Formal Logic

- **Logic** is a language for reasoning.
- An argument is a sequence of statements aimed at demonstrating the truth of an assertion.
    - The assertion at the end of the sequence is called the **conclusion**, and the preceding statements are called **premises**.
- We are interested in whether a **statement** is true or false, and in determining truth/falsehood of statements from other statements.
- **Statement** (or **proposition**)**:** a sentence that is true or false, but not both.
- Much of Mathematics is about *proving* a statement is true, or *demonstrating* a statement is false.

Logical Connectives

- **Connectives** are key words/symbols that connect two or more simple statements to form new, longer ones.
- We use *p*, *q*, *r*, … to denote simple statements (**statement variables**) i.e. *p*: I need to work hard in MATH221.
- There are 5 Connectives:

Name	Example	Definition
Negation	~ *p*	NOT *p*
Disjunction	$p \vee q$	*p* OR *q*
Conjunction	$p \wedge q$	*p* AND *q*
Conditional	*p* => *q* (*p* -> *q*)	*p* IMPLIES *q*
Biconditional	*p* <=> *q* (*p* <-> *q*)	*p* IF AND ONLY IF *q*

- **Compound statement:** an expression of simple statements and connectives.
    - Each simple statement has a truth value T for true and 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*.

Negation

- If *p* is a statement variable, then "NOT *p*", denoted by ~*p*, has the opposite value.
    - If *p* is true, ~*p* is false.
    - If *p* is false. ~*p* is true.

Definition

If *p* is a statement variable, the **negation** of *p* is "not *p*" or "it is not the case that *p*" and is denoted ~*p*. It has the opposite truth value from *p*: if *p* is true, ~*p* is false; if *p* is false, ~*p* is true.

- The truth values for **negation** are summarised in a table.

p	***~p***
T	F
F	T

- NOTE:
  - The truth table above tells us that for any statement *p*, exactly *one* of *p* and ~*p* is true.
  - This gives us 2 options for proving *p* is true:
    - Show it directly
    - Show indirectly by proving ~*p* is false **(proof by contradiction)**

Priority

- In expressions that include the symbol ~ as well as $\wedge$ or $\vee$, the **order of operations** specifies that ~ is performed first.
- $\sim p \vee q$ means $(\sim p) \vee q$, which is different from $\sim(p \vee q)$
- In logical expressions, as in ordinary algebraic expressions, the order of operations can be overridden through the uses of parentheses.

Conjunction

- If *p* and *q* are statement variables, the conjunction is "*p* AND *q*", denoted by $p \wedge q$.
  - If *p* AND *q* are both true, then $p \wedge q$ is true.
  - Otherwise, $p \wedge q$ is false.

Definition

If *p* and *q* are statement variables, the **conjunction** of *p* and *q* is "*p* and *q*,' denoted by $p \wedge q$. It is true when, and only when, both *p* and *q* are true. If either p or q is false, or if both are false, $p \wedge q$ is false.

- The truth table for conjunction is:

p	***q***	$\boldsymbol{p \wedge q}$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

- If p and q are statement variables, the disjunction is "p OR q", denoted by $p \vee q$.
  - If p and q are both false, $p \vee q$ is false.
  - Otherwise, $p \vee q$ is true.

> **Definition**
>
> If p and q are statement variables, the **disjunction** of p and q is "p or q," denoted by $p \vee q$. It is true when either p is true, or q is true, or both p and q are true; it is false only when both p and q are false.

- The truth table for disjunction is:

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

- NOTE:
  - The word "OR" can be used in an exclusive sense, i.e. p OR q but not both.

Exclusive OR

- The **exclusive or** statement is sometimes denoted by $\otimes$
- It can also be represented by AND/OR/NOT symbols. i.e. $p \otimes q$ = "p OR q, but NOT BOTH"
- Note that when *or* is used in its exclusive sense, the statement "p or q" means "p or q but not both" or "p or q and not both p and q," which can be denoted as: $(p \vee q) \wedge \sim(p \wedge q)$.
- The truth table for exclusive or is:

p	q	$p \vee q$	$p \wedge q$	$\sim(p \wedge q)$	$(p \vee q) \wedge \sim(p \wedge q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

Conditionals

- When you make a logical inference or deduction, you reason from a *hypothesis* 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 "If *p*, then *q*" or "*p* IMPLIES *q*", denoted by *p* => *q*.
  - If *p* is true and *q* is false, then *p* => *q* is false.
  - Otherwise, *p* => *q* is true
  - *p* is the **hypothesis** (**antecedent**)
  - *q* is the **conclusion** (**consequent**)
- Conditionals take priority over conjunctions and disjunctions.

> **Definition**
>
> IF *p* and *q* are statement variables, the **conditional** of *q* by *p* is "if *p*, then *q*" or "*p* implies *q*," denoted by *p* => *q*. If *p* is true and *q* is false, then *p* => *q* is false. Otherwise, *p* => *q* is true.

- The truth table for conditionals is:

p	***q***	***p* => *q***
T	T	T
T	F	F
F	T	T
F	F	T

- NOTE:
  - Why is *p* => *q* true when *p* is false.
  - If a statement cannot be said to be false, then it is true.
  - If *p* is false, then we cannot say that *p* => *q* is false, it is true.
  - Consider the claim, "if it rains, then I will go home."
    - Only if it rains can we make a judgement on its truth.
    - If it doesn't rain, then regardless of whether or not I go home, we cannot claim that the statement is false. So, it is true.

Exercise:

Write using connectives: "If $x^2 = 4$, then x = 2 or x = -2."

$p: x^2 = 4$

$q: x = 2$

$r: x = -2$

$p \Rightarrow (q \vee r)$

Biconditionals

- A **biconditional** statement has the form "*p* if and only if *q*" or "*p* IFF *q*."
- It's true only if both variables have the same value.
- It is denoted by *p* <=> *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*
- The truth table for biconditionals is:

p	***q***	***p <=> q***
T	T	T
T	F	F
F	T	F
F	F	T

Exercise:

a) *p*: $x^3 = -8$, *q*: x = -2, *p* <=> *q*.

p	q	p => q	q => p	(p => q) ∧ (q => p)
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

b) Write using connectives: "Michael is a bachelor if and only if he is male and never married."

p: Michael is a bachelor

q: Michael is a male

r: Michael is never married

p <=> (q ∧ r)

EXERCISE:
Complete the table

p	***q***	***p* => *q***	***q* => *p***	***p* <=> *q***	**(*p* => *q*) ∧ (*q* => *p*)**
T	**T**	T	T	T	T
T	**F**	F	T	F	F
F	**T**	T	F	F	F
F	**F**	T	T	T	T

- Notice that the last two columns are the same.
- This means that *p* <=> *q* and (*p* => *q*) ∧ (*q* => *p*) are **logically equivalent**.
- NOTE:
  - Notice that *p* <=> *q* means (*p* => *q*) ∧ (*q* => *p*)

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 connectives in a statement.
- E.g.

