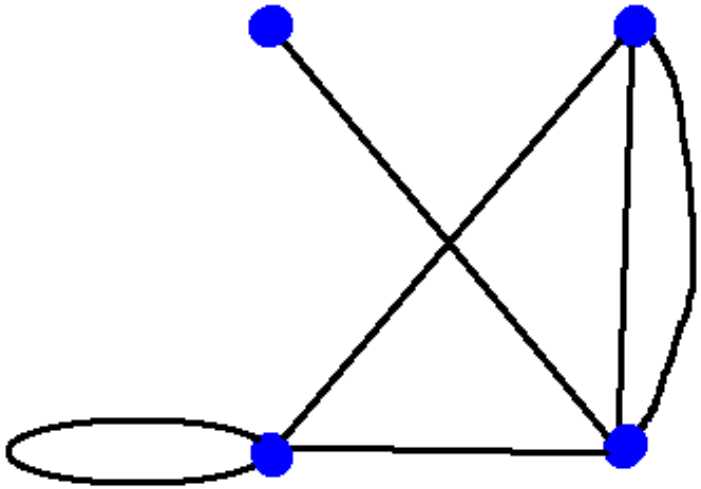


Definition

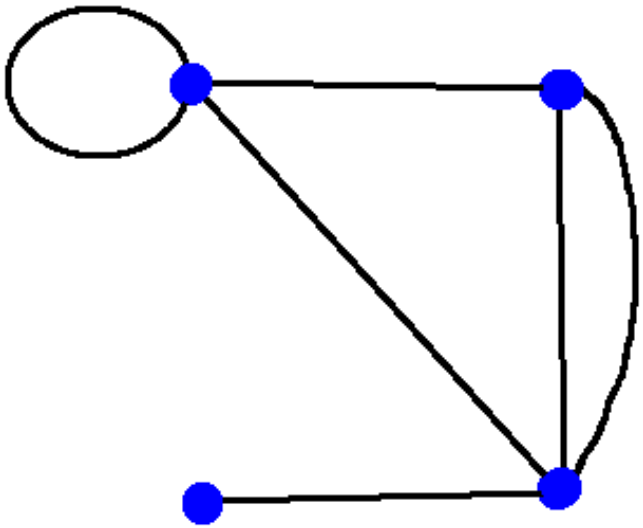
Let $G = (V, E)$, $G' = (V', E')$ be graphs. We say that G is ***isomorphic*** *to G' if there exist bijective functions $f : V \to V'$ and $h : E \to E'$ that preserve adjacency, that is, v is an endpoint of $e \Leftrightarrow f(v)$ is an endpoint of $h(e)$ $\forall\ v \in V, \forall\ e \in E$.*

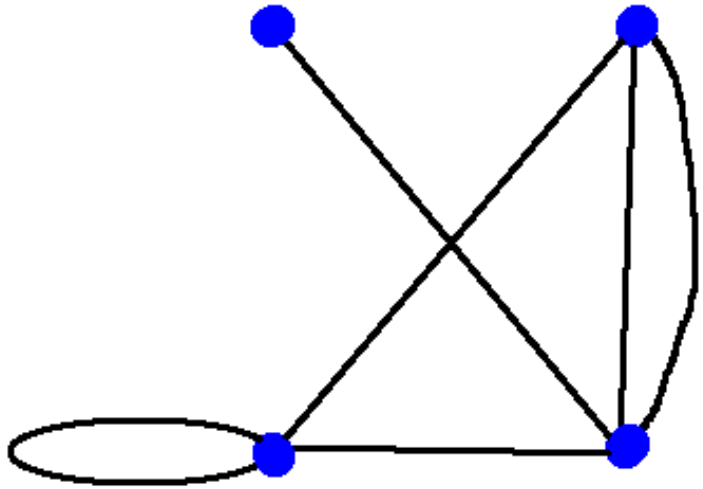
Example. Show that these two graphs are isomorphic.





Example. Show that these two graphs are isomorphic.

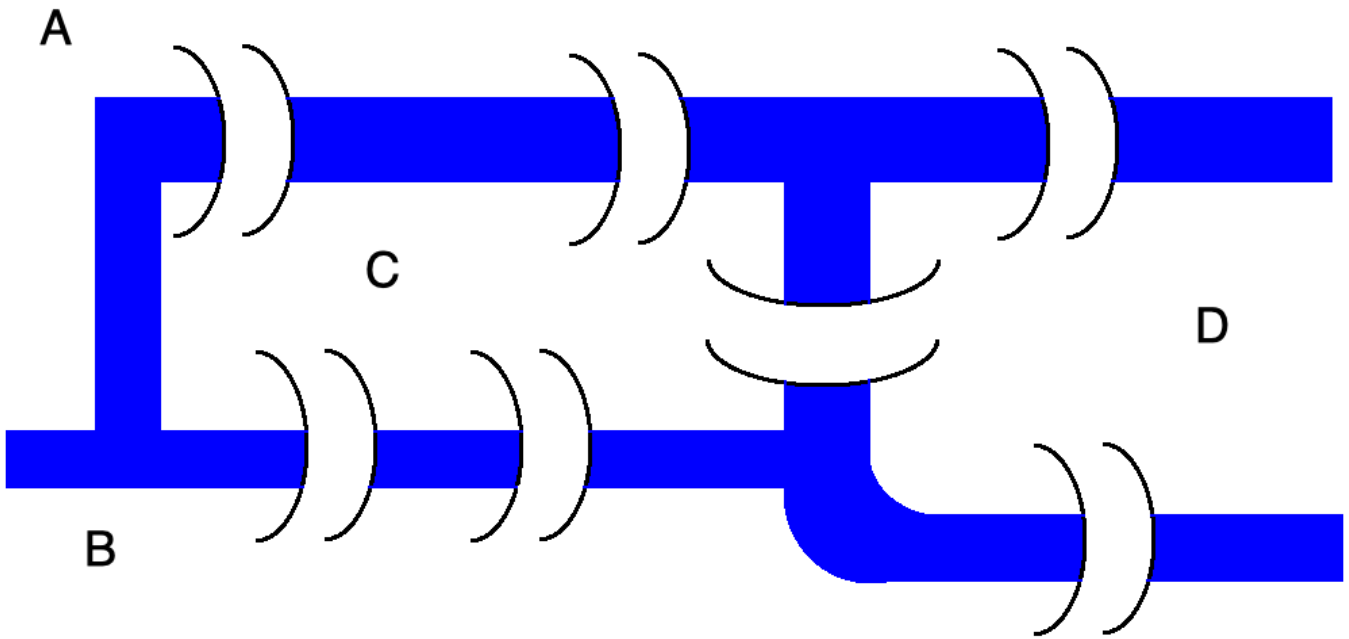




Example. Draw all possible graphs (up to isomorphism) with $|V| = |E| = 2$.

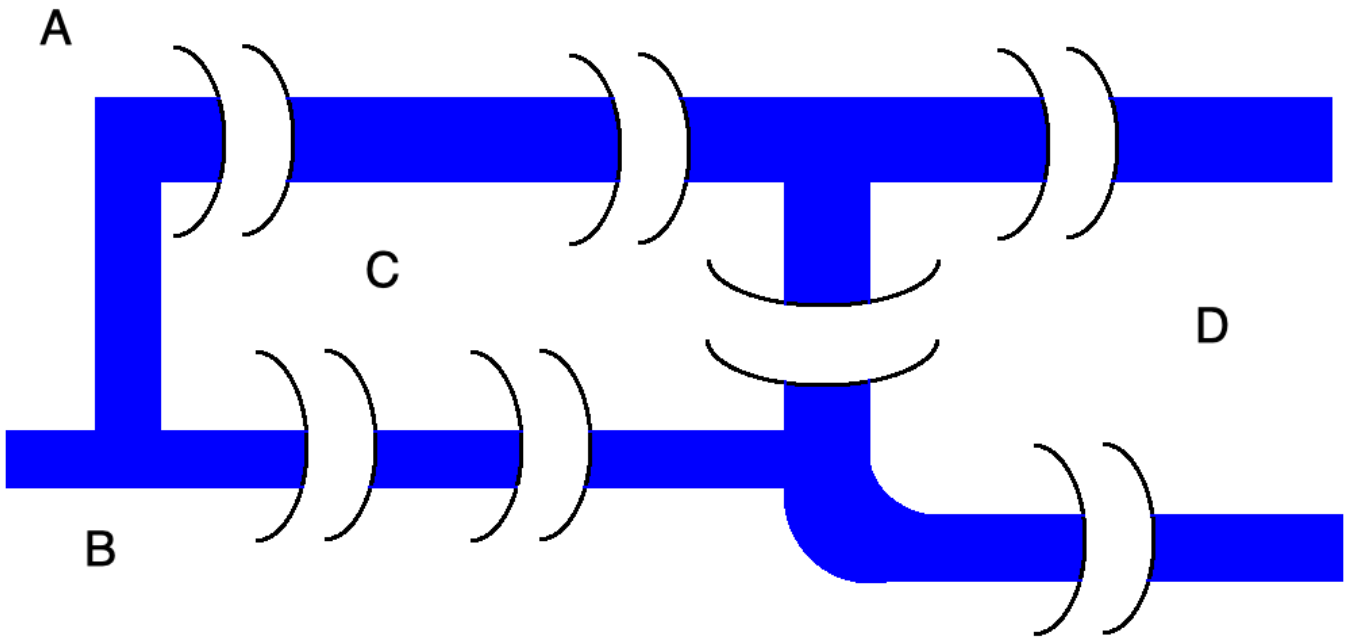
The Königsberg bridge problem

In 1736, graph theory was invented by considering the following problem.



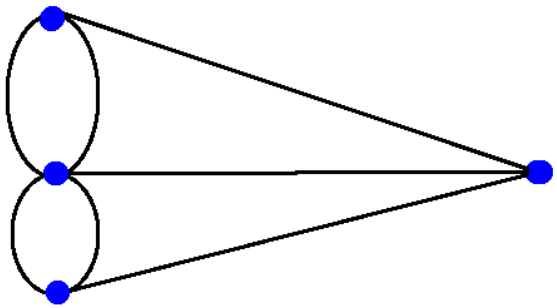
The Königsberg bridge problem

In 1736, graph theory was invented by considering the following problem.



Is it possible for one to walk in Könisberg, starting and ending at the same point, and crossing each bridge exactly once?

The problem can be translated to a graph: bridges are edges and regions A, B, C, D are vertices.



Is it possible to find a route through the graph that starts and ends at the same vertex and traverses each edge exactly once?

Walks, Paths and Circuits

1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.

Walks, Paths and Circuits

1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.
2. A **trail** is a walk that does not contain a repeated edge.

Walks, Paths and Circuits

1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.
2. A **trail** is a walk that does not contain a repeated edge.
3. A **path** is a trail that does not contain a repeated vertex.

Walks, Paths and Circuits

1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.
2. A **trail** is a walk that does not contain a repeated edge.
3. A **path** is a trail that does not contain a repeated vertex.
4. A **circuit** is a walk whose first and last vertices are the same.

Walks, Paths and Circuits

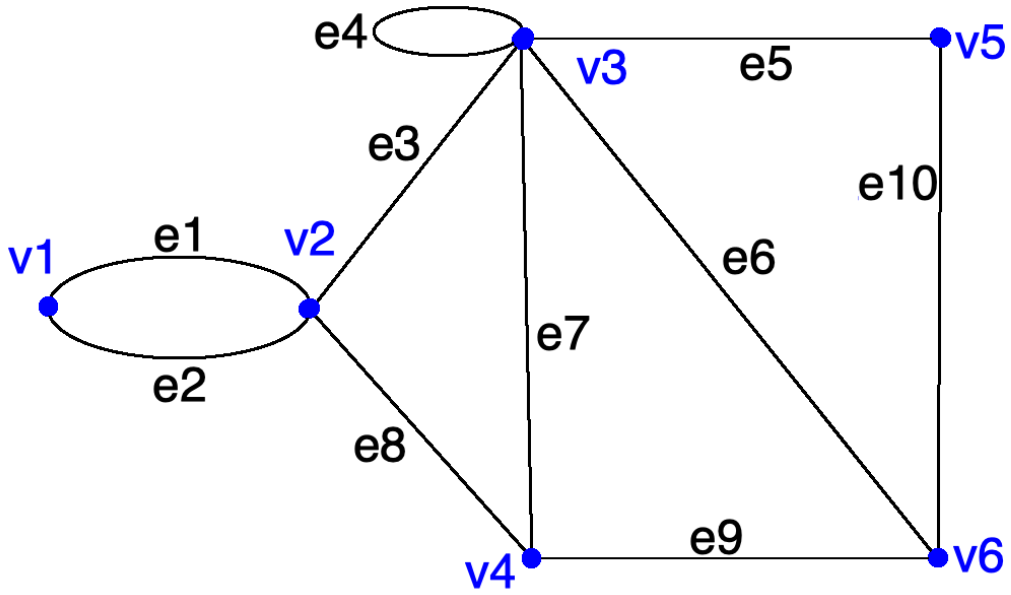
1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.
2. A **trail** is a walk that does not contain a repeated edge.
3. A **path** is a trail that does not contain a repeated vertex.
4. A **circuit** is a walk whose first and last vertices are the same.
5. A **simple circuit** is a trail whose first and last vertices are the same.

Walks, Paths and Circuits

1. A **walk** from vertex v_0 to vertex v_n in G is a finite alternating sequence of adjacent vertices and edges of G that starts at v_0 and ends at v_n: $v_0 e_1 v_2 e_2 \cdots v_{n-1} e_n v_n$. The length of the walk is the number of edges in the sequence.
2. A **trail** is a walk that does not contain a repeated edge.
3. A **path** is a trail that does not contain a repeated vertex.
4. A **circuit** is a walk whose first and last vertices are the same.
5. A **simple circuit** is a trail whose first and last vertices are the same.

Note. If it is not ambiguous, a walk can be denoted by a sequence of only vertices or only edges.

Example. Are the following walks, trails, paths, circuits or simple circuits?