(*p* ∨ ~*q*) => (*p* ∧ *q*)

Main Connective

~[(*p* ∧ *q*) ∨ (~*p* ∧ *q*)]

Tautology and Fallacy

- A **tautology** is a compound statement that is always true, for all values of the basic statements
  - E.g. *p* ∨ ~*p*
- A **fallacy** is a compound statement that is always false, for all values of the basic statements
  - E.g. *p* ∧~*p*
- Any statement that is neither a tautology nor a fallacy is called **contingent** or **intermediate**.
- Note that the negative of a tautology is a fallacy, and vice versa.

Definition

A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**.

A **contradiction** (**fallacy**) is a statement that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a **contradictory statement**.

Exercise:

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

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F

Exercise:

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

p	q	$\sim p$	$\sim p \wedge q$	$\sim[(\sim p \wedge q) \wedge p]$
T	T	F	F	T
T	F	F	F	T
F	T	T	T	T
F	F	T	F	T

It is a fallacy.

"Quick" Method of Identifying Tautologies

- With truth tables, 2^n rows are required.
  - This gets big and impractical quickly (i.e. 4 statements requires 16 rows, 5 statements requires 32 rows, …)
- There is a quicker method we can use:
- NOTE:
  - Truth tables are reliable; it's not easy to make mistakes. The quick method can be more difficult in that respect.
- It relies on the fact that if a false can occur under the main connective, then the statement is not a tautology.
- If a false is not possible, it is a tautology.
- They method is:
  - Assume the main connective yields a false, then work backwards to see if a valid combination of values exists.
  - Firstly, place an F under the main connective.

$$(p \wedge q) \Rightarrow (r \wedge s)$$

F

- Remember the conditional table: for this to happen, $p \wedge q$ must be true and $r \wedge s$ must be false.

$$(p \wedge q) \Rightarrow (r \wedge s)$$

F

T F

$\therefore p:T,\ q:T \quad r/s = ?$

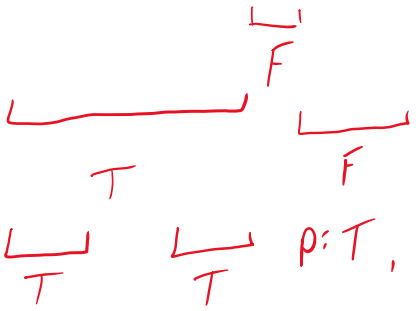
e.g. $p:T,\ q:T,\ r:T,\ s:F,$

the main connective is validly false

- Since these are perfectly valid values for p, q, r, s, we have that $(p \wedge q) \Rightarrow (r \wedge s)$ is *not* a tautology.

Exercise:

a) Is [(*p* => *q*) ∧ (*q* => *r*)] => (*p* => *r*) a tautology?



T T p:T, r:F?

p:T, q:T q:T, r:T?

There is no possible combination to make the main connective false. Therefore, this is a tautology

b) Make the truth table for this statement, and verify that the last column is all T.

p	*q*	*r*	*p* => *q*	*q* => *r*	*p* => *r*	[(*p* => *q*) ∧ (*q* => *r*)] => (*p* => *r*)
T	T	T	T	T	T	T
T	T	F	T	F	F	F T F
T	F	T	F	T	T	F T T
T	F	F	F	T	F	T
F	T	T	T	T	T	T
F	T	F	T	F	T	I T T
F	F	T	T	T	T	T
F	F	F	T	T	T	T

Logical Equivalence

- Two statements are called **logically equivalent** if, and only if, they have identical truth tables.
- The logical equivalence of *p* and *q* is denoted by $p \equiv q$.
- *p* and *q* are logically equivalent IFF $p \iff q$ is a tautology.

Exercise:
Is $p \equiv \sim(\sim p)$?

p	***~p***	***~(~p)***
T	F	T
F	T	F

↑ ↑
These are identical,
So, yes they are equivalent

Substitution of Equivalence

- We can make substitutions in statements, using equivalence expressions.
- There are 2 rules:

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 as well, and $[(p \vee q) \Rightarrow r] \vee \sim[(p \vee q) \Rightarrow r]$ is as well.

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 $\sim(\sim p) \vee \sim p$.

Exercise:

$p \Rightarrow q$ is logically equivalent to $\sim p \vee q$. $q \Rightarrow (p \Rightarrow q)$ is a tautology.

Prove that $s \Rightarrow (\sim r \vee s)$ is a tautology.

$q \Rightarrow (p \Rightarrow q)$

- Substitute q for s

$s \Rightarrow (p \Rightarrow s)$

- Substitute r for p

$s \Rightarrow (r \Rightarrow s)$

- Since $p \Rightarrow q$ is logically equivalent to $\sim p \vee q$, we can substitute $r \Rightarrow s$ for $\sim r \vee s$

$s \Rightarrow (\sim r \vee s)$

Truth Tables Cheat Sheet

Conjunction

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

Disjunction

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

Conditionals

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditionals

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Logical Equivalence Laws

Commutative Laws

1. $p \vee q \equiv q \vee p$
2. $p \wedge q \equiv q \wedge p$
3. $p \Leftrightarrow q \equiv q \Leftrightarrow p$

Associative Laws

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

Distributive Laws

1. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (q \vee r)$
2. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
3. $p \Rightarrow (q \vee r) \equiv (p \Rightarrow q) \vee (p \Rightarrow r)$
4. $p \Rightarrow (q \wedge r) \equiv (p \Rightarrow q) \wedge (p \Rightarrow r)$

Double Negative Law

1. $\sim (\sim p) \equiv p$

De Morgan's Laws

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

Implication Laws

1. $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
2. $p \Rightarrow q \equiv \sim p \vee q$
3. $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$
4. $\sim (p \Rightarrow q) \equiv p \wedge \sim q$

Definition

The negation of an *and* statement is logically equivalent to the *or* statement in which each component is negated.

The negation of an *or* statement is logically equivalent to the *and* statement in which each component is negated.

Exercise:
To understand De Morgan's Laws, write negatives of these:

a) John is 6 feet tall and he weighs at least 200 pounds

p: John is 6 feet tall
q: John weighs at least 200 pounds

$\sim(p \wedge q) \equiv \sim p \vee \sim q$

John is not 6 feet tall or he weighs less than 200 pounds

b) The bus was late or Tom's watch was slow

p: the bus was late
q: Tom's watch was slow

$\sim(p \vee q) \equiv \sim p \wedge \sim q$

The bus was not late and Tom's watch was not slow

Exercise:
Prove De Morgan's Laws using truth tables.