(1) $v_1\, e_1\, v_2\, e_3\, v_3\, e_4\, v_3\, e_5\, v_5$

(2) $e_1\, e_3\, e_4\, e_4\, e_6$

(3) $v_2\, v_3\, v_4\, v_6$

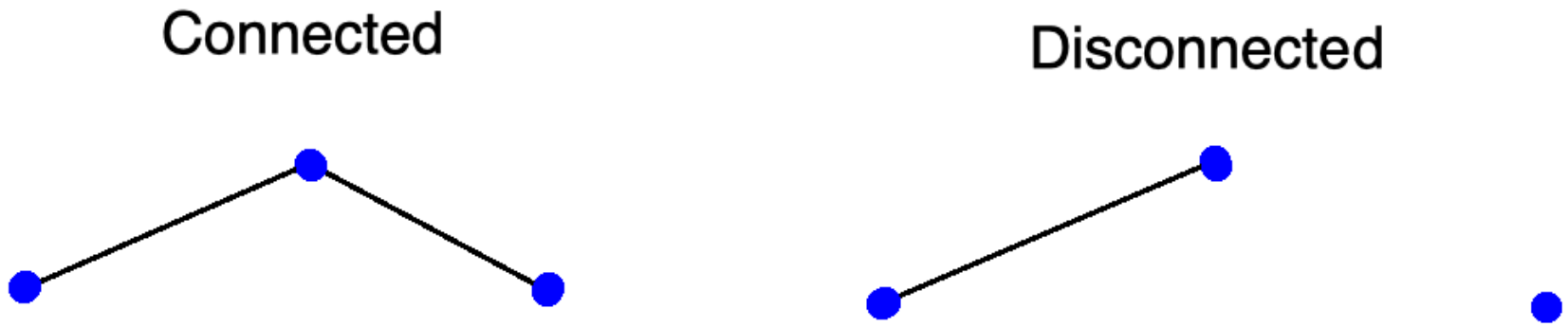
(4) $v_2\, v_3\, v_4\, v_2$

(5) $v_1\, e_1\, v_2\, e_1\, v_1$

(6) v_1

Definition

*Vertices v, w in G are **connected** if there exists a walk from v to w. The graph G is connected is there exists a walk between every pair of vertices. Otherwise, G is **disconnected**.*

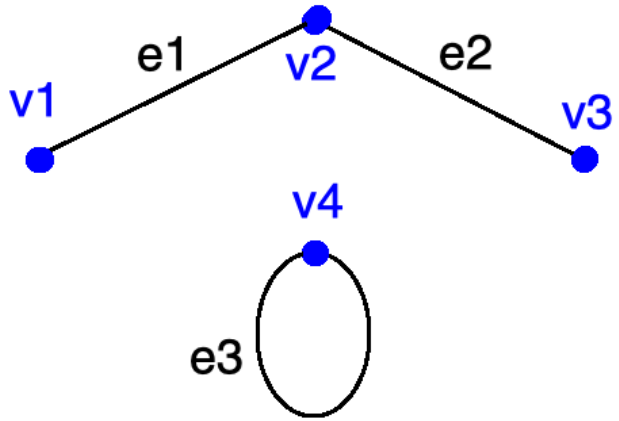


A graph H is a connected component of G if

1. H is a subgraph of G,
2. H is connected and
3. no connected subgraph of G has H as a subgraph and contains a vertex or an edge outside H.

A graph H is a connected component of G if

1. H is a subgraph of G,
2. H is connected and
3. no connected subgraph of G has H as a subgraph and contains a vertex or an edge outside H.



$(\{v_1, v_2, v_3\}, \{e_1, e_2\})$ is a connected component.
$(\{v_1, v_2\}, \{e_1\})$ is not.

Definition

1. *An **Eulerian circuit** of G is a simple circuit that contains every edge and every vertex. If such a circuit exists, G is an **Eulerian graph**.*
2. *An **Eulerian path** from v to w is a path from v to w that passes through every vertex at least once and every edge exactly once.*

Theorem

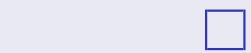
If G is an Eulerian graph, then every vertex of G has even degree.

Corollary

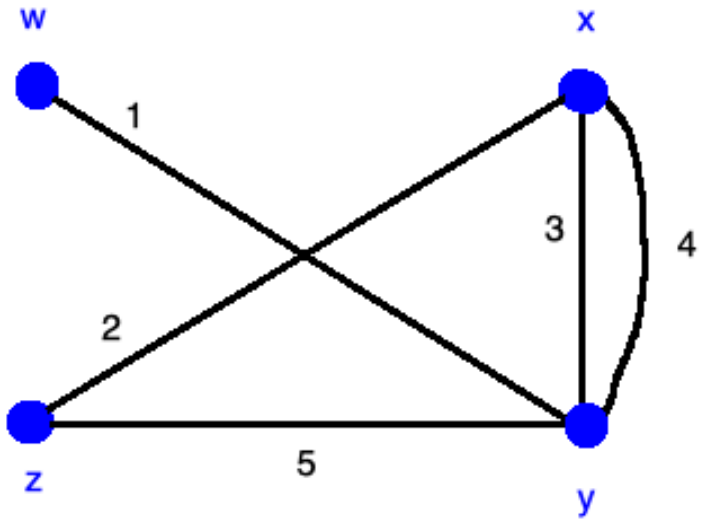
If some vertex of G has odd degree, then G is not an Eulerian graph.

Proof.

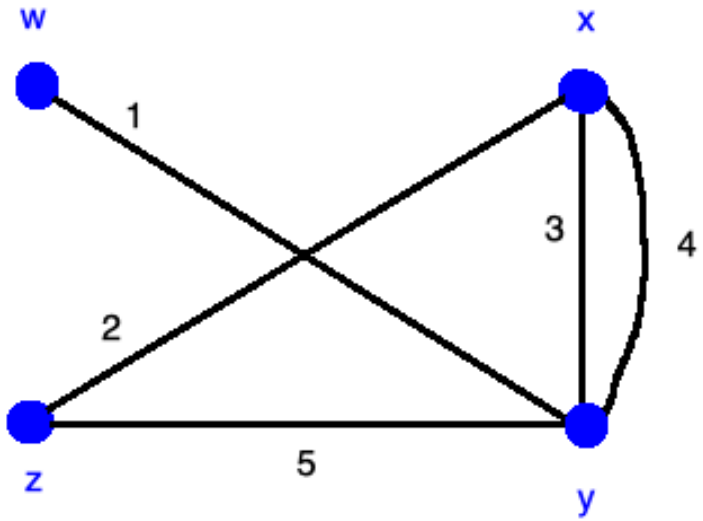
- G has an Eulerian circuit, which uses each edge exactly once.
- Beginning at vertex v, follow the circuit. As the circuit passes through a vertex w, it uses 2 edges: one to arrive at w and another to leave. Each edge is used only once, so w uses an even number of incident edge endpoints.
- The starting point v has even degree as well, since the circuit begins by leaving v, then uses v an even number of times as above, then ends by arriving at v.
- The corollary is the contrapositive of the theorem.



Example. Does the following graph have an Eulerian circuit? An Eulerian path?



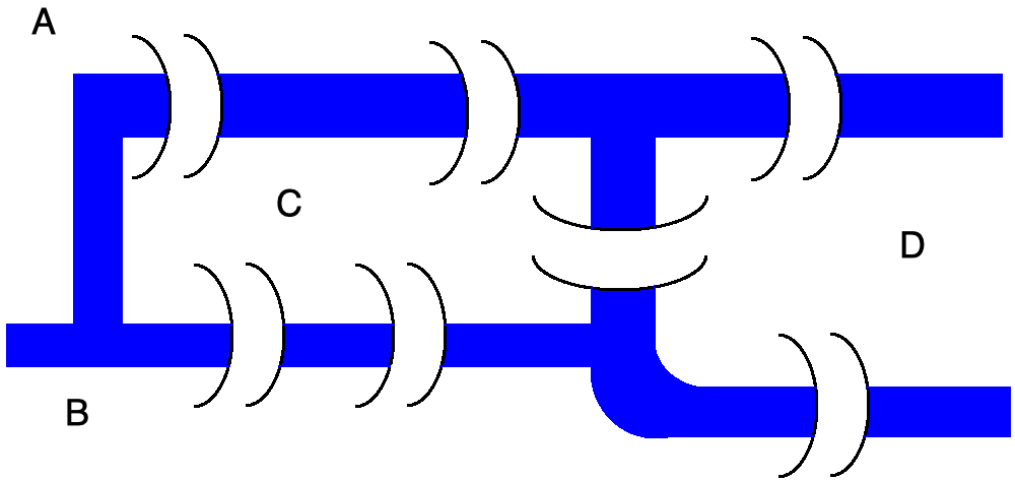
Example. Does the following graph have an Eulerian circuit? An Eulerian path?

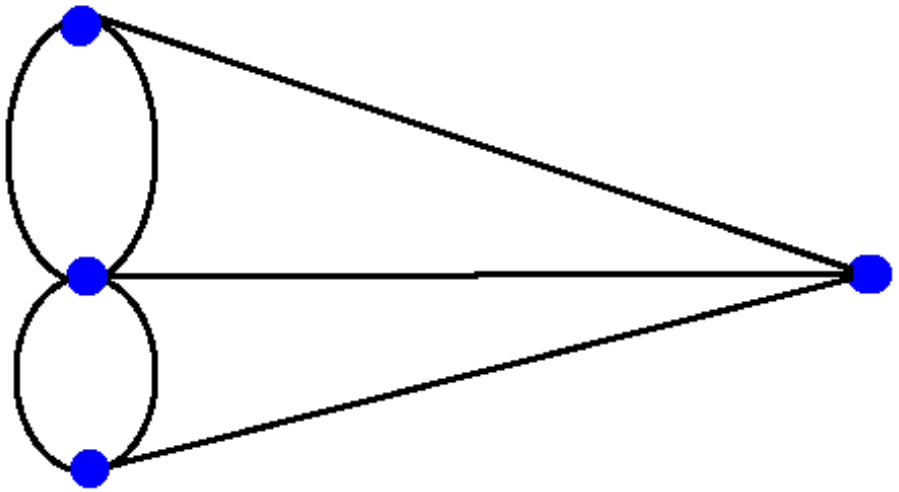


Theorem (Euler's Theorem)

In a connected graph, the degree of every vertex is even and positive iff the graph is Eulerian.

Example. Solve the Königsberg bridge problem.





Definition

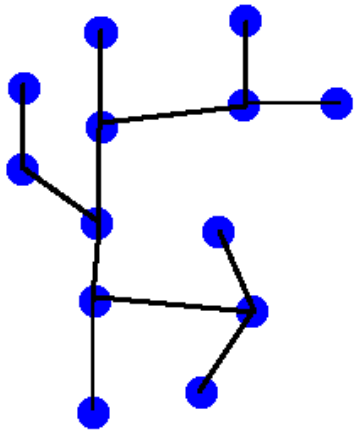
*A graph is a **tree** if it is connected and has no circuits.*

Definition

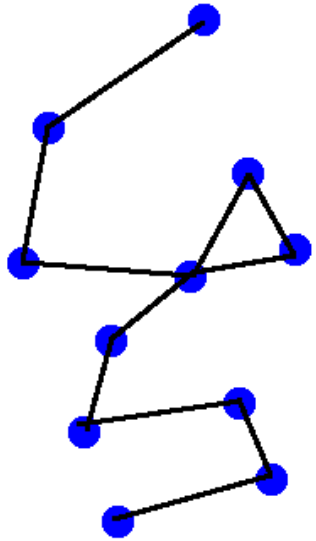
*A graph is a **tree** if it is connected and has no circuits.*

Example. Which are trees?

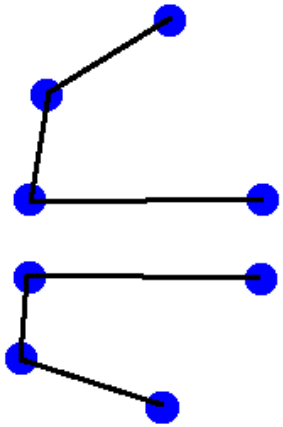
(a)



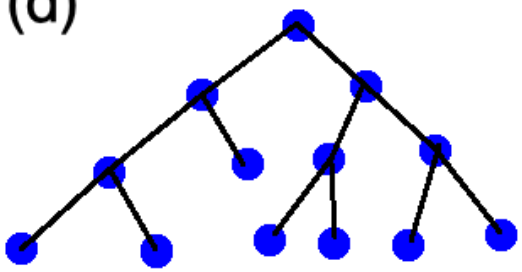
(b)



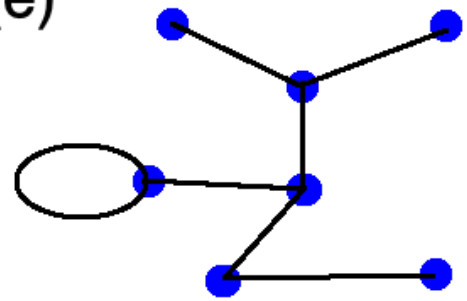
(c)



(d)



(e)



(f)

Theorem

For any $n \in \mathbb{N}$, a tree with n vertices has $n - 1$ edges.

Theorem

For any $n \in \mathbb{N}$, if G is connected with $|V| = n$ and $|E| = n - 1$, then G is a tree.

Theorem

For any $n \in \mathbb{N}$, a tree with n vertices has $n - 1$ edges.

Theorem

For any $n \in \mathbb{N}$, if G is connected with $|V| = n$ and $|E| = n - 1$, then G is a tree.

Example. (a) Draw a tree with 5 vertices and 4 edges.

(b) Draw a graph with 5 vertices and 4 edges that is not a tree.

Definition

*A **spanning tree** of G is a subgraph that contains every vertex of G and is a tree.*

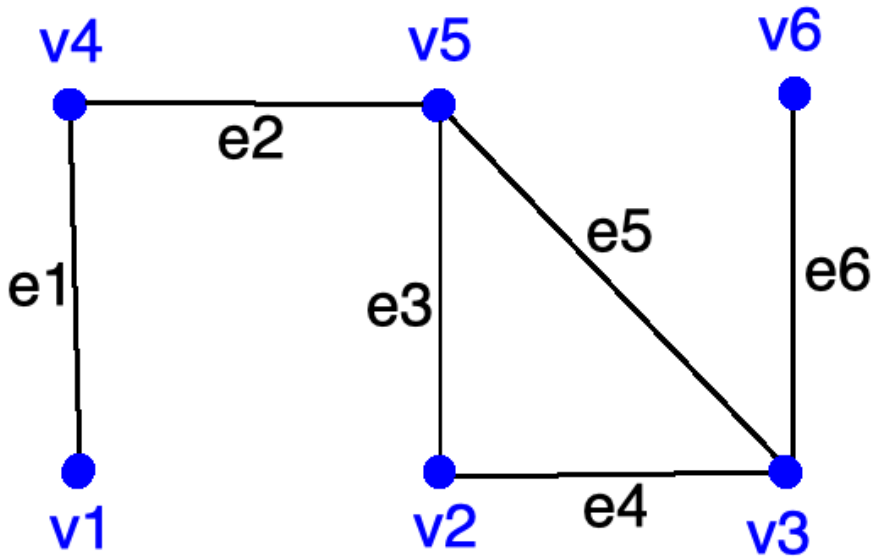
- Every connected graph has a spanning tree.
- Any two spanning trees of a graph have the same number of edges.

Definition

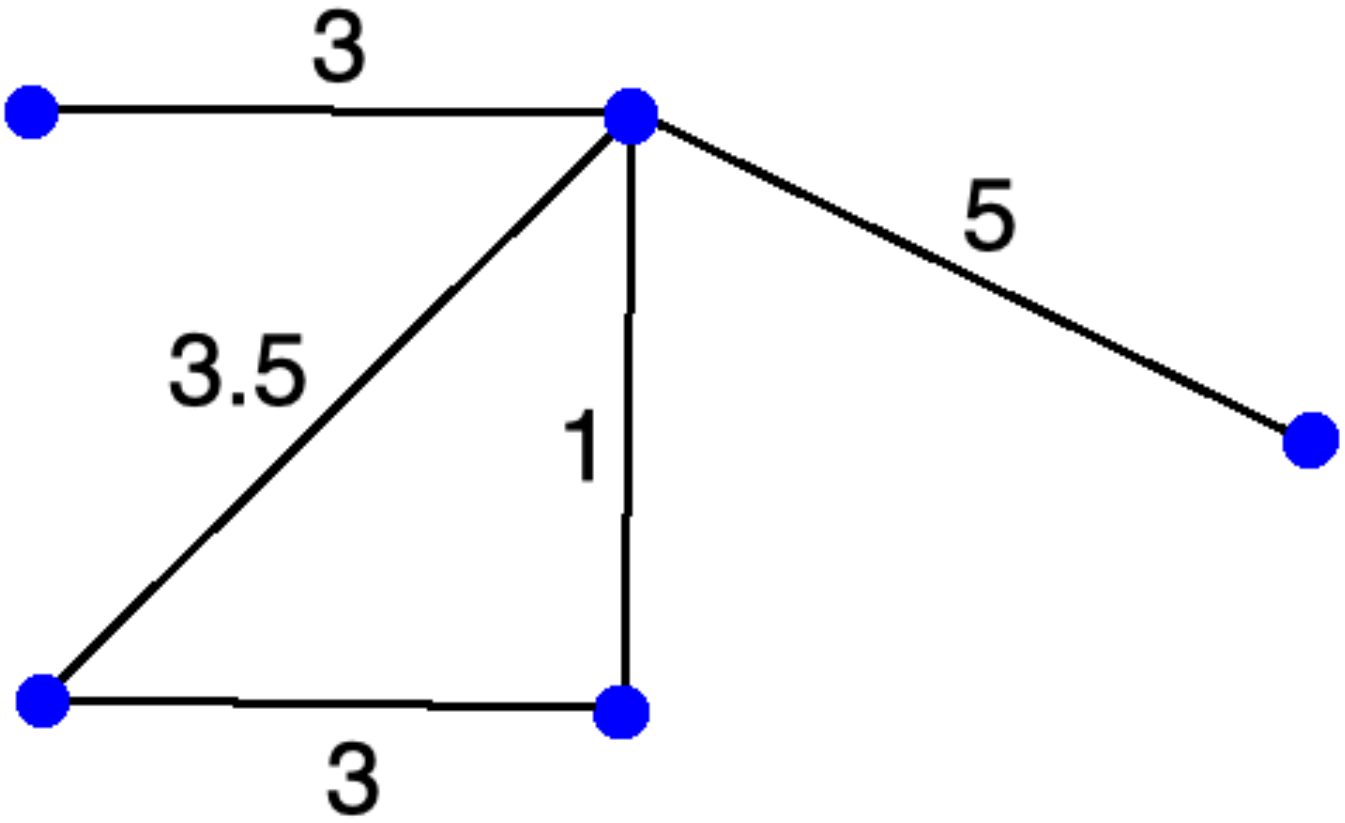
*A **spanning tree** of G is a subgraph that contains every vertex of G and is a tree.*

- Every connected graph has a spanning tree.
- Any two spanning trees of a graph have the same number of edges.

Example. Find all spanning trees.



Example. Let the edges represent telephone lines, the numbers represent the cost in thousands of installation. Determine the minimum cost of installing the network.



Definition

*A **weighted graph** is a graph for which each edge has an associated positive weight. The sum of edge weights is the **weight** of the graph.*

Definition

*A **weighted graph** is a graph for which each edge has an associated positive weight. The sum of edge weights is the **weight** of the graph.*

A **minimum spanning tree** for a connected, weighted graph is a spanning tree that has the least possible weight. Minimum spanning trees are not necessarily unique. We use $w(e)$ and $w(G)$ for the weights of edge e and graph G.

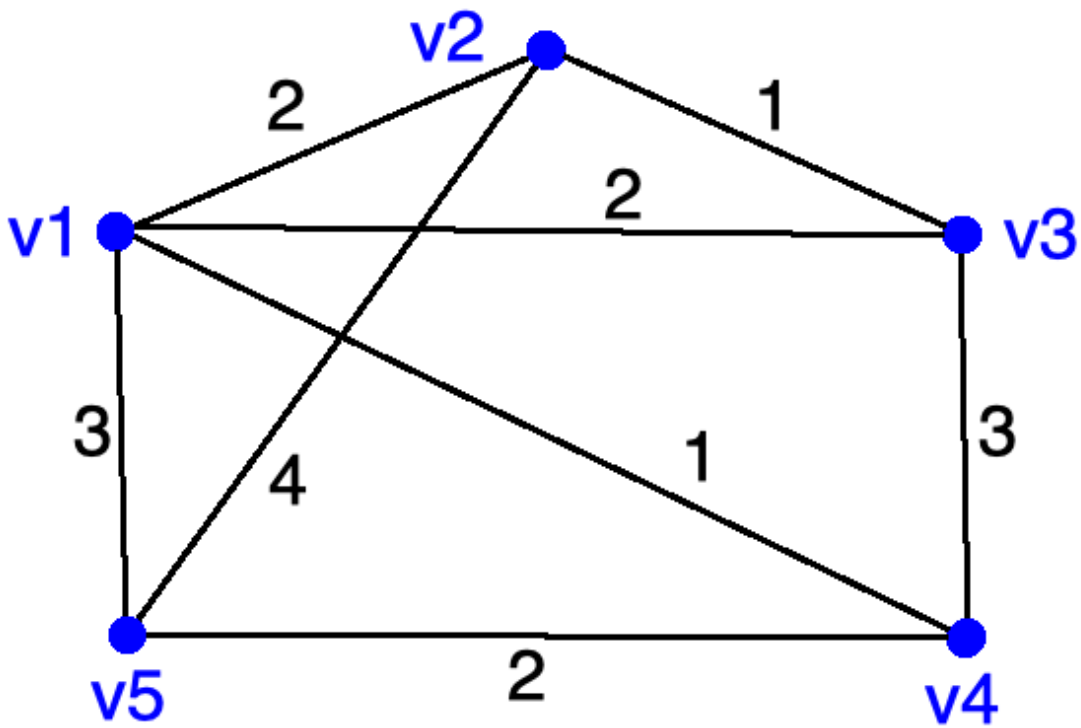
Kruskal's Algorithm

To find a minimum spanning tree, the edges are examined in order of increasing weight. At each step, we add an edge to the tree, one that does not create a circuit.

Kruskal's Algorithm

To find a minimum spanning tree, the edges are examined in order of increasing weight. At each step, we add an edge to the tree, one that does not create a circuit.

Example. Find a minimum spanning tree.



Edge	Weight	Circuit?	Action	Total

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4

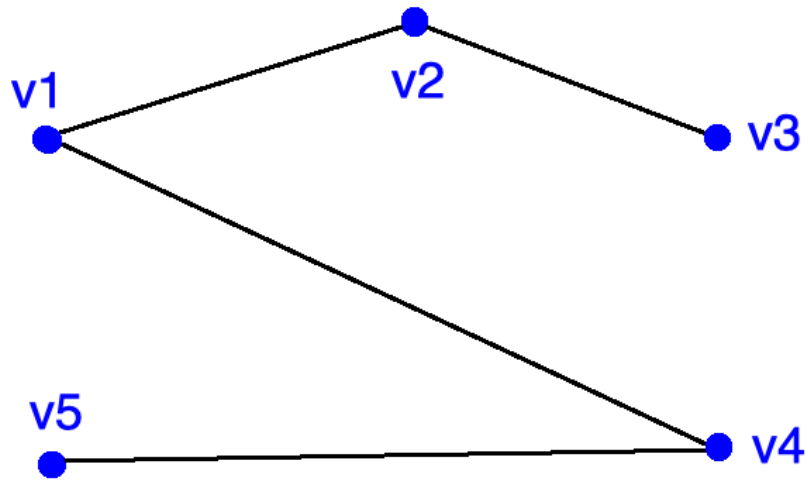
Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6
v_1v_5	3	Yes	Skip	6

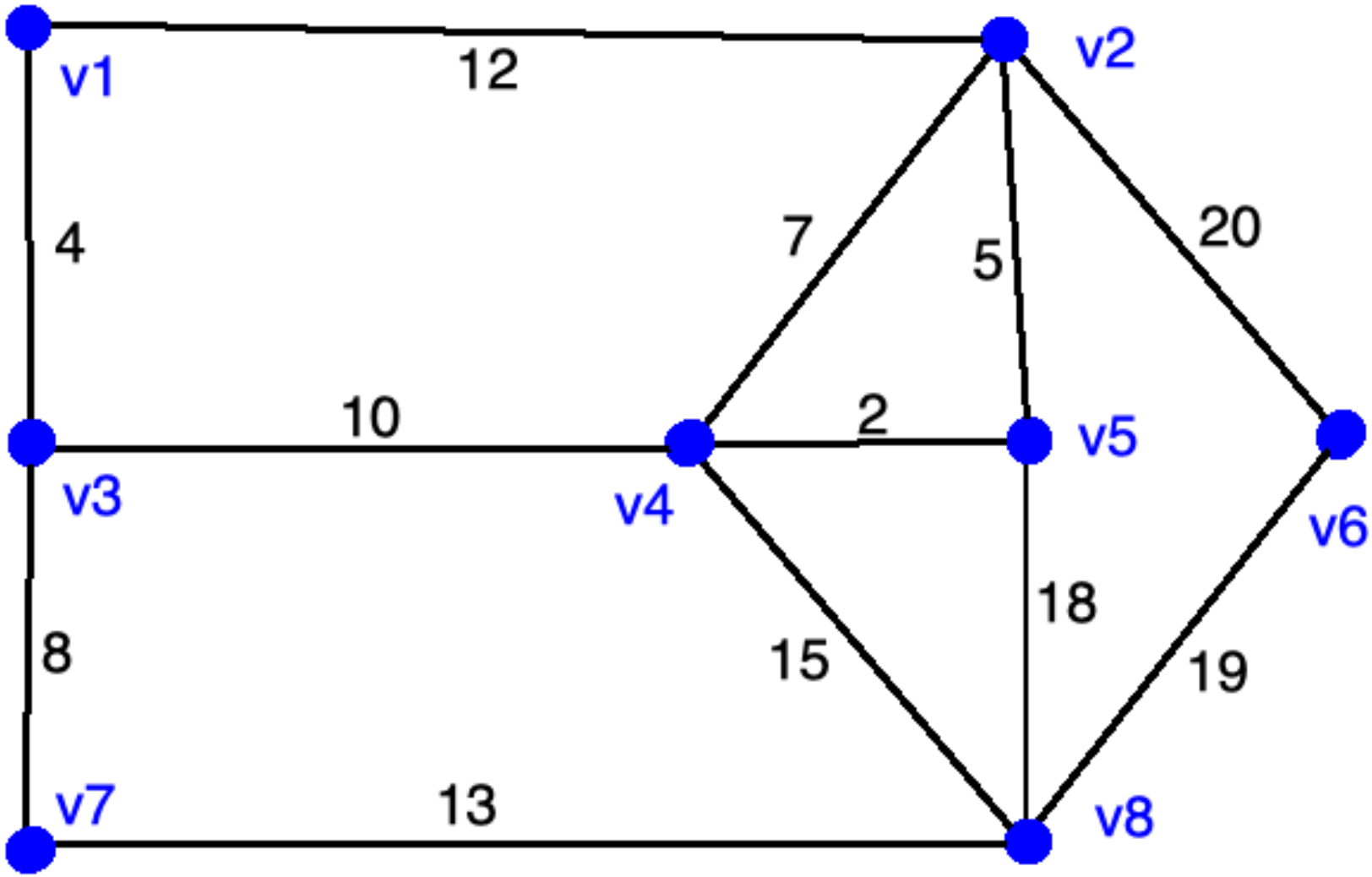
Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6
v_1v_5	3	Yes	Skip	6
v_3v_4	3	Yes	Skip	6

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6
v_1v_5	3	Yes	Skip	6
v_3v_4	3	Yes	Skip	6
v_2v_5	4	Yes	Skip	6

Edge	Weight	Circuit?	Action	Total
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_2	2	No	Add	4
v_1v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6
v_1v_5	3	Yes	Skip	6
v_3v_4	3	Yes	Skip	6
v_2v_5	4	Yes	Skip	6



Example. Find a minimum spanning tree.



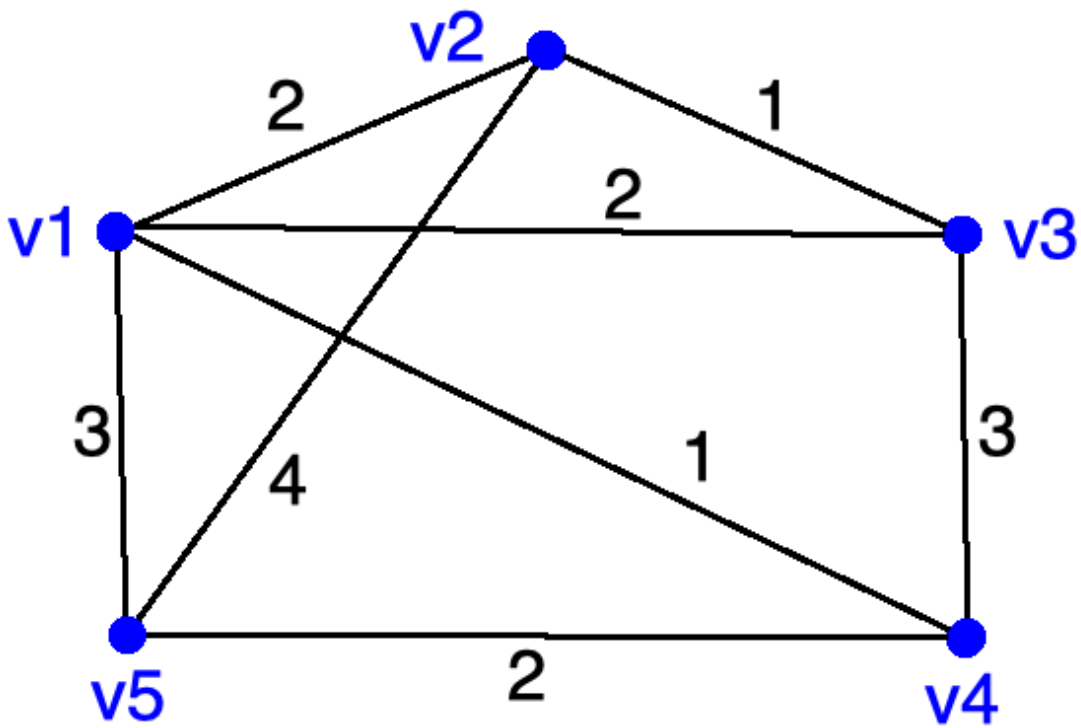
Prim's Algorithm

Build a minimum spanning tree by choosing a vertex and expanding outwards adding one edge and one vertex at each step.

Prim's Algorithm

Build a minimum spanning tree by choosing a vertex and expanding outwards adding one edge and one vertex at each step.

Example. Find a minimum spanning tree.



Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total

Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total
v_4	$v_1 v_4$	1	1

Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total
v_4	$v_1 v_4$	1	1
v_3	$v_1 v_3$	2	3

Start with (arbitrarily) v_1.