$\sim (p \wedge q) \equiv \sim p \vee \sim q$

p	**q**	**$\sim (p \wedge q)$**	**$\sim p \vee \sim q$**
T	T	F	F
T	F	T	T
F	T	T	T
F	F	T	T

$\sim (p \vee q) \equiv \sim p \wedge \sim q$

p	**q**	**$\sim (p \vee q)$**	**$\sim p \wedge \sim q$**
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

Inequalities and De Morgan's Laws

Textbook Exercise:
Use De Morgan's laws to write the negation of $-1 < x \leq 4$.

$-1 < x \leq 4 \equiv (-1 < x) \wedge (x \leq 4)$

By De Morgan's laws, the negation is:

$(-1 \not< x) \vee (x \not\leq 4)$

This is equivalent to:

$(-1 \geq x) \vee (x > 4)$

x is between these points

- De Morgan's laws are frequently used in writing computer programs.
  - For instance, supposed you the program to delete all files modified outside a certain range of dates, say from date1 through date2 inclusive.
  - You would use the fact that:

    ~(*date1* ≤ *file_modification_date* ≤ *date2*)

    is equivalent to:

    (*file_modification_date* < *date1*) or (*date2* < *file_modification_date*)

Exercise:
Is ($p \wedge \sim q) \wedge (\sim p \vee q$) a tautology or a fallacy?

F

T F

$p:T; \sim q:T \quad q:F, \sim p:F$

Since this combination is possible, it is not a tautology.

Exercise:
Is (p <=> q) <=> (~p <=> q) a tautology or a fallacy?

T

T T

$p:T; q:T \quad \sim p:F;$

Since q cannot be a true, the main connective cannot be possible.
This is a fallacy.

F

T F

① T T → F T ✓
② F F → T F ✓

} Wat a tautology

Exercise:

Prove the equivalence $(p \Rightarrow q) \Rightarrow r \equiv [(\sim p \Rightarrow r) \wedge (q \Rightarrow r)]$

p	***q***	**r**	**(p => q)**	**(~p => r)**	**(q => r)**	**(p => q) => r**	**[(~*p* => *r*) ∧ (*q* => *r*)]**
T	T	T	T	T	T	T	T
T	T	F	T	T	F	F	F
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	F	F
F	F	T	T	T	T	T	T
F	F	F	T	F	T	F	F

These are the same

$(p \Rightarrow q) \Rightarrow r \equiv [(\sim p \Rightarrow r) \wedge (q \Rightarrow r)]$

Let α be the tautology $s \Rightarrow t \equiv \sim s \vee t$

$(p \Rightarrow q) \Rightarrow r \equiv (\sim p \vee q) \vee r$ (Substitute $s \Rightarrow t$ for $(p \Rightarrow q)$)

$\equiv (\sim\sim p \wedge \sim q) \vee r$ (De Morgan's) → flip $\vee$ to $\wedge$ by adding negation

$\equiv (p \wedge \sim q) \vee r$ (Double negation)

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

$\equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$ α again

Predicate Logic

- The connectives ~, ∧, ∨, =>, and <=> are not enough to prove or disprove all types of logical statements.
- For example:
  - All UOW math courses are fun,
  - Math 221 is a UOW math course,
  - Therefore, Math 221 is fun.
- This 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."
- **Predicate:** 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 value are denoted: **p(x)**, **q(x)**
- Notation:

Symbol	Name	Example
$\mathbb{R}$	Set of all **real numbers**	Can be integers, fractions, etc…
$\mathbb{Q}$	Set of all **rational numbers**	Can be written as a fraction.
$\mathbb{Z}$	Set of **integers**	Whole numbers … -2, -1, 0, 1, 2, …
$\mathbb{N}$	Set of **natural numbers**	Counting numbers … 1, 2, 3, …
$\in$	**Contention**	"Is contained in," "belongs to," "is a member of…"
$\forall$	**Universal quantifier**	"For all"
$\exists$	**Existential quantifier**	"There exists"
$\ni$	**Such that**	

Exercise:

The predicate p(x): "x is a positive integer strictly less than 5" with $dom_p = \mathbb{Z}$ has truth set {…, -2, -1, 0, 1, 2, 3, 4}.

$dom_p = \mathbb{Z}$ has a truth set $\{1, 2, 3, 4\}$

Exercise:

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

$$\{x : x^2 > x\} = \{x : x < -1 \text{ OR } x > 1\}$$
$$= \{x : |x| > 1\}$$
$$= (-\infty, -1) \cup (1, \infty)$$

The Universal Quantifier ∀

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

Exercise:

a) "All humans are mortal."
b) "All real numbers have a nonnegative square."

a) $\forall$ Humans x, x is mortal
b) $\forall x \in \mathbb{R}$, $x^2 \geq 0$

- **Universal statement:** has the form, ∀ x ∈ D, p(x).
- It is true IFF (if and only if) p(x) is true for every x ∈ D if at least one x ∈ D can be found that makes p(x) false, the statement is false.
- Such an x is called a counterexample (contrapositive).

Exercise:

∀ x ∈ ℝ, $x^2 > x$.

This is false if $x = \frac{1}{2}$ (counterexample)

Exercise:

Write using ∀.

a) All dogs are animals
b) Every integer greater than zero has a prime factor.

a) $\forall$ dogs $x \in$ {animals}
b) $\forall \mathbb{Z}\ x \in$ {PRIMES} $\exists$ $x > 0$

Exercise:

Let D = {1, 2, 3, 4, 5}.

a) Show that the statement ∀ x ∈ D, $x^2 \geq x$ is true.
b) Show that the statement x ∈ D, $\frac{1}{x}$ is false.

a) $x^2 \geq x$, $1^2 \geq 1$, $2^2 \geq 2$, ..., $5^2 \geq 5$ □
This is true.

b) If $x = 1$, $\frac{1}{1^2} \neq \frac{1}{1}$ □
This is false.

The Existential Quantifier ∃

Exercise:

a) "There is a cat in my house."
b) "There are integers m and n such that m + n = mn."

a) $\exists$ A cat $x \ni x$ is in my house.

b) $\exists m, n \in \mathbb{Z} \ni m + n = mn$

- **Existential statement:** has the form $\exists x \in D \ni p(x)$.
- It is true IFF (if and only if) p(x) is true for at least one $x \in D$.
- It is false IFF p(x) is false for all $x \in D$.

Exercise:

Write using ∃.

a) There exists a real number whose square is negative.
b) Some person is a vegetarian.

a) $\exists x \in \mathbb{R} \ni x^2 < 0$

b) $\exists$ Person $x \ni x$ is vegetarian

Exercise:

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

Let $m = 1$, $m \in \mathbb{Z}$

$1^2 = 1$

$\therefore$ This statement is true

Exercise:

Let E = {5, 6, …, 10}. Show that the statement ""$\exists m \in E \ni m2 = m$" is false.