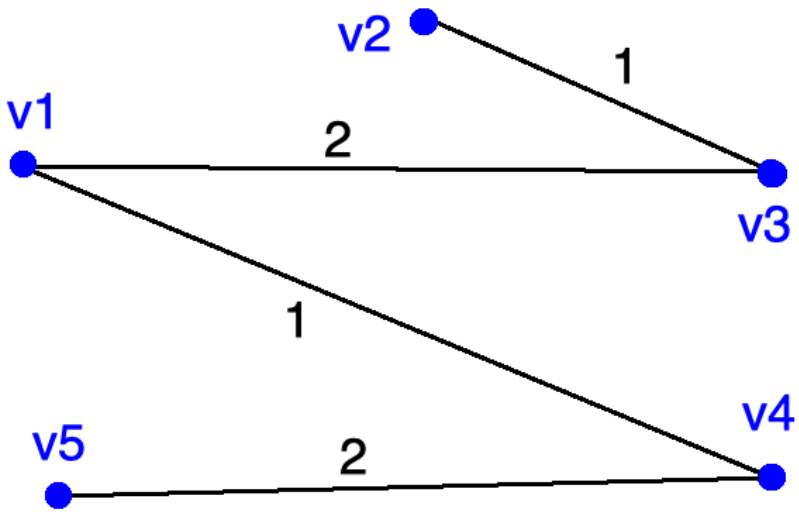
Vertex	Edge	Weight	Total
v_4	v_1v_4	1	1
v_3	v_1v_3	2	3
v_2	v_2v_3	1	4

Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total
v_4	v_1v_4	1	1
v_3	v_1v_3	2	3
v_2	v_2v_3	1	4
v_5	v_4v_5	2	6

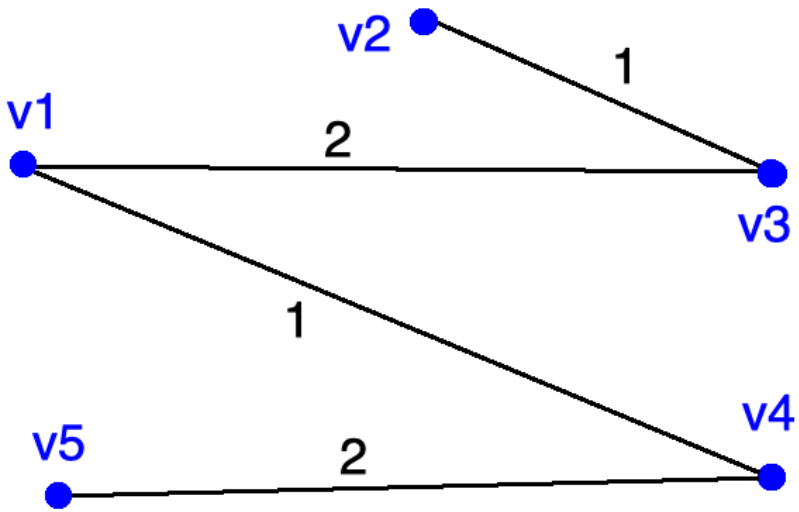
Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total
v_4	$v_1 v_4$	1	1
v_3	$v_1 v_3$	2	3
v_2	$v_2 v_3$	1	4
v_5	$v_4 v_5$	2	6



Start with (arbitrarily) v_1.

Vertex	Edge	Weight	Total
v_4	v_1v_4	1	1
v_3	v_1v_3	2	3
v_2	v_2v_3	1	4
v_5	v_4v_5	2	6



Exercise. Repeat the last exercise with Prim's Algorithm.

Chapter 8:

Probability

Probabililty

- **Random phenomenon:** cannot be predicted with certainty.
- **Outcome:** single observed result of random phenomenon.
- **Sample space:** set of all possible outcomes.
- **Empty set:** set containing no outcomes.
- **Event:** subset of sample space.

Definition

*The **probability** of an event is a number* $0 \leq p \leq 1$ *that describes how likely it is that the event occurs. An event of probability 1 will happen for sure; an event of probability 0 will certainly not happen.*

- $P(S) = 1$, as the sample space includes all possibilities.
- $P(\varnothing) = 0$, as $\varnothing$ contains no possibilities.
- If all outcomes are equally likely, then $P(E) = \frac{|E|}{|S|}$, where $|X|$ is the number of outcomes in X.
- Some probabilities can be calculated; others found experimentally as long-run proportions. They can be added, provided they are *disojint* (mutually exclusive).

Example: A coin is tossed twice; the sequence of heads and tails is recorded. $S = \{HH, HT, TH, TT\}$. Let $E = \{HH, TT\}$ denote the event "same result for both tosses".

- $P(S) = 1$, as the sample space includes all possibilities.
- $P(\varnothing) = 0$, as $\varnothing$ contains no possibilities.
- If all outcomes are equally likely, then $P(E) = \frac{|E|}{|S|}$, where $|X|$ is the number of outcomes in X.
- Some probabilities can be calculated; others found experimentally as long-run proportions. They can be added, provided they are *disojint* (mutually exclusive).

Example: A coin is tossed twice; the sequence of heads and tails is recorded. $S = \{HH, HT, TH, TT\}$. Let $E = \{HH, TT\}$ denote the event "same result for both tosses".Since all 4 outcomes have equal probability,

$$P(E) = \frac{|E|}{|S|} = \frac{2}{4} = \frac{1}{2}.$$

Example: The probabilities that a random student obtains grades in MATH223 are the following.

F	P	C	D	HD
0.2	0.35	0.2	0.15	0.1

Let E denote the event "credit or better".

Example: The probabilities that a random student obtains grades in MATH223 are the following.

F	P	C	D	HD
0.2	0.35	0.2	0.15	0.1

Let E denote the event "credit or better".Then

$$P(E) = 0.2 + 0.15 + 0.1 = 0.45.$$

This is valid because events $\{C\}$,$\{D\}$ and $\{HD\}$ are disjoint (non-overlapping).

Example: 2 fair dice are rolled. What is the probability that the sum of faces is 4?

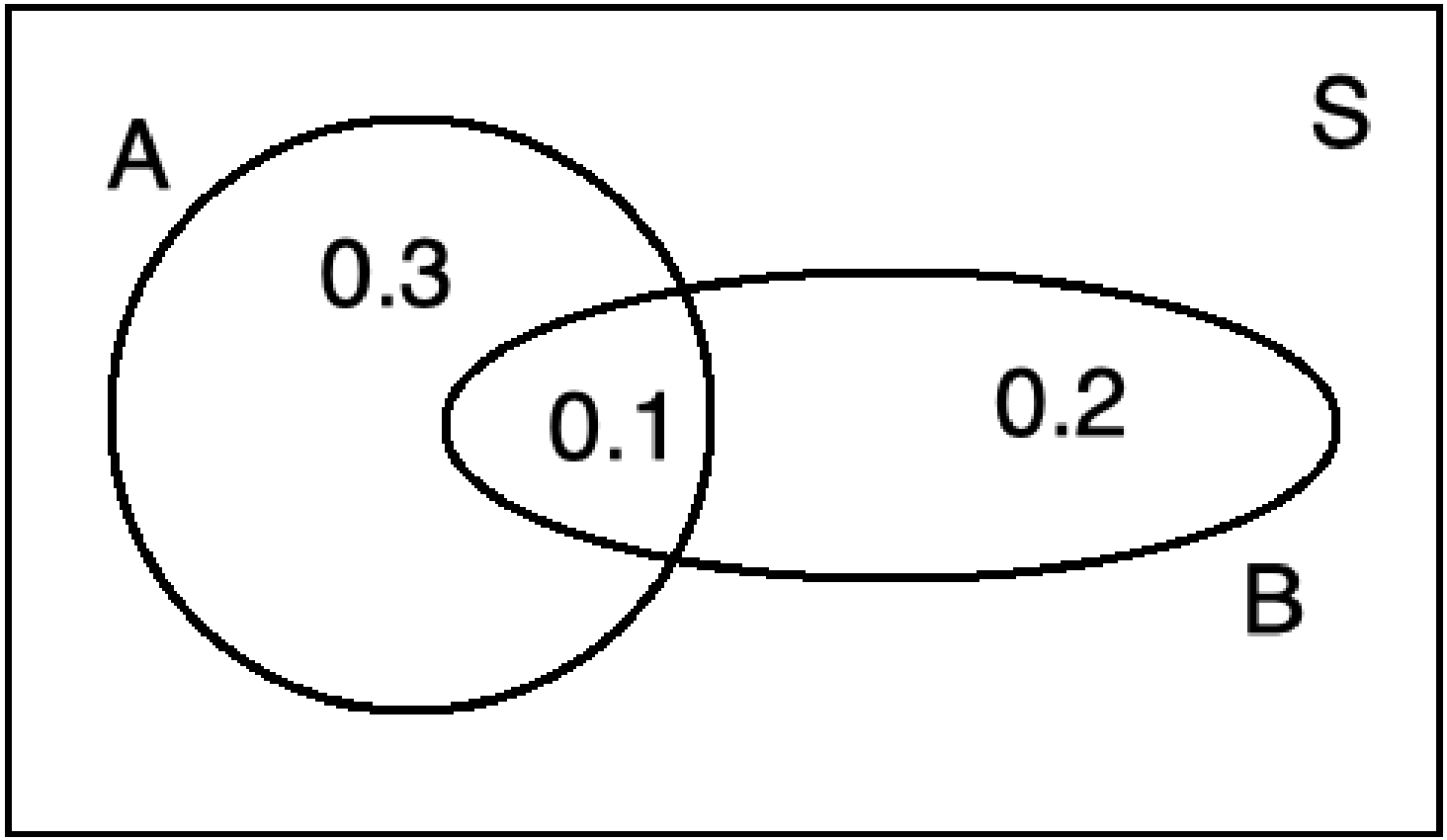
Example: 2 fair dice are rolled. What is the probability that the sum of faces is 4?

	1	2	3	4	5	6	Total
1	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
2	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
3	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
4	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
5	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
6	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
Total	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	1

All 36 outcomes have equal probability, and 3 of them meet our needs. Let $E = \{(1,3),(2,2),(3,1)\}$. Then

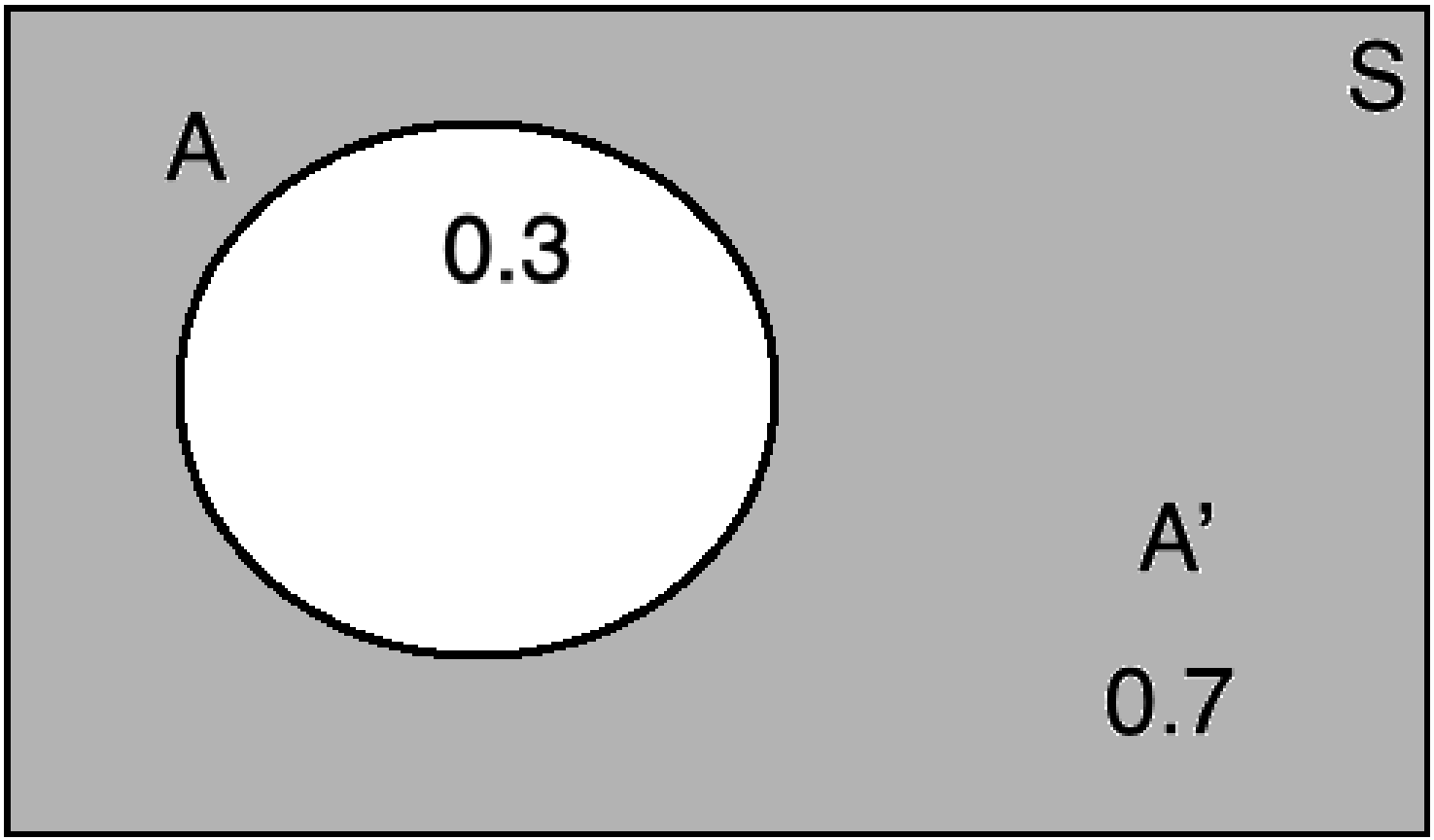
$$P(E) = \frac{|E|}{|S|} = \frac{3}{36} = \frac{1}{12}.$$

A Venn diagram represents the sample space and all events. Probabilities are represented as areas.

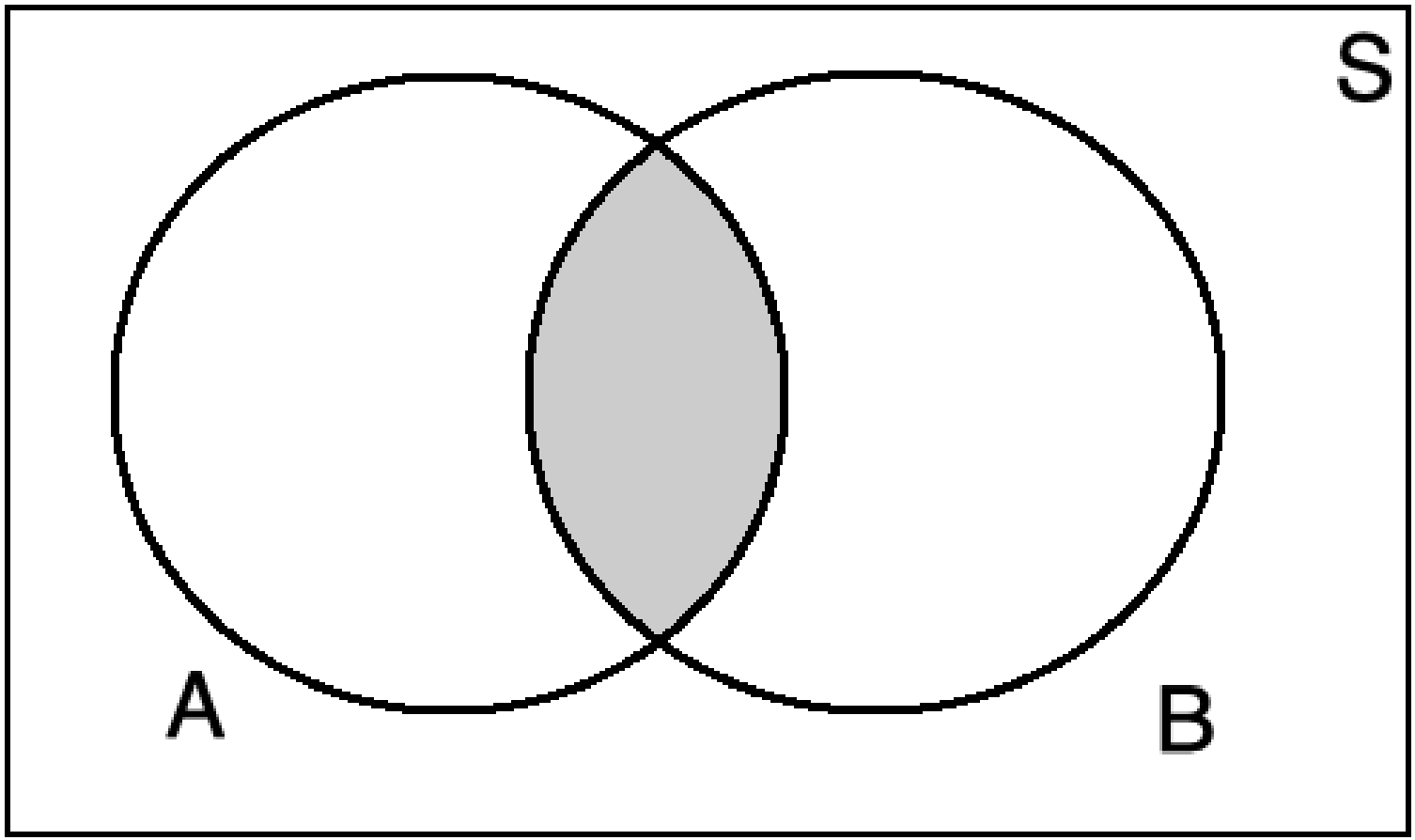


Complement: the complement of A, denoted by A^c, A' or $\overline{A}$, is the set of all outcomes not in A.

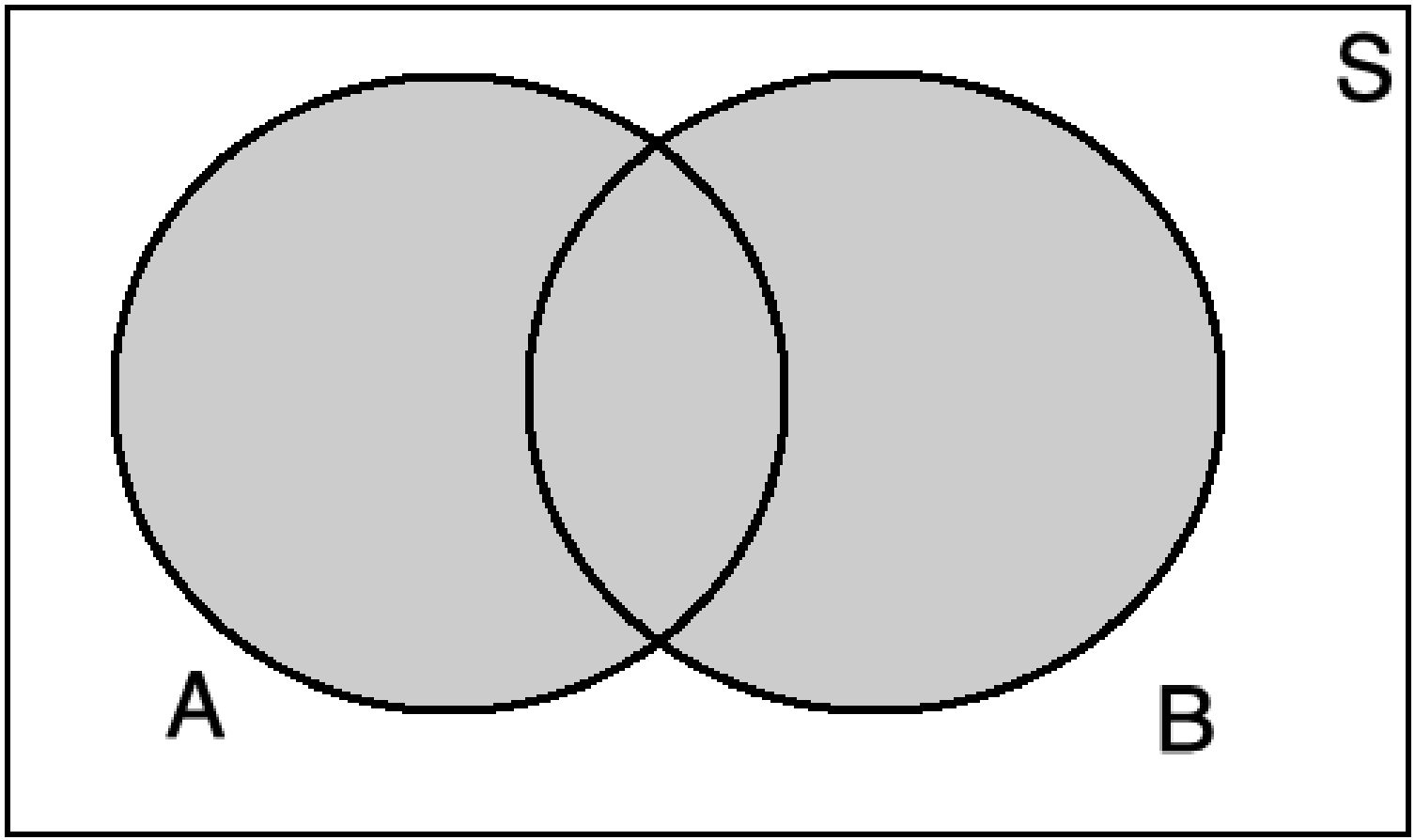
$$P(A') = 1 - P(A)$$



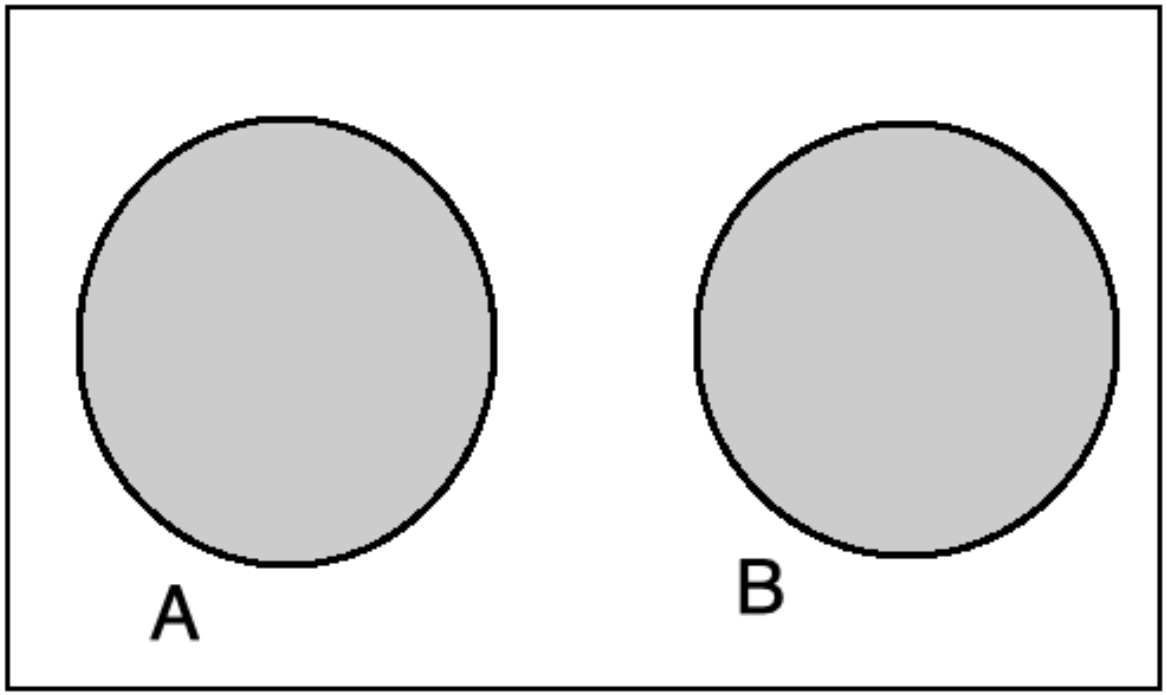
Intersection: the intersection $A \cap B$ is the event that A and B both occur.



Union: the union $A \cup B$ is the event that A or B (or both) occurs.



Two events are disjoint (cannot occur simultaneously) if $A \cap B = \varnothing$.



For disjoint events A and B,

$$P(A \cup B) = P(A) + P(B),$$
$$P(A \cap B) = 0.$$

The *conditional probability* of event A given that event B has occurred is denoted by $P(A|B)$. In general (disjoint or not),

$$P(A \cap B) = P(B)P(A|B) = P(A)P(B|A).$$

That is, for A and B both to happen, one event happens and then given that, the other event happens. This gives us a formula for conditional probability:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

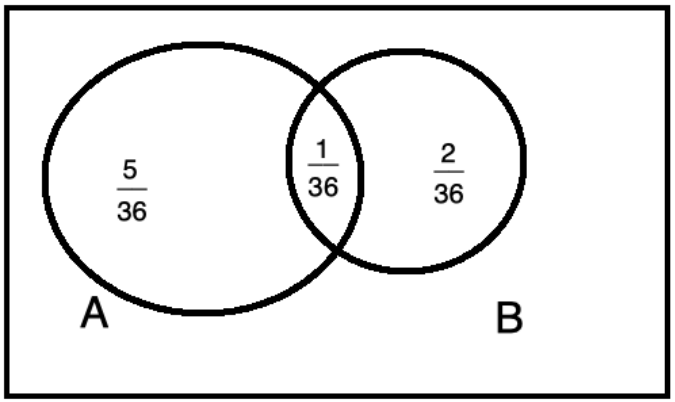
Example: given that you throw 2 dice and the sum is 4, what is the probability of "doubles"?

Example: given that you throw 2 dice and the sum is 4, what is the probability of "doubles"?

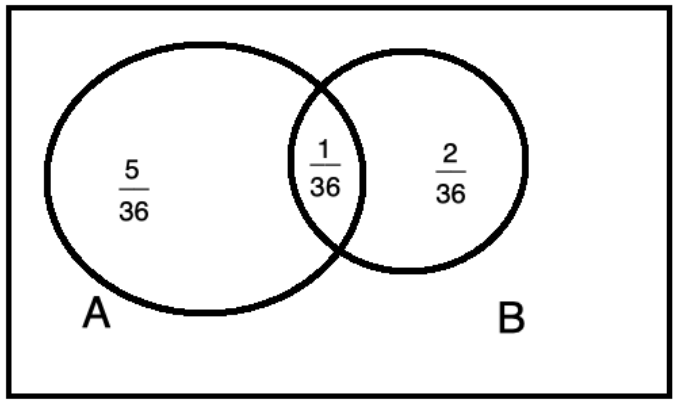
Ans. Let A = "doubles", B = "sum is 4". We found that $P(B) = \frac{1}{12}$, and since there is only one way out of 36 possibilities to obtain doubles that sum to 4, we have $P(A \cap B) = \frac{1}{36}$. Hence,

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{1/36}{1/12} = \frac{1}{3}.$$

One can use Venn diagrams to calculate $P(A|B)$ as well. In that case, B' is discarded and B becomes the new sample space. For the previous example:



One can use Venn diagrams to calculate $P(A|B)$ as well. In that case, B' is discarded and B becomes the new sample space. For the previous example:



There are 3 out of 36 possibilities that sum to 4, with one of them being a double. There are 6 doubles altogether. Then to find $P(A|B)$, consider B as the entire sample space and find $P(A \cap B)$ in that reduced space.

$$P(A|B) = \frac{\frac{1}{36}}{\frac{1}{36} + \frac{2}{36}} = \frac{1}{3}$$

Probability Rules

1. $P(S) = 1$, $P(\varnothing) = 0$.
2. $P(E) \geq 0$ for any event $E \subseteq S$.
3. If $A \cap B = \varnothing$, then $P(A \cup B) = P(A) + P(B)$.
4. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
5. $P(A') = 1 - P(A)$.
6. $P(A \cap B) = P(A)P(B|A) = P(B)P(A|B)$.

A two-way table presents probabilities of all possible intersections of two events.

	B	B'	Total
A	$P(A \cap B)$	$P(A \cap B')$	$P(A)$
A'	$P(A' \cap B)$	$P(A' \cap B')$	$P(A')$
Total	$P(B)$	$P(B')$	1

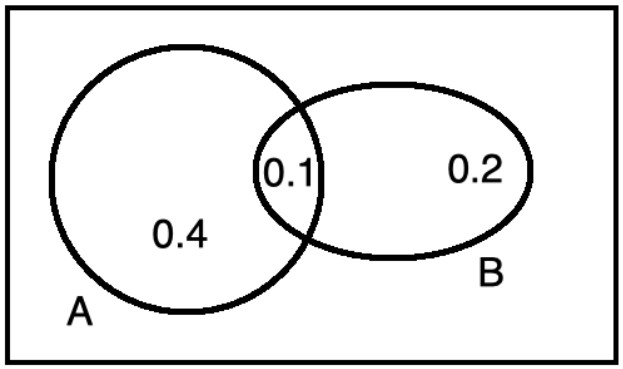
A two-way table presents probabilities of all possible intersections of two events.