$5^2 \neq 5$, $6^2 \neq 6$, $7^2 \neq 7$, …, $10^2 \neq 10$

$\therefore$ This is false

Exercise:

Rewrite using informal language.

a) $\forall x \in \mathbb{R}, x^2 \geq 0$

b) $\exists m \in \mathbb{Z} \ni m^2 = m$

c) $\forall$ Students s, $\exists$ Math subject y $\ni$ s likes y

d) $\forall x \in \mathbb{R}, x^2 \neq -1$

a) For all real numbers, the square of that number is a positive int.

b) There exists a number in the set of integers where its square is equal to itself.

c) For all students, there exists a math subject where the student likes that math subject.

d) For all real numbers, the square of that number cannot equal -1.

Negation of Quantifiers

- Consider the statement, "all mathematicians wear glasses."
  - What is the negation of the statement?
  - It is natural to think it's "no mathematician wears glasses," but that's not correct.
- The negation is: "there exists a mathematician who does not wear glasses."
- If just one counterexample can be found, the original statement is false.

Negation of a Universal Statement

- The negation of the statement:

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

- This is logically equivalent to the statement:

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

- Symbolically:

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

Exercise:

Write negations:

a) No computer hacker is over 40
b) ∀ Primes p, p is odd
c) ∀ People x, if x is blonde, then x has blue eyes.

a) There exists a computer hacker over 40.
b) There exists a prime number that is even
$\exists p \in \{PRIMES\} \ni p = 2m$
c) ∃ person $x \ni x$ is not blonde and x has blue eyes

- Consider the statement "some fish breathe air."
- What is the negation of this statement?
- It is, "no fish breathes air."
- You might think it should be "some fish do not breathe air," but this and the original statement can both be true at the same time.

Negation of Existential Statements

- The negation of the statement:

  $\exists \mathbf{x} \in \mathbf{D} \ni \mathbf{p(x)}$

- This is logically equivalent to the statement:

  $\exists \mathbf{x} \in \mathbf{D} \ni \mathbf{\sim p(x)}$

- Symbolically:

  $\mathbf{\sim(\exists x \in D \ni p(x)) \equiv \forall x \in D \ni \sim p(x)}$

Exercise:

Write negations.

a) ∃ A triangle whose sum of angles is 200 degrees.
b) There is a woman who is 120 years old.
c) $\exists x \in \mathbb{R} \ni x^2 = -1$

a) $\forall x \in \{\text{triangles}\} \ni$ Sum of angles $\neq 200°$
b) $\forall$ woman $x \in \{\text{Women}\}, x \neq$ 120 years old
c) $\forall x \in \mathbb{R}, x^2 \neq -1$

Summary

- The negation of “all are” is “at least one is not.”
- The negation of “at least one sis” is “all are not.”

Exercise:

Write negations and decide which statements are true.

a) $\exists\, x \in \mathbb{R} \ni 3x = 1$

b) $\forall\, \varepsilon \in \mathbb{R}, \forall\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Q} \ni \varepsilon > 0 \Rightarrow |x - y| < \varepsilon$

a) $\sim(\exists x \in \mathbb{R} \ni 3x = 1) \equiv \forall x \in \mathbb{R},\ 3x \neq 1$

b) $\forall \varepsilon \in \mathbb{R}, \forall x \in \mathbb{Z}, \exists y \in \mathbb{Q} \ni \varepsilon > 0 \Rightarrow |x-y| < \varepsilon$

$\equiv \exists \varepsilon \in \mathbb{R}, \exists x \in \mathbb{Z} \ni \forall y \in \mathbb{Q}, \varepsilon > 0 \wedge |x-y| \geq \varepsilon$

Methods of Proof

Argument → statement
statement
Conclusion
} Assumptions

Arguments

Consider the sequence of statements.

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

- **Argument:** a sequence of statements, all but the final of which are called assumptions/premises/ hypotheses, and final of which is called the conclusion.
- The word "therefore" is normally placed just before the conclusion.
- The logical form of the above argument is:

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

- An argument is **valid** the conclusion is true whenever all the assumptions are true (no matter what particular statements are substituted for the variables).
- **Proof:** 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.

Exercise:

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

$n \in \mathbb{N}$ EVEN (given)
$n = 2m$ for some $m \in \mathbb{N}$ (def. of even numbers).
$x^n = x^{2m}$ (substitution)
$x^n = (x^m)^2$ (rule of exponents)
≥ 0 ($y^2 \geq 0 \; \forall y \in \mathbb{R}$) □

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

Testing Validity

- To test an argument for validity, follow these steps:
  - Identify the assumptions and conclusion.
  - Construct a truth table of all the assumptions and the conclusion.
  - If the conclusion is true in every case where all the assumptions are true, the argument is valid.
  - If there is a row of all true assumptions and false conclusion, the argument is invalid.

Exercise:
Is the argument valid?
P => Q ∨ ~R,
Q => P ∧ R,
∴ P => R.

p	***q***	***r***	***p => q ∨ ~r***	***q => p ∧ r***	***p => r***
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	T
T	F	F	T	T	F
F	T	T	T	F	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

NOT VALID
All assumptions, true,
conclusion MUST
be true.

Exercise:

Test the validity:

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

p	*q*	*r*	*~r*	*p ∨ (q ∨ r)*	*p ∨ q*
T	T	T	F	T	T
T	T	F	T	T	T
T	F	T	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	T	F	T	T	T
F	F	T	F	T	F
F	F	F	T	F	F

This statement satisfies the validity test.

b) $p \Rightarrow q$, (Modus Ponens)
p,
$\therefore q$.

p	*q*	*p => q*
T	T	T
T	F	F
F	T	T
F	F	T

This syllogism is valid.

- An argument consisting of 2 premises 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.