	B	B'	Total
A	$P(A \cap B)$	$P(A \cap B')$	$P(A)$
A'	$P(A' \cap B)$	$P(A' \cap B')$	$P(A')$
Total	$P(B)$	$P(B')$	1

Example: using the previous Venn diagram,

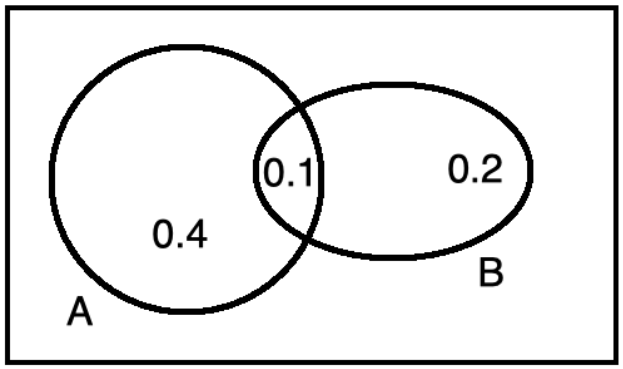
	B	B'	Total
A	$\frac{1}{36}$	$\frac{5}{36}$	$\frac{6}{36}$
A'	$\frac{2}{36}$	$\frac{28}{36}$	$\frac{30}{36}$
Total	$\frac{3}{36}$	$\frac{33}{36}$	1

To find conditional probability using a two-way table, divide the intersection value by the row or column total. Example:



	B	B'	Total
A	0.1	0.4	0.5
A'	0.2	0.3	0.5
Total	0.3	0.7	1

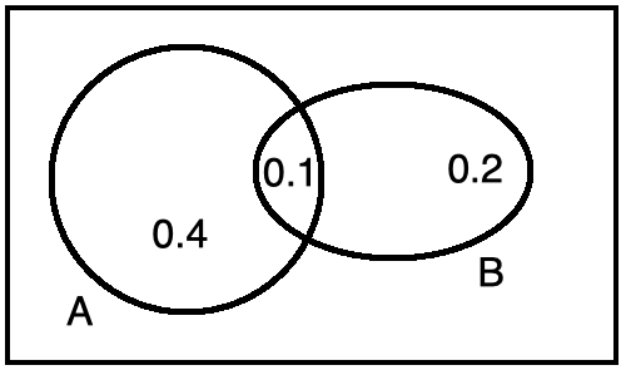
To find conditional probability using a two-way table, divide the intersection value by the row or column total. Example:



	B	B'	Total
A	0.1	0.4	0.5
A'	0.2	0.3	0.5
Total	0.3	0.7	1

$$P(B|A) = \frac{0.1}{0.5} = \frac{1}{5}; \quad P(A|B) = \frac{0.1}{0.3} = \frac{1}{3}$$

To find conditional probability using a two-way table, divide the intersection value by the row or column total. Example:



	B	B'	Total
A	0.1	0.4	0.5
A'	0.2	0.3	0.5
Total	0.3	0.7	1

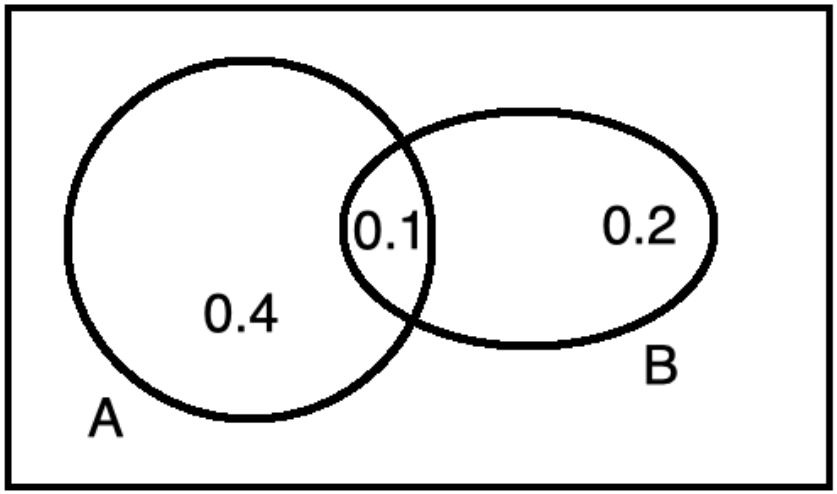
$$P(B|A) = \frac{0.1}{0.5} = \frac{1}{5}; \quad P(A|B) = \frac{0.1}{0.3} = \frac{1}{3}$$

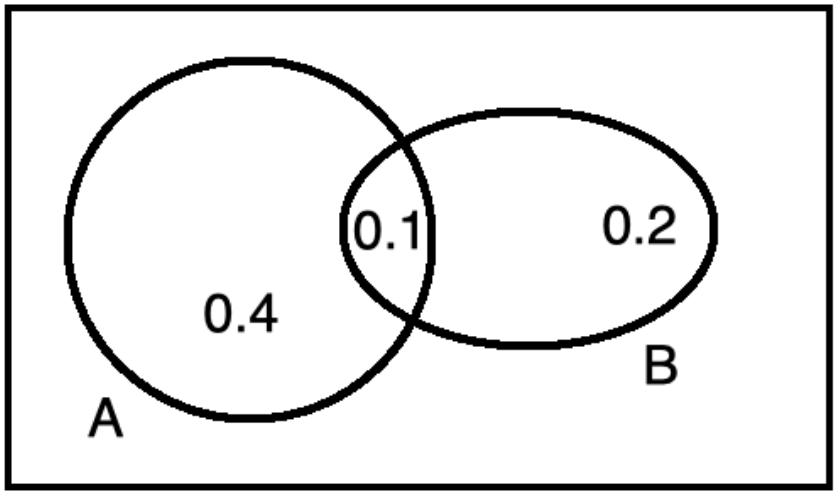
Exercise: verify the table values.

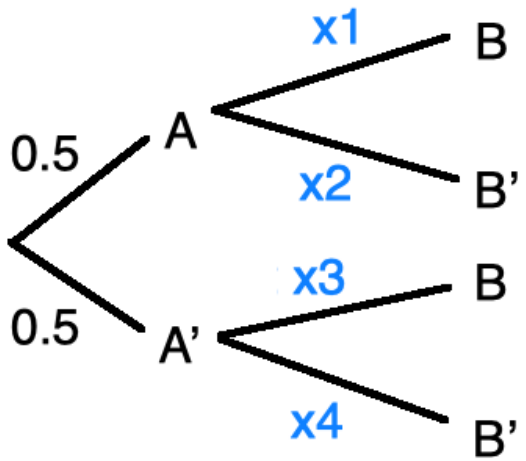
Conditional probabilities correspond to second-level (or higher) branches in a *tree diagram*.

- Multiply probabilities of all branches along a path to find the intersection probability.
- Add probabilities of all paths leading to an event to find its probability.

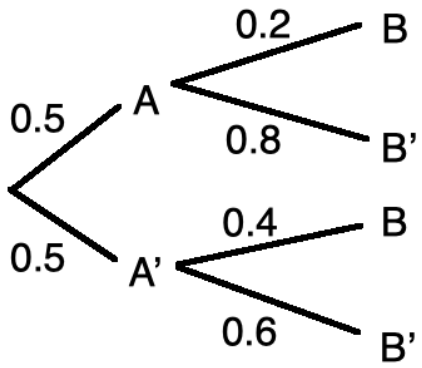
Example: use the previous Venn diagram to build a tree diagram and calculate all conditional probabilities branching on A first.


0.1
0.2
0.4
B
A

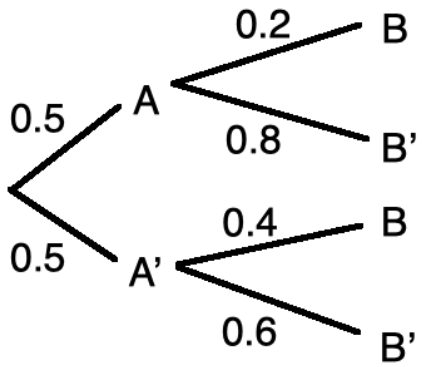




The x_i values are the conditional probabilities. First, figure out the intersection probabilities using the Venn diagram. We have $P(A \cap B) = 0.1$, etc. Then find the conditional probabilities with the formula.

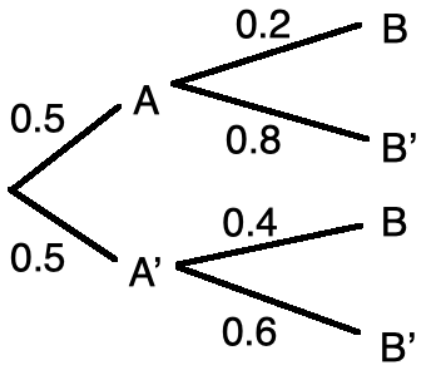


$$P(A \cap B) = 0.1$$
$$P(A \cap B') = 0.4$$
$$P(A' \cap B) = 0.2$$
$$P(A' \cap B') = 0.3$$



$$P(A \cap B) = 0.1$$
$$P(A \cap B') = 0.4$$
$$P(A' \cap B) = 0.2$$
$$P(A' \cap B') = 0.3$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{0.1}{0.5} = 0.2$$
$$P(B'|A) = \frac{P(A \cap B')}{P(A)} = \frac{0.4}{0.5} = 0.8$$
$$P(B|A') = \frac{P(A' \cap B)}{P(A')} = \frac{0.2}{0.5} = 0.4$$
$$P(B'|A') = \frac{P(A' \cap B')}{P(A')} = \frac{0.3}{0.5} = 0.6$$



$$P(A \cap B) = 0.1$$
$$P(A \cap B') = 0.4$$
$$P(A' \cap B) = 0.2$$
$$P(A' \cap B') = 0.3$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{0.1}{0.5} = 0.2$$
$$P(B'|A) = \frac{P(A \cap B')}{P(A)} = \frac{0.4}{0.5} = 0.8$$
$$P(B|A') = \frac{P(A' \cap B)}{P(A')} = \frac{0.2}{0.5} = 0.4$$
$$P(B'|A') = \frac{P(A' \cap B')}{P(A')} = \frac{0.3}{0.5} = 0.6$$

Exercise: repeat, branching on B first.

Law of Total Probability

$P(A)$ can be found by decomposing A into disjoint pieces, then using the sum and product rules:

$$\begin{aligned} P(A) &= P(A \cap B) + P(A \cap B') \\ &= P(B)P(A|B) + P(B')P(A|B') \end{aligned}$$

Example: for the previous example:

$$P(B) = P(A)P(B|A) + P(A')P(B|A') = 0.5(0.2) + 0.5(0.4) = 0.3$$

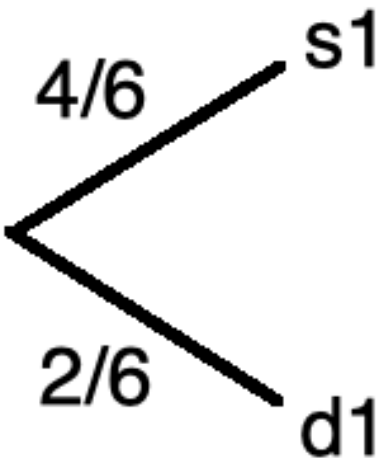
Example: 2 items are randomly selected without replacement from a production batch of 6. The batch contains 2 defective items. What is the probability that at least 1 defective item is found?

Example: 2 items are randomly selected without replacement from a production batch of 6. The batch contains 2 defective items. What is the probability that at least 1 defective item is found?

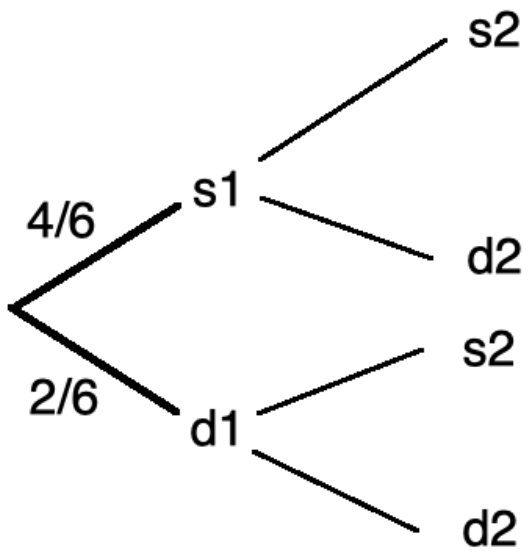
Ans. Let s_i denote the event that item i is satisfactory, d_i that it is defective. **Step 1:** inspect the first item.

Example: 2 items are randomly selected without replacement from a production batch of 6. The batch contains 2 defective items. What is the probability that at least 1 defective item is found?

Ans. Let s_i denote the event that item i is satisfactory, d_i that it is defective. **Step 1:** inspect the first item.

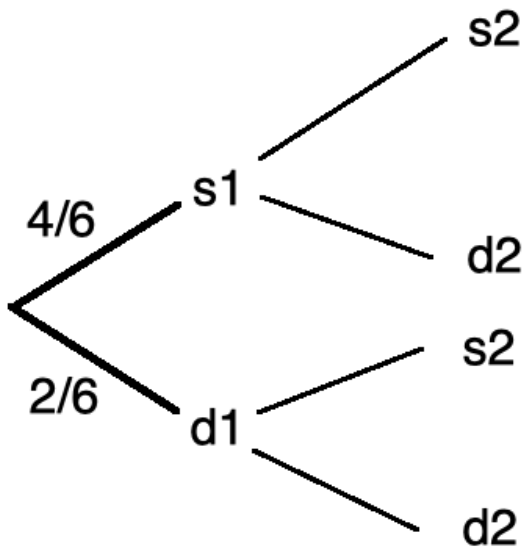


Step 2: given Step 1, inspect the second item.



Conditional probabilities: if s_1, then there remain 3 satisfactory items out of 5 total, so $P(s_2|s_1) = \frac{3}{5}$. Fill in the rest of the tree in this manner. Then the formula gives intersection probabilities.

Step 2: given Step 1, inspect the second item.



Conditional probabilities: if s_1, then there remain 3 satisfactory items out of 5 total, so $P(s_2|s_1) = \frac{3}{5}$. Fill in the rest of the tree in this manner. Then the formula gives intersection probabilities.

$$P(s_1 \cap s_2) = \frac{4}{6} \cdot \frac{3}{5} = \frac{2}{5}; P(s_1 \cap d_2) = \frac{4}{6} \cdot \frac{2}{5} = \frac{4}{15};$$

$$P(d_1 \cap s_2) = \frac{2}{6} \cdot \frac{4}{5} = \frac{4}{15}; P(d_1 \cap d_2) = \frac{2}{6} \cdot \frac{1}{5} = \frac{1}{5}$$

$P(\text{at least one defective}) =$
$P(s_1 \cap d_2) + P(d_1 \cap s_2) + P(d_1 + d_2) = \frac{4}{15} + \frac{4}{15} + \frac{1}{15} = \frac{3}{5}$

OR

$1 - P(\text{no defectives}) = 1 - P(s_1 \cap s_2) = 1 - \frac{2}{5} = \frac{3}{5}$

Independence

If the probability that A occurs is not affected by whether or not B occurs, i.e. $P(A|B) = P(A)$, we say that A and B are independent events. We have that $P(A|B) = P(A \cap B)/P(B)$, so A and B are independent iff

$$\boxed{P(A \cap B) = P(A)P(B).}$$

Independence

If the probability that A occurs is not affected by whether or not B occurs, i.e. $P(A|B) = P(A)$, we say that A and B are independent events. We have that $P(A|B) = P(A \cap B)/P(B)$, so A and B are independent iff

$$\boxed{P(A \cap B) = P(A)P(B).}$$

Examples:

- Successive coin tosses are not affected by previous results. Results of different tosses are independent.
- The events "drug is present" and "positive test result" are not independent, as a drug test is much more likely to be positive if the drug is present.

Example: events A and B are independent, $P(A) = 0.4$ and $P(B) = 0.5$. Construct the two-way table and tree diagram.

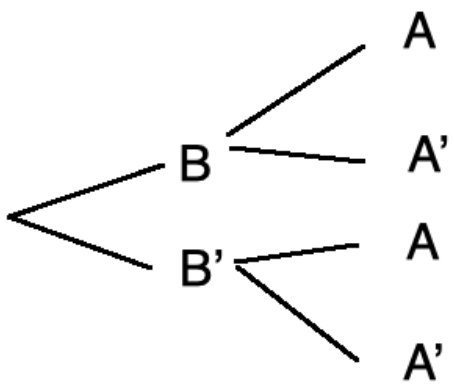
Example: events A and B are independent, $P(A) = 0.4$ and $P(B) = 0.5$. Construct the two-way table and tree diagram.

Ans. Start with what you know and use $P(A \cap B) = P(A)P(B)$.

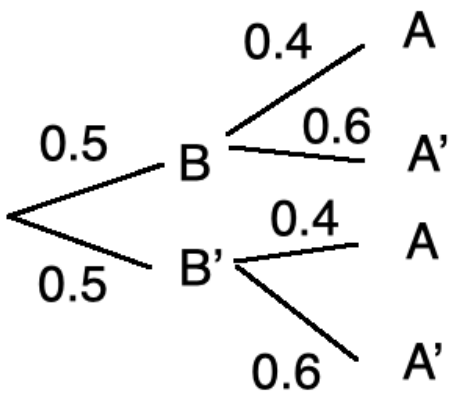
	B	B'	Total
A	0.2		0.4
A'			
Total	0.5		1

Find the remaining entries by subtraction.

	B	B'	Total
A	0.2	0.2	0.4
A'	0.3	0.3	0.6
Total	0.5	0.5	1



	B	B'	Total
A	0.2	0.2	0.4
A'	0.3	0.3	0.6
Total	0.5	0.5	1



$$0.5(0.4) = 0.2 = P(A \cap B)$$
$$0.5(0.6) = 0.3 = P(A' \cap B)$$
$$0.5(0.4) = 0.2 = P(A \cap B')$$
$$0.5(0.6) = 0.3 = P(A' \cap B')$$

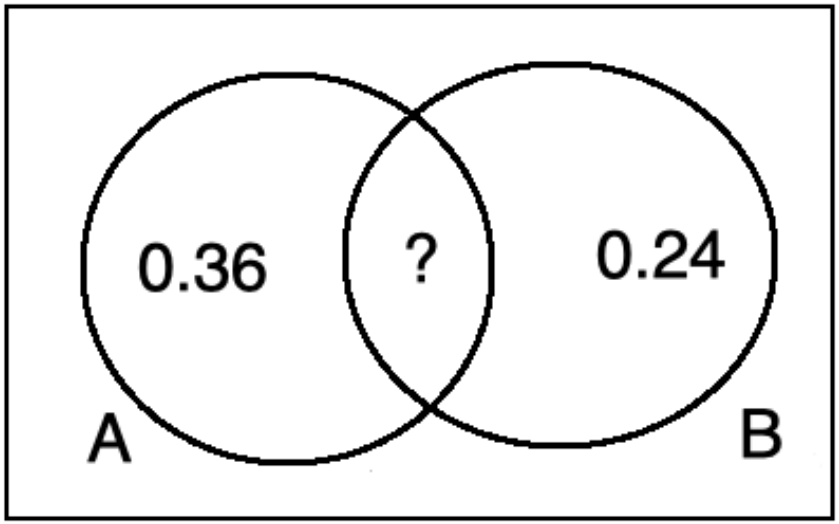
Example: If $P(A \cap B') = 0.36$, $P(A' \cap B) = 0.24$ and $P(A|B) = 0.5$, then A and B are

1. disjoint and independent
2. disjoint and not independent
3. independent and not disjoint
4. not independent nor disjoint

Example: If $P(A \cap B') = 0.36$, $P(A' \cap B) = 0.24$ and $P(A|B) = 0.5$, then A and B are

1. disjoint and independent
2. disjoint and not independent
3. independent and not disjoint
4. not independent nor disjoint

Ans. Recall that disjoint means $P(A \cap B) = 0$.



Remember you can think about $P(A|B)$ as $P(A)$ when B is the whole space.

Remember you can think about $P(A|B)$ as $P(A)$ when B is the whole space. Since $P(A|B) = 0.5$, then $P(A'|B) = 0.5$ as well (why?).

Remember you can think about $P(A|B)$ as $P(A)$ when B is the whole space. Since $P(A|B) = 0.5$, then $P(A'|B) = 0.5$ as well (why?). Then

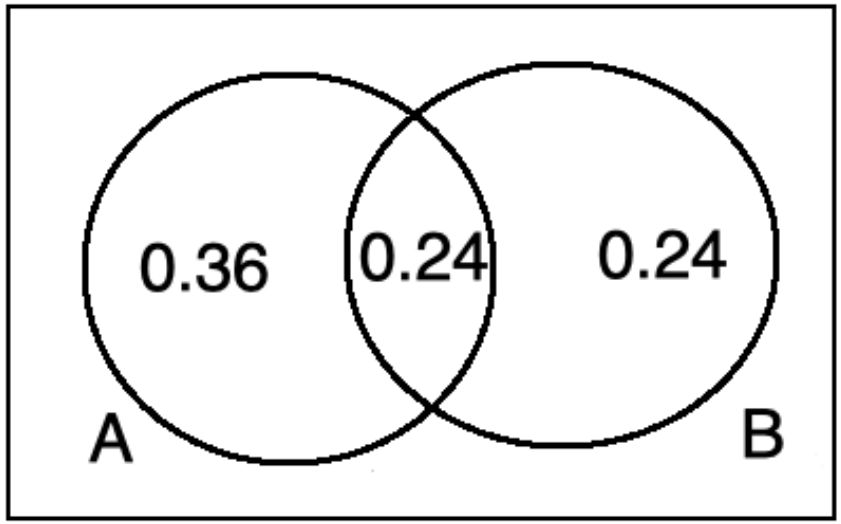
$$P(B) = \frac{P(A' \cap B)}{P(A'|B)} = \frac{0.24}{0.5} = 0.48$$

and we have $P(A \cap B) = 0.24$.

Remember you can think about $P(A|B)$ as $P(A)$ when B is the whole space. Since $P(A|B) = 0.5$, then $P(A'|B) = 0.5$ as well (why?). Then

$$P(B) = \frac{P(A' \cap B)}{P(A'|B)} = \frac{0.24}{0.5} = 0.48$$

and we have $P(A \cap B) = 0.24$.



Therefore, A and B are not disjoint.

Independence means $P(A \cap B) = P(A)P(B)$.

$$P(A)P(B) = 0.6(0.48) = 0.288 \neq 0.24.$$

Therefore, A and B are not independent.

For events A and B, Bayes' Rule provides a way to reverse the order of conditional probabilities.

$$\boxed{P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B)+P(A|B')P(B')}}$$

This comes directly from the formula $P(B|A) = \frac{P(A \cap B)}{P(A)}$ and the product rule (numerator) and Law of Total Probability (denominator). In terms of a tree, the numerator defines one path and the denominator is the sum of paths that lead to A.

Example: A drug test has 0.96 chance of positive test result if the drug is present in the body and 0.93 chance of negative result if not present. The probability of the drug being present in a randomly selected athlete is 0.007. Given a positive test result, what is the probability that the drug is actually present?

Example: A drug test has 0.96 chance of positive test result if the drug is present in the body and 0.93 chance of negative result if not present. The probability of the drug being present in a randomly selected athlete is 0.007. Given a positive test result, what is the probability that the drug is actually present?

Let $A =$ "positive test result", $B =$ "drug is present".

Example: A drug test has 0.96 chance of positive test result if the drug is present in the body and 0.93 chance of negative result if not present. The probability of the drug being present in a randomly selected athlete is 0.007. Given a positive test result, what is the probability that the drug is actually present?

Let $A =$ "positive test result", $B =$ "drug is present".

$P(A|B) = 0.96$;

Example: A drug test has 0.96 chance of positive test result if the drug is present in the body and 0.93 chance of negative result if not present. The probability of the drug being present in a randomly selected athlete is 0.007. Given a positive test result, what is the probability that the drug is actually present?

Let $A =$ "positive test result", $B =$ "drug is present".

$P(A|B) = 0.96$; $P(A'|B') = 0.93$;

Example: A drug test has 0.96 chance of positive test result if the drug is present in the body and 0.93 chance of negative result if not present. The probability of the drug being present in a randomly selected athlete is 0.007. Given a positive test result, what is the probability that the drug is actually present?

Let $A =$ "positive test result", $B =$ "drug is present".

$P(A|B) = 0.96$; $P(A'|B') = 0.93$; $P(B) = 0.007$

$$\begin{aligned} P(B|A) &= \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|B')P(B')} \\ &= \frac{0.96(0.007)}{0.96(0.007) + (1 - 0.93)(1 - 0.007)} \\ &= 0.08815 \end{aligned}$$

So a positive test result on a random athlete is 91% likely to be false!!

Binomial Scenario

- Fixed number of independent trials.
- 2 possible outcomes, success and failure.
- Constant probability of success for each trial.
- The quantity of interest is the total number of successes.

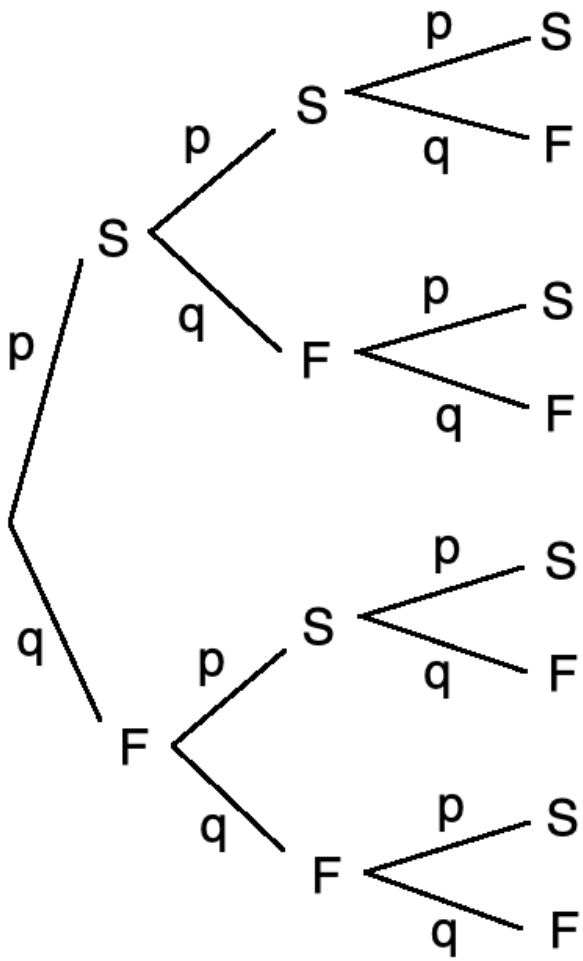
Binomial Scenario

- Fixed number of independent trials.
- 2 possible outcomes, success and failure.
- Constant probability of success for each trial.
- The quantity of interest is the total number of successes.

Notation:

$n =$ number of trials
$p =$ probability of success for a single trial
$q = 1 - p =$ probability of failure
$x =$ number of successes

For small n, a tree can be used to work out the probabilities.



p^3

p^2q

p^2q

pq^2

p^2q

pq^2

pq^2

q^3

We are interested in x, the number of successes.

x	0	1	2	3	Total
Prob.	q^3	$3pq^2$	$3p^2q$	p^3	1

We are interested in x, the number of successes.

x	0	1	2	3	Total
Prob.	q^3	$3pq^2$	$3p^2q$	p^3	1

For larger n, use combinatorics. Recall that there are $n!$ ways of arranging n objects and by definition $0! = 1$.

The binomial coefficient (number of ways to select k objects out of n unordered) is $\binom{n}{k} = C_k^n = \frac{n!}{k!(n-k)!}$

An alternative interpretation is that there are $\binom{n}{x}$ ways of grouping n objects, x of one type (success) and $(n-x)$ of another type (failure). Example: $\binom{3}{2} = SSF, SFS, FSS$.

An alternative interpretation is that there are $\binom{n}{x}$ ways of grouping n objects, x of one type (success) and $(n-x)$ of another type (failure). Example: $\binom{3}{2} = SSF, SFS, FSS$.

Since the binomial scenario events are independent, the probability of a particular instance of x successes and $(n-x)$ failures in n trials (single path along the tree) is

$$\underbrace{p \cdot p \cdot \ldots \cdot p}_{x \text{ times}} \cdot \underbrace{q \cdot q \cdot \ldots \cdot q}_{(n-x) \text{ times}} = p^x q^{n-x}$$

An alternative interpretation is that there are $\binom{n}{x}$ ways of grouping n objects, x of one type (success) and $(n-x)$ of another type (failure). Example: $\binom{3}{2} = SSF, SFS, FSS$.

Since the binomial scenario events are independent, the probability of a particular instance of x successes and $(n-x)$ failures in n trials (single path along the tree) is

$$\underbrace{p \cdot p \cdot \ldots \cdot p}_{x \text{ times}} \cdot \underbrace{q \cdot q \cdot \ldots \cdot q}_{(n-x) \text{ times}} = p^x q^{n-x}$$

The number of such paths is $\binom{n}{x}$, so the probability of x successes is

$$\boxed{\binom{n}{x} p^x q^{n-x}}$$

Note that the sum of all binomial probabilities must be 1. We verify this by the Binomial Theorem.

Note that the sum of all binomial probabilities must be 1. We verify this by the Binomial Theorem.

$$\begin{aligned}\binom{n}{0}q^n + \binom{n}{1}pq^{n-1} + \binom{n}{2}p^2q^{n-2} + \cdots + \binom{n}{n}p^n &= \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k} \\ &= (q+p)^n \\ &= (1-p+p)^n \\ &= 1\end{aligned}$$

Example: The probability that an email message is junk is 0.25, independently of all other messages. What is the probability that exactly 5 out of your 20 most recent messages are junk?

Example: The probability that an email message is junk is 0.25, independently of all other messages. What is the probability that exactly 5 out of your 20 most recent messages are junk?

Ans. $n = 20$ is far too big for a diagram, so use the binomial probability formula with $n = 20$, $x = 5$, $p = 0.25$.

$$P(5) = \binom{20}{5} 0.25^5 0.75^{20-5} = 0.2023$$

- A *random variable* is a numerical measurement of the outcome of a random phenomenon.
- An upper-case letter, such as X, refers to a random variable, which cannot be predicted with certainty.
- A lower-case letter, such as x, refers to a particular value of the variable X.

A discrete random variable has values restricted to separate points. The *probability distribution function (pdf* of a discrete RV is defined by

$$f(x) = P(X = x).$$

A discrete random variable has values restricted to separate points. The *probability distribution function (pdf* of a discrete RV is defined by

$$f(x) = P(X = x).$$

A probability function must satisfy

$$f(x) \geq 0 \ \forall x, \quad \text{and} \quad \sum_x f(x) = 1.$$

A discrete random variable has values restricted to separate points. The *probability distribution function (pdf* of a discrete RV is defined by

$$f(x) = P(X = x).$$

A probability function must satisfy

$$f(x) \geq 0 \ \forall x, \quad \text{and} \quad \sum_x f(x) = 1.$$

The function may be specified by table or by formula:

x	0	1	2	Total
$f(x)$	0.3	0.55	0.15	1

$$g(x) = \binom{2}{x} p^x (1-p)^{2-x}, \ x = 0, 1, 2.$$

Binomial Distribution Function

Let X be the number of successes in n independent trials, with constant probability p of success. The X has a binomial probability function

$$f(x) = P(X = x) = \binom{n}{x} p^x q^{n-x}, \ x = 0, 1, \ldots, n, q = 1 - p.$$

Example: a multiple choice quiz has 11 questions with 5 possible answers each. What is the probability that a student who guesses at every question gets a score of 4 out of 11?

Example: a multiple choice quiz has 11 questions with 5 possible answers each. What is the probability that a student who guesses at every question gets a score of 4 out of 11?