Exercise:

a) Is the statement "$n \in \mathbb{N}$ is even => n^2 is even" true? Prove it.

b) Let n = 9866. Is it true or false to say n^2 is even?

a) $n = 2m$, $n \in \mathbb{N}$ (definition of even numbers)

$$n^2 = (2m)^2$$
$$= 4m^2$$
$$= 2(2m^2)$$

$\therefore n^2$ is even $\square$

b) Let $n = 9866$,

$$n^2 = (9866)^2$$
$$= 97,337,956$$

$\therefore n^2$ is even

Principles of Mathematical Induction

- If p(n) is a statement with $dom_p = \mathbb{N}$ such that
  a) p(1) is true, and
  b) p(k) true => p(k + 1) true,

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

Exercise:

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

Review this

A: $p(n): 4^n - 1$ is a multiple of 3

$$\frac{4^n - 1}{3} = m \text{ for some } m \in \mathbb{Z}$$

$$\Rightarrow 4^n - 1 = 3m$$

$$\Rightarrow 4^n = 3m + 1$$

← very first case of $\mathbb{N}$

a) $p(1): 4^1 - 1 = 4 - 1 = 3$, a multiple of 3. (Proved first case)

b) $p(k+1)$: Let $4^k - 1$ be a multiple of 3, $\frac{4^{k+1} - 1}{3}$ is a whole number?

$$\Rightarrow \frac{4^{k+1} - 1}{3} = \frac{4 \cdot 4^k - 1}{3}$$

$$= \frac{4(3m+1) - 1}{3}$$

$$= \frac{12m + 4 - 1}{3}$$

$$= 4m + 1 \in \mathbb{Z} \quad \square$$

whole number in $\mathbb{Z}$

$\therefore 4^n - 1$ is a multiple of 3 for all $n \in \mathbb{N}$

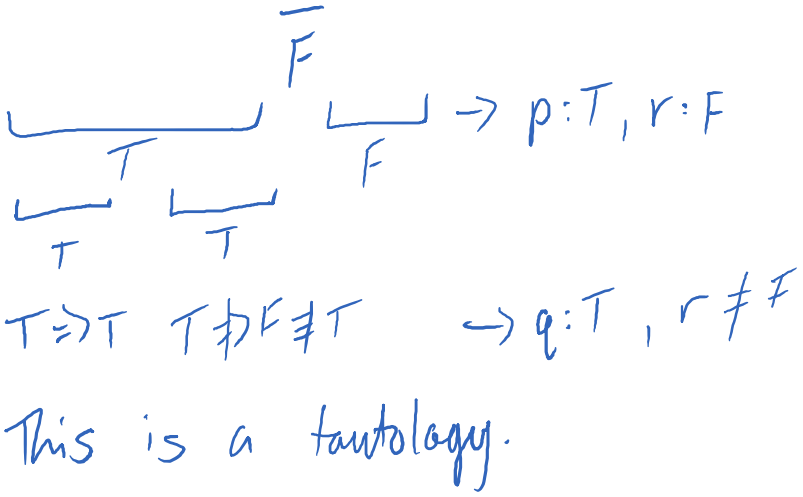
p(k) – any general case

Induction b only applicable to $\mathbb{N}$

The Law of Syllogisms

- Is the following a tautology?

  [([p => q) ∧ (q => r)] => p => r



This is a tautology.

> **Law of Syllogism**
>
> If p => q and q => r, then p => r

Exercise:

Suppose these 2 statements are true.

a) If it rains today, then I'll drive to school.
b) If I drive to school today, then I'll go over my gas budget.

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

c) If it rains today, then I'll go over my gas budget.

Proving ∃ Statements

- How do we prove a statement of the form?

  ∃ x ∈ D ∋ p(x)

- We need to find at least one x ∈ D that makes p(x) true.

Exercise:

Prove that there exists an even number that can be written in two ways as the sum of two prime numbers.

Find one example that makes p(x) true.

2 = 1 + 1, 4 = 2 + 2, 8 = 5 + 3, 10 = 7 + 3, 5 + 5 ⇒ 10

Exercise:

Prove $\exists x \in \mathbb{R} \ni x + 5 = 0$

If $x = -5$, $(-5) + 5 = 0$ □

Exercise:

Prove there is a month of the year whose name has 3 letters.

May

Proving ∀ Statements

- How do we prove a statement of the form:

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

- There are two options:
  1) **Method of Exhaustion**
  2) **Generalized Proof**

- The method of exhaustion checks that p(x) is true for every $x \in D$.
- This is dine when D is small, but becomes a lot of work for D large.
- If D is infinite, this method fails to be of any use.

Exercise:

Prove that every even number between 4 and 16 can be written as the sum of 2 primes.

$4 = 3 + 1$ $\quad 10 = 5 + 5$ $\quad 16 = 11 + 5$

$6 = 3 + 3$ $\quad 12 = 7 + 5$

$8 = 3 + 5$ $\quad 14 = 7 + 7$

$\therefore$ As proven above □

Exercise:

Prove that every even $n \in \mathbb{N}$ can be written as the sum of 2 primes.

$p(n)$: $\forall$ even $n \in \mathbb{N} \exists\ n = m + n$, $m, n \in \mathbb{P}$.

Let $k = 1$, $n = 2$,

$\Rightarrow 2 = 1 + 1$

$\therefore$ This statement is not true for $n \leq 2$

Trick Question

- The generalized proof is constructed so that it applies to every possible situation.

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.

Exercise:

Prove that if a, b ∈ ℤ, then 10a + 8b is divisible by 2.

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

Since $a, b \in \mathbb{Z}$, $5a + 4b \in \mathbb{Z}$

$\Rightarrow 2(5a + 4b)$ is even (given even number definition $n = 2m$)

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

Disproving ∃ Statements

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

  ~(∃ x ∈ D ∋ p(x)) ≡ ∀ x ∈ D ∋ ~p(x)

- To disprove an ∃ statement, we must prove a ∀ statement, via method of exhaustion or generalized proof.

Exercise:

Disprove the statement "there exists an even prime number larger than 2."

A: p(n): "there exists an even prime number larger than 2"

~p(n): "for all prime numbers x larger than 2, x is odd"

Let $x > 2$ be prime.

Suppose x is even, then $x = 2n$ for some $n \in \mathbb{N}$

$\Rightarrow \frac{x}{2} = \frac{2n}{2} = n$,

So x is divisible by 2 and is not a prime.

- This is an example of proof by contradiction.

Disproving ∀ Statements

- To disprove a ∀ statement, we must prove an ∃ statement.

  ~(∀ x ∈ D, p(x)) ≡ ∃ x ∈ D ∋ ~p(x)

- We must find one x ∈ D such that p(x) is false (a counterexample).

Exercise:

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

$p(n): \forall x \in \mathbb{R}, x < 0 \vee x > 0$

$\sim p(n): \exists x \in \mathbb{R} \ni x \not> 0 \wedge x \leq 0$

Let $x = 0$, then $x \not> 0 \wedge x \leq 0$ □

Exercise:

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

$\sim p(n): \exists a, b \in \mathbb{R} \ni$ if $a^2 = b^2 \wedge a \neq b$

Let $a = 1$, $b = -1$, then

$\Rightarrow a^2 = b^2 \wedge a \neq b$

$1^2 = (-1)^2 \wedge 1 \neq -1$ □

∴ The original statement is not true

Exercise:

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

A: $x + y = 0$, $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$

Let $x \in \mathbb{R}$, $y = -x$, then $y \in \mathbb{R}$ and

$\Rightarrow x + y = x + (-x) = 0$ □

Generalized Proof 1: Direct Proof

- A **direct proof** works in a straightforward manner from assumptions to solution.
- We often rewrite assumptions in logical notation.