Ans. $n = 11$, $x = 4$, $p = 0.2$

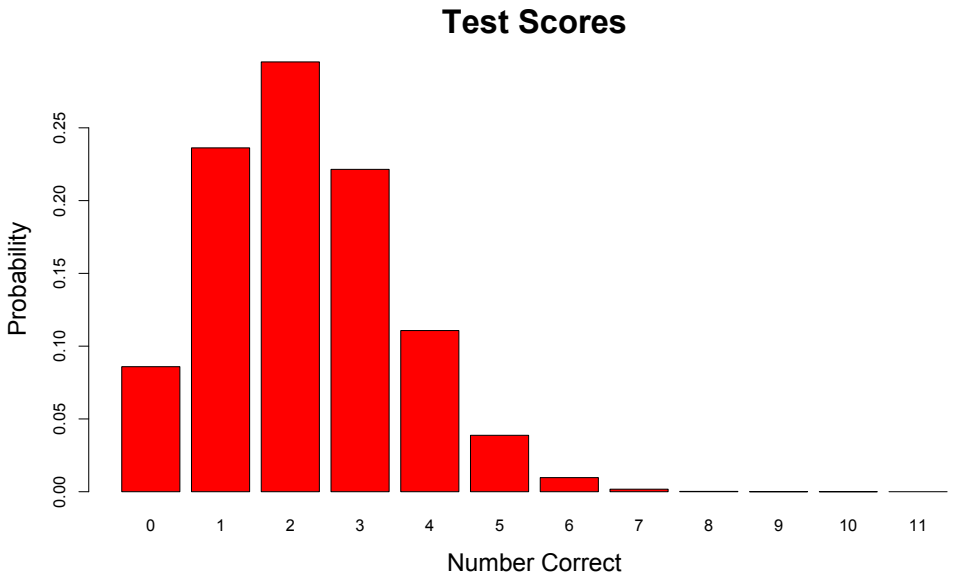
$$f(4) = P(X = 4) = \binom{11}{4} 0.2^4 0.8^{11-4} = 0.1107$$

Example: a multiple choice quiz has 11 questions with 5 possible answers each. What is the probability that a student who guesses at every question gets a score of 4 out of 11?

Ans. $n = 11$, $x = 4$, $p = 0.2$

$$f(4) = P(X = 4) = \binom{11}{4} 0.2^4 0.8^{11-4} = 0.1107$$

One can calculate each outcome and graph them:



So don't guess; you'll most likely get 2/11.

Cumulative Distribution

This gives $P(X \leq 3) = f(0) + f(1) + f(2) + f(3) = 0.8389$ for $n = 11$ and $p = 0.2$. By hand, this is

$$\binom{11}{0}0.2^0 0.8^{11} + \binom{11}{1}0.2^1 0.8^{10} + \binom{11}{2}0.2^2 0.8^9 + \binom{11}{3}0.2^3 0.8^8.$$

Cumulative Distribution

This gives $P(X \leq 3) = f(0) + f(1) + f(2) + f(3) = 0.8389$ for $n = 11$ and $p = 0.2$. By hand, this is

$$\binom{11}{0}0.2^0 0.8^{11} + \binom{11}{1}0.2^1 0.8^{10} + \binom{11}{2}0.2^2 0.8^9 + \binom{11}{3}0.2^3 0.8^8.$$

Example: In the previous example, what is the probability that the student gets at least 4 out of 11?

Cumulative Distribution

This gives $P(X \leq 3) = f(0) + f(1) + f(2) + f(3) = 0.8389$ for $n = 11$ and $p = 0.2$. By hand, this is

$$\binom{11}{0}0.2^0 0.8^{11} + \binom{11}{1}0.2^1 0.8^{10} + \binom{11}{2}0.2^2 0.8^9 + \binom{11}{3}0.2^3 0.8^8.$$

Example: In the previous example, what is the probability that the student gets at least 4 out of 11?

Ans. The long way:
$P(X \geq 4) = P(X = 4) + P(X = 5) + \cdots + P(x = 11)$.

Cumulative Distribution

This gives $P(X \leq 3) = f(0) + f(1) + f(2) + f(3) = 0.8389$ for $n = 11$ and $p = 0.2$. By hand, this is

$$\binom{11}{0}0.2^0 0.8^{11} + \binom{11}{1}0.2^1 0.8^{10} + \binom{11}{2}0.2^2 0.8^9 + \binom{11}{3}0.2^3 0.8^8.$$

Example: In the previous example, what is the probability that the student gets at least 4 out of 11?

Ans. The long way:
$P(X \geq 4) = P(X = 4) + P(X = 5) + \cdots + P(x = 11)$.
The short way:
$P(X \geq 4) = 1 - P(X < 4) = 1 - 0.8389 = 0.1611$.

The *cumulative distribution function (cdf)* of a discrete RV X, denoted by $F(x)$, is defined by

$$\boxed{F(x) = P(X \leq x) = \sum_{k \leq x} f(k)}$$

The *cumulative distribution function (cdf)* of a discrete RV X, denoted by $F(x)$, is defined by

$$\boxed{F(x) = P(X \leq x) = \sum_{k \leq x} f(k)}$$

To avoid sums with many terms, we use differences of cdfs:

$$\boxed{P(a < X \leq b) = F(b) - F(a)}$$

Be careful with $<$ and $\leq$ for discrete variables, eg.:

$$P(20 \leq X \leq 25) = F(25) - F(19)$$

We find $F(x)$ by summing values of $f(k)$. To find f from F, we use differences.

$$\begin{aligned} f(x) &= P(X = x) \\ &= P(X \leq x) - P(X < x) \\ &= F(x) - F(x-1) \end{aligned}$$

We find $F(x)$ by summing values of $f(k)$. To find f from F, we use differences.

$$\begin{aligned} f(x) &= P(X = x) \\ &= P(X \leq x) - P(X < x) \\ &= F(x) - F(x-1) \end{aligned}$$

Example:

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1
$F(x)$	0.4	0.7	0.9	1

We find $F(x)$ by summing values of $f(k)$. To find f from F, we use differences.

$$\begin{aligned} f(x) &= P(X = x) \\ &= P(X \leq x) - P(X < x) \\ &= F(x) - F(x-1) \end{aligned}$$

Example:

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1
$F(x)$	0.4	0.7	0.9	1

$F(2) = f(0) + f(1) + f(2) = 0.4 + 0.3 + 0.2 = 0.9$

We find $F(x)$ by summing values of $f(k)$. To find f from F, we use differences.

$$\begin{aligned} f(x) &= P(X = x) \\ &= P(X \leq x) - P(X < x) \\ &= F(x) - F(x-1) \end{aligned}$$

Example:

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1
$F(x)$	0.4	0.7	0.9	1

$F(2) = f(0) + f(1) + f(2) = 0.4 + 0.3 + 0.2 = 0.9$
$f(2) = F(2) - F(1) = 0.9 - 0.7 = 0.2$

We find $F(x)$ by summing values of $f(k)$. To find f from F, we use differences.

$$\begin{aligned} f(x) &= P(X = x) \\ &= P(X \leq x) - P(X < x) \\ &= F(x) - F(x-1) \end{aligned}$$

Example:

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1
$F(x)$	0.4	0.7	0.9	1

$F(2) = f(0) + f(1) + f(2) = 0.4 + 0.3 + 0.2 = 0.9$
$f(2) = F(2) - F(1) = 0.9 - 0.7 = 0.2$
$P(0 < X \leq 2) = f(1) + f(2) = F(2) - F(0) = 0.5$

Consider n observations of a discrete RV X. On average, we expect the observed relative frequency $\frac{n_x}{n}$ of a fixed value x to be equal to the probability function $f(x) = P(X = x)$. Recall the formula for the mean of a sample: $\bar{x} = \sum_x x \frac{n_x}{n}$. This leads to the following definition.

Consider n observations of a discrete RV X. On average, we expect the observed relative frequency $\frac{n_x}{n}$ of a fixed value x to be equal to the probability function $f(x) = P(X = x)$. Recall the formula for the mean of a sample: $\bar{x} = \sum_x x\frac{n_x}{n}$. This leads to the following definition.

Def: The *expected value* $E(X)$ of a discrete RV X is defined by

$$E(X) = \sum_x xf(x).$$

$E(X)$ is a weighted average; greater weight is assigned to more likely values of X.

Example: Find the expected value of $f(x) = 0.1(4 - x)$, $x = 0, 1, 2, 3$.

Example: Find the expected value of $f(x) = 0.1(4 - x)$, $x = 0, 1, 2, 3$.

Ans.

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1

Example: Find the expected value of $f(x) = 0.1(4 - x)$, $x = 0, 1, 2, 3$.

Ans.

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1

$$E(X) = \sum_{x=0}^{3} xf(x) = 0(0.4) + 1(0.3) + 2(0.2) + 3(0.1) = 1$$

Example: Find the expected value of $f(x) = 0.1(4 - x)$, $x = 0, 1, 2, 3$.

Ans.

x	0	1	2	3
$f(x)$	0.4	0.3	0.2	0.1

$$E(X) = \sum_{x=0}^{3} xf(x) = 0(0.4) + 1(0.3) + 2(0.2) + 3(0.1) = 1$$

Similarly, the expected value of any function $g(X)$ is $E[g(X)] = \sum_x g(x)f(x)$. For the above example,

$$E(X^2) = \sum_{x=0}^{3} x^2 f(x) = 2$$

Properties of $E(X)$

- $E(a) = a$ for any constant a.
- For a linear transformation, $E(a + bX) = a + bE(X)$.

Properties of $E(X)$

- $E(a) = a$ for any constant a.
- For a linear transformation, $E(a + bX) = a + bE(X)$.

Note: for a nonlinear transformation $g(X)$, $E[g(X)]$ usually differs from $g(E(X))$, as in the last example $E(X^2) \neq [E(X)]^2$.

The *mean* of a discrete RV X is defined as

$$\mu = \mu_X = E(X)$$

For a large sample of observations, we expect the sample mean $\bar{x}$ to be close to the theoretical mean μ.

The *mean* of a discrete RV X is defined as

$$\mu = \mu_X = E(X)$$

For a large sample of observations, we expect the sample mean $\bar{x}$ to be close to the theoretical mean μ.

Recall the sample variance is the average of squared distances from the sample mean:

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2.$$

The *variance* of a discrete RV X is the expected squared distance from μ:

$$\sigma^2 = \mathrm{Var}(X) = E[(X-\mu)^2] \tag{4}$$

A useful alternative representation is

$$\sigma^2 = E(X^2) - \mu^2 \tag{5}$$

Exercise: use properties of $E(X)$ to prove (4) = (5).

A useful alternative representation is

$$\sigma^2 = E(X^2) - \mu^2 \tag{5}$$

Exercise: use properties of $E(X)$ to prove (4) = (5).

The *standard deviation* of X is the positive square root of the variance: $\sigma = \sqrt{\text{Var}(X)}$.

Example: find the variance for the previous example.

Example: find the variance for the previous example.

Ans. Recall that $\mu = 1$ and $E(X^2) = 2$, so $\sigma^2 - E(X^2) - \mu^2 = 1$.
Or the longer way:

$$\sigma^2 = E[(X-\mu)^2] = \sum_x (x-1)^2 f(x)$$
$$= (0-1)^2 0.4 + (1-1)^2 0.3 + (2-1)^2 0.2 + (3-1)^2 0.1 = 1$$

Properties of Variance

- $\text{Var}(X) \geq 0 \; \forall X$, and $\text{Var}(X) = 0 \Leftrightarrow X$ is constant.
- $\text{Var}(X + a) = \text{Var}(X) \; \forall a \in \mathbb{R}$
- $\text{Var}(aX) = a^2 \, \text{Var}(X) \; \forall a \in \mathbb{R}$
- $\sigma_{a+bX} = |b| \sigma_X$

If a R has large variance, it means that observations are expected to vary greatly.

Example: For $f(x) = 0.1(4 - x)$, we found $\sigma^2 = 1$.

- $\text{Var}\left(\frac{X}{2}\right) = \left(\frac{1}{2}\right)^2 \text{Var}(X) = \frac{1}{4}$
- $\text{Var}(X + 6) = \text{Var}(X) = 1$
- $\text{Var}(6 - 2X) = (-2)^2 \text{Var}(X) = 4$

Example: For $f(x) = 0.1(4 - x)$, we found $\sigma^2 = 1$.

- $\text{Var}\left(\frac{X}{2}\right) = \left(\frac{1}{2}\right)^2 \text{Var}(X) = \frac{1}{4}$
- $\text{Var}(X + 6) = \text{Var}(X) = 1$
- $\text{Var}(6 - 2X) = (-2)^2 \text{Var}(X) = 4$

For a binomial distribution, we find that

1. $\mu = E(X) = np$
2. $\sigma^2 = \text{Var}(X) = np(1 - p)$
3. $\sigma = \sqrt{\text{Var}(X)} = \sqrt{np(1 - p)}$

Example: Find the mean and standard deviation of the number X of heads obtained in 100 tosses of a fair coin.

Example: Find the mean and standard deviation of the number X of heads obtained in 100 tosses of a fair coin.

Ans. Binomial distribution, $n = 100$, $p = 0.5$.

$$\mu = np = 50$$
$$\sigma = \sqrt{np(1-p)} = 5$$

This means that although X will be about 50 on average, it would not be uncommon to observe values between 45 and 55 ($\mu - \sigma$ and $\mu + \sigma$).

1. **Logic**
   - What is a statement? What are connectives?
   - Simple vs. compound statements.
   - Truth tables - don't skip too many steps.
   - Contingencies, tautologies, fallacies and the quick method.
   - Logical equivalence and substitution.
   - Equivalence laws (de Morgan, distributive, negation, ...).
   - Predicates, quantifiers and their negations.
   - Methods of proof.
     - Argument, assumption, conclusion, validity, syllogism
     - Proof of validity by truth table.
     - Proof by regular, strong and generalised induction.
     - Proof by contradiction.
     - Direct proof.
     - Proof by cases.

2 Numbers

- What is an operation? A binary operation?
- Sets, closed sets, identity and inverse elements.
- Commutative, associative and distributive operations.
- Well-ordered sets.
- Sequences and series.
- Recursion.
- Divisibility.
- Quotient-remainder Theorem.
- Fundamental Theorem of Arithmetic.
- gcd, lcm, Euclidean Algorithm, coprime numbers.
- Pigeonhole principle, generalised pigeonhole.

3. **Modular Arithmetic**
   - Definition of congruence.
   - Congruence arithmetic laws.
   - Cancellation law.
   - Congruence classes $\mathbb{Z}_n$.
   - Addition and multiplication of classes.
   - Multiplicative inverse.
4. **Set Theory**
   - Empty/finite/infinite sets.
   - Cardinality.
   - Subsets, power sets, proper subsets.
   - Prove equality of sets.
   - Set operations.
   - Venn diagrams.
   - Set algebra laws.

5. **Combinatorics**
   - Multiplication rule
   - Permutation/combination/factorial.
   - Counting strategies.
   - Binomial coefficients/binomial theorem.
6. **Functions and Relations**
   - Cartesian product
   - Definition of relation.
   - Reflexivity, symmetry, transitivity.
   - Equivalence relations/classes.
   - Inverse relations.
   - Definition of function.
   - Domain and range of functions.
   - Injective/surjective/bijective functions.
   - Inverse functions.

7. **Graph Theory**
   - Definition of graph.
   - Loops, parallel edges, isolation, adjacencies, simple graphs.
   - Complete graphs.
   - Bipartite graphs.
   - Subgraphs.
   - Degrees.
   - Isomorphism.
   - Walks, paths, circuits, trails.
   - Connected components.
   - Eulerian circuits, Euler's theorem.
   - Trees, spanning trees.
   - Weighted graphs.
   - Minimum spanning trees, Kruskal's and Prim's algorithms.

8. **Probability**
   - Venn diagrams, disjointness.
   - Conditional probability, independence.
   - Two-way tables, tree diagrams.
   - Bayes' rule.
   - Binomial distribution.
   - Discrete probabilities.
   - Cumulative functions.
   - Expected value and variance/standard deviation.