Exercise:

Prove that if 3x – 9 = 15, then x = 8.

A: $3x - 1 = 15$

$3x = 15 + 1$

$x = \frac{16}{3}$

$x = 8$ □

Exercise:

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

A: Let a, b be even, then $\exists c, d \in \mathbb{Z} \ni a = 2c, b = 2d$

$a + b = 2c + 2d$

$= 2(c + d)$ $c, d \in \mathbb{Z} \Rightarrow c + d \in \mathbb{Z}$.

$\Rightarrow a + b = 2e, e \in \mathbb{Z}$

$\therefore a + b$ is even.

Exercise:

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 $y \in \mathbb{Z}$)

A: Let $a, b \in \mathbb{Z}$ be two perfect squares $\exists x, y \in \mathbb{Z} \ni a = x^2, b = y^2$

$ab = x^2 \cdot y^2$

$= (xy)^2$

$\therefore ab = k^2$ where $k \in \mathbb{Z}$ □, ab is a perfect square

Exercise:

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

A: $-x^2 + 2x + 1 \leq 2 \Leftrightarrow -x^2 + 2x - 1 \leq 0$

$\Leftrightarrow x^2 + 2x + 1 \geq 0$

$\Leftrightarrow (x-1)^2 \geq 0$ (Tautology)

This is always positive

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

Generalised Proof 2: Proof by Contradiction

Exercise:

Prove that p => q ≡ ~q => ~p

← Can do

p	*q*	*p => q*	*~q => ~p*
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

- To prove p => q, one may instead prove ~q => ~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.

Exercise:

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

$p(n)$: n^2 is even, $n^2 = 2m$

$q(n)$: n is even, $n = 2m$

If $p \Rightarrow q$, we will prove $\sim q \Rightarrow \sim p$

Let n be odd, $\exists m \in \mathbb{Z} \ni n = 2m + 1$

$$\begin{aligned} n^2 &= (2m+1)^2 \\ &= (2m+1)(2m+1) \\ &= 4m^2 + (2m + 2m) + 1 \\ &= 4m^2 + 4m + 1 \\ &= 2(2m^2 + 2m) + 1 \end{aligned}$$

$\therefore n^2$ is odd

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

Exercise:

Prove by contradiction that $y \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow y + 7 \in \mathbb{R} \setminus \mathbb{Q}$. — irrationals

A: To prove, assume $y+7 \in \mathbb{Q}$ and show that $y \in \mathbb{Q}$

Let $y + 7 \in \mathbb{Q}$, then $\exists a, b \in \mathbb{Z}, b \neq 0 \ni y + 7 = \frac{a}{b}$

$$\begin{aligned} y &= \frac{a}{b} - 7 \\ &= \frac{a}{b} - \frac{7b}{b} \\ &= \frac{a - 7b}{b} \in \mathbb{Q} \end{aligned}$$

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

Set minus symbol "\"

{Real numbers} set minus {rationals} $\therefore$ {irrationals}

Generalized Proof 3: 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 $x \neq 0$, the if $y \neq 0$.
- Any statement of the form:

  $(p \vee q) \Rightarrow r$

  Can be done this way, because of the logical equivalence

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

Exercise:

Prove "$x \neq 0$ or $y \neq 0 \Rightarrow x^2 + y^2 > 0$."

Case 1: Let $x \neq 0$, then $x^2 > 0$, and $y^2 \geq 0$
$\Rightarrow x^2 + y^2 > 0$

Case 2: Let $y \neq 0$, then $x^2 \geq 0$, and $y^2 > 0$
$\Rightarrow x^2 + y^2 > 0$

$\therefore$ If $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$

Exercise:

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

Case 1: Let m be even, the 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 (odd + odd = even)
$\Rightarrow m^2 + m + 1$ is odd.

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

Numbers

- **Set:** a collection of objects called **elements**.
- We write x ∈ 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 ∅
- **Subset:** A subset of S is a set T with the property $x \in T \Rightarrow x \in S$.
- Every element of T is an element of S.
- Trivially, S ⊆ S and ∅ ⊆ S
- The subset symbol is denoted by ⊆.
- 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.
- **Binary operations:** combines pairs of elements to prove another.

A binary operation $*$ is **closed** if:

Definition

$$x, y \in S \Rightarrow x * y \in S$$

- Four common operations on numbers are $+, -, \cdot, /$.

Exercise:

Are +, -, ·, / closed on ℕ? Prove or disprove

+) $a, b \in \mathbb{N} \Rightarrow a+b \in \mathbb{N}$ (Closed)

-) $1, 5 \in \mathbb{N} \Rightarrow 1-5 = -4 \notin \mathbb{N}$ (Not closed)

·) Closed on ℕ

/) $5, 3 \in \mathbb{N} \Rightarrow \frac{5}{3} \notin \mathbb{N}$ (Not closed)

An element e ∈ S is called an **identity** if:

Definition

$$x * e = x \; AND \; e * x = x \; \forall \; x \in S$$

Exercise:
Does $\mathbb{N}$ have an identity under $+$? Under $\cdot$?

+) $e + x = x \wedge x + e = x$
Let $x = 1$, $e = 2$
$1 + 2 \neq 1 \wedge 2 + 1 \neq 1$
$\therefore$ Under $+$ binary operations on set of $\mathbb{N}$, there is NO identity.

•) $e \cdot x = x \wedge x \cdot e = x$
Let $e = 1$, $x = 2$,
$1 \cdot 2 = 2 \wedge 2 \cdot 1 = 2$
$\therefore$ Under $\cdot$ binary operations, $e = 1$ is the identity.

If $\exists\ e$ identity of S, an element $x \in S$ is called **invertible** when $\exists\ y \in S \ni$:

> *Definition*
> $x * y = e$ *AND* $y * x = e$

Then **y** is called the **inverse** of **x**.

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

+) No identity $\therefore$ no invertible elements
•) $x \cdot y = e \wedge y \cdot x = e$
Let $x = 1$, $y = 1$
$1 \cdot 1 = 1 \wedge 1 \cdot 1 = 1$
$\therefore$ Under $\cdot$ for the set of $\mathbb{N}$, 1 is an inverse of itself.

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

> *Definition*
> $x * y = y * x \ \forall\ x, y \in S$

It is **associative** if:

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

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

Exercise:

Rock-Paper-Scissors.

Let M = {r, p, s} and consider the binary operation that gives the winner of the game.

$r * p = p * r = p$

$s * p = p * s = s$

$r * s = s * r = r$

} Communative.

$p * p = s * s = r * r =$ TIE

Is $*$ associative?

$(r * p) * s \neq r * (p * s)$ □

∴ Rock-paper-Scissors is not associative.

A binary operation $*$ is **distributive** over another $\cdot$ if for all $a, b, c \in S$.

Definition

$\boldsymbol{a * (b \cdot c) = (a * b) \cdot (a * c)}$ ***AND*** $\boldsymbol{(a \cdot b) * c = (a * c) \cdot (b * c)}$

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

Exercise:

Prove that addition does not distribute over multiplication on $\mathbb{N}$.

$a + (b \cdot c) = (a + b) \cdot (a + c) \wedge (a \cdot b) + c = (a + b) \cdot (b + c) \quad \forall a, b, c \in \mathbb{N}$

Let $a = 1, b = 2, c = 3 \in \mathbb{N}$

$1 + (2 \cdot 3) = (1 + 2) \cdot (1 + 3)$

$7 \neq 6$ □

∴ + does not distribute over · $\forall a, b, c \in \mathbb{N}$

Exercise:

Let a, b ∈ ℕ. Simplify the following expression, giving reasons for each step. [8(a + b)] + 2a

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

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

$= (8 + 2)a + 2b$ (distribution)

$= 10a + 2b$ □

A set S with order ≤ is called **well-ordered** if every nonempty subset T of S has at least one smallest element.

> *Definition*
> That is, if $\boldsymbol{T \subseteq S, T \neq \emptyset}$, then $\exists\ \mathbf{s_0 \leq s}\ \forall\ \mathbf{s \in T}$

The set ℕ with the usual order ≤ is well-ordered.

The set of integers ℤ = {..., -2, -1, 0, 1, 2, ...} can be constructed from ℕ:

- It is the set of differences {m-n} ∀ m, n ∈ ℕ.
- The order ≤ on ℕ extends to ℤ.

Exercise:

a) Are +, -, ·, / closed on ℤ?
b) Does ℤ has identities under +, ·?
c) What are the invertible elements of ℤ under +, ·?

a) $x, y \in \mathbb{Z} \Rightarrow x * y \in \mathbb{Z}$
+) Yes, closed.
-) Yes, closed.
·) Yes, closed
/) Not closed, $1, 0 \in \mathbb{Z} \not\Rightarrow 1/0 \notin \mathbb{Z}$

b) $x * e = x \wedge e * x = x \quad \forall x \in \mathbb{Z}$
+) $e = 0$
·) $e = 1$

c) $x * y = e \wedge y * x = e$
+) If $\exists e$, x is invertible if
$\exists y \ni x + y = 0 \wedge y + x = 0$
Let $x < 0$, then $y = -x$
$\therefore x + (-y) = 0 \wedge -y + x = 0 \quad \forall x \in \mathbb{Z}$
·) Proof: $x \neq \pm 1 \Rightarrow \frac{1}{x} \notin \mathbb{Z}$

- On ℤ, + and · are commutative and associative.
- On ℤ, - and / are **not** commutative and associative.
- However, if we define a **– b = a + (-b)** and **a/b = a · 1/b**, then we have commutativity and associativity.

$\boldsymbol{a - b \neq b - a, BUT\ a + (-b) = -b + a}$ (associativity)
$\boldsymbol{\frac{a}{b} \neq \frac{b}{a}, BUT a \cdot \frac{1}{b} = \frac{1}{b} \cdot a}$ (distribution)

- Multiplication distributes over addition and subtraction on $\mathbb{Z}$:

$$\boldsymbol{a} \cdot (\boldsymbol{b} \pm \boldsymbol{c}) = (\boldsymbol{a} \cdot \boldsymbol{b}) \pm (\boldsymbol{a} \cdot \boldsymbol{c})$$
$$(\boldsymbol{a} \pm \boldsymbol{b}) \cdot \boldsymbol{c} = (\boldsymbol{a} \cdot \boldsymbol{c}) \pm (\boldsymbol{b} \cdot \boldsymbol{c})$$

Exercise:
Is $\mathbb{Z}$ well-ordered?

Well Ordered: if $T \subseteq S$, $T \neq \emptyset$, then $\exists s_0 \in S \; \forall s \in T$
Given $T = \{x \in T \ni -x\}$
$= \{\mathbb{Z}^-\}$

Some Common Rules

An integer $m \in \mathbb{Z}$ is **even** if $m = 2k$ for some $k \in \mathbb{Z}$.
An integer $m \in \mathbb{Z}$ is **odd** if $m = 2k + 1$ for some $k \in \mathbb{Z}$
An integer $m > 1$ is **prime** if whenever $m = rs$ for $r, s \in \mathbb{N}$, either $r = 1$ or $s = 1$
An integer $m > 1$ is **composite** if it is not prime (i.e. $m = ab$ with $a, b > 1$ AND $a, b < m, a, b \in \mathbb{N}$)

- The set of Rationals $\mathbb{Q}$ is the set of numbers q that can be written $q = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$
- $\mathbb{Q}$ can be constructed from $\mathbb{Z}$.

Dedekind Cuts

- To construct the Real Numbers $\mathbb{R}$, we can 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:
  - A and B are nonempty
  - $A \cup B = \mathbb{Q}$
  - A is closed downwards: If $q \in A$ and $r < q$, then $r \in A$
  - B is closed upwards: if $q \in B$ and $r > q$, then $r \in B$
  - A contains no greatest element: $\forall\, q \in A \; \exists\, r \in A \ni q < r$

- Given $q \in Q$, we can form a Dedekind Cut (A,B) where:

$$A = \{x \in Q : x < q\} \text{ AND } B = \{x \in Q : x \geq q\}$$

- That is the Dedekind-Cut identification of all rational numbers $q \in \mathbb{Q}$
- But we can make such cuts at non-rational numbers as well.
- An irrational number is one that cannot be written as $\frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$.
  - An example is $\sqrt{2}$

Exercise:

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

- The following Dedekind Cut defines $\sqrt{2}$:

  $\boldsymbol{A = \{x : x < 0 \ OR \ x^2 < 2\}, B = \{x : x > 0 \ AND \ x^2 \geq 2\}}$

- The numbers defined by <u>ALL</u> Dedekind Cuts of $\mathbb{Q}$ make up the set of Real Numbers $\mathbb{R}$.
- The usual order $\leq$ on $\mathbb{R}$ is inherited from $\mathbb{N}$.

Exercise:

a) Which of $+, -, \cdot, /$ are closed on $\mathbb{R}$?
b) Does $\mathbb{R}$ have identities under $+, \cdot$?
c) What are the invertible elements of $\mathbb{R}$ under $+, \cdot$?

a) $*$ is closed on S if $\forall a, b \in S, a * b \in S$
$+, -, \cdot$ are closed on $\mathbb{R}$
$/$ is not closed on $\mathbb{R}$ e.g. $1, 0 \in \mathbb{R}$, $\frac{1}{0} \notin \mathbb{R}$

b) Under $+$, $\mathbb{R}$ has the identity $e = 0$
Under $\cdot$, $\mathbb{R}$ has the identity $e = 1$

c) Under $+$, all values are invertible in $\mathbb{R}$
Under $\cdot$, all values except 0 are invertible.

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

Induction

- Recall the induction principle:

  If $dom_p = \mathbb{N}$ such that,
  a) $p(1)$ is true
  b) $p(k)$ is true $\Rightarrow p(k+1)$ is true
  Then $p(n)$ is true $\forall\, n \in \mathbb{N}$

Exercise:

1) Prove that $1 + 2 \ldots + n = \frac{n(n+1)}{2}$ $\forall\, n \in \mathbb{N}$

1) $p(n): \frac{n(n+1)}{2} \iff \sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

a) $p(1): \frac{1(1+1)}{2} = 1$ ✓

b) Suppose $1 + 2 + \ldots + k = \frac{k(k+1)}{2} \iff \sum_{j=1}^{k} j = \frac{k(k+1)}{2}$

Prove that $1 + 2 + \ldots + k \quad \frac{(k+1)(k+2)}{2}$

$$\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2} = \sum_{j=1}^{k} j = \frac{k(k+1)}{2} + (k+1) \quad \text{(By the supposition)}$$

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

$$= \frac{k^2 + 3k + 2}{2}$$

$$= \frac{(k+1)(k+2)}{2} \quad \square$$

2) Prove that $n^3 > 2n - 2 \; \forall n \in \mathbb{N}$

$p(1): 1^3 > 2(1) - 2 \iff 1 > 0$ ✓

$p(k)$: Suppose $k^3 > 2k - 2$, prove that $(k+1)^3 > 2(k+1) - 2$

$(k+1)^3 = k^3 + 3k^2 + 3k + 1$

$> (2k-2) + 3k^2 + 3k + 1$ (By the supposition)

$= 3k^2 + 5k - 1$

Substituted

$(k+1)^3 > 2(k+1) - 2 \iff 3k^2 + 5k - 1 > (2k+2) - 2$

$\iff 3k^2 + 5k - 1 > 2k$

$\iff 3k^2 + 3k - 1 > 0$

$\iff 3k(k+1) > 1$

$\iff k(k+1) > \frac{1}{3}$ □ ✓

$\therefore n^3 > 2n - 2 \; \forall n \in \mathbb{N}$

3) Prove that $(n+1)! \geq 2^n \; \forall n \in \mathbb{N}$

$(n+1)! \geq 2^n$

a) $p(1): (1+1)! \geq 2^1 \iff 2 \geq 2$ ✓

b) Suppose $(k+1)! \geq 2^k$ is true.

c) Prove that $((k+1)+1)! \geq 2^{k+1}$

$(k+2)! = (k+1)!(k+2)$ ← Substitute case k

$\geq 2^k (k+2)$ (By the supposition)

$= k2^k + 2 \cdot 2^k$

$\geq k2^k + 2^{k+1}$ ← from case k, already supposed to true; adding any number makes the sign >

$> 2^{k+1}$

$\therefore (n+1)! \geq 2^n \; \forall n \in \mathbb{N}$

4) Prove that $6 \mid (3n^2 + 3n)\ \forall n \in \mathbb{N}$ (a|b: "a divides b")

$p(n)$: $6 \mid (3n^2 + 3n)\ \forall n \in \mathbb{N}$

$p(1)$: $6 \mid 3(1)^2 + 3(1) = 6 \mid 6$ ✓

$p(k)$: Suppose $6 \mid (3k^2 + 3k)$

$p(k+1)$: Prove $6 \mid [3(k+1)^2 + 3(k+1)]$

$$3(k+1)^2 + 3(k+1) = 3(k^2 + 2k + 1) + 3k + 3$$
$$= 3k^2 + 3k + 6k + 6$$
$$= (3k^2 + 3k) + 6(k + 1)$$

$(3k^2 + 3k) + (k+1) =$ (By the Supposition)

How did you go from * to $6\left(\frac{3k^2+3k}{6} + k + 1\right)$

Supposition, but why the 6

Sigma Notation

We use capital sigma $\sum$ to shorten notation of long sums:

$$\sum_{i=0}^{k} a_i = a_1 + a_2 + a_3 + \cdots + a_k$$

Exercise:

Expand

a) $\sum_{i=2}^{6} 2i^2$

b) $\sum_{i=1}^{10} 2$ ← constant

a) $2 \cdot 2^2 + 2 \cdot 3^2 + 2 \cdot 4^2 + 2 \cdot 5^2 + 2 \cdot 6^2 = 180$

b) $2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 = 20$

Exercise:

Simplify

a) $1 + 3 + 5 + \cdots + 13$

b) $1 + 4 + 9 + \cdots + m^2$

a) $\sum_{i=0}^{13} 2i + 1$ b) $\sum_{i=1}^{n} i^2$

- By the laws of addition, we have the following properties:

1)

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

2)

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

Generalised Mathematical Induction

- Let $p(n)$ be defined for all $n \in \mathbb{N}$, and let $a \in \mathbb{N}$. If
  a) $p(a)$ is true, and
  b) For all $k \in \mathbb{N}, k \geq a$, $p(k)$ is true $\Rightarrow p(k+1)$ is true
  Then $p(n)$ is true for all $n \in \mathbb{N} \ni n \geq a$

Exercise:

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

If we tried $p(1)$: $2^1 > 2(1) + 1 \Leftrightarrow 2 \not> 3$

Prove that $2^n > 2n+1 \; \forall n \geq 3$

$p(3)$: $2^3 > 2(3) + 1 \Leftrightarrow 8 > 7$ ✓

$p(k)$: $2^k > 2k + 1$, $k \geq 3$, prove that $2^{k+1} > 2(k+1) + 1$

$p(k+1)$: $2^{k+1} > 2(k+1) + 1$

$2^{k+1} = 2 \cdot 2^k > 2(2k+1) = 4k + 2$ (By the supposition)

$4k + 2 > 2(k+1) + 1 \Leftrightarrow 4k + 2 > 2k + 3$

$\Leftrightarrow 2k + 2 > 3$

$\Leftrightarrow 2k > 1$ □

$\therefore 2^n > 2n+1 \; \forall n \geq 3$

Exercise:

Prove that.

$$\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \quad \forall\, n \geq 2$$

$P(2)$: $\sum_{i=1}^{2-1} \frac{i}{i+1} < \frac{k^2}{k+1} \iff \frac{1}{1+1} < \frac{2}{2+1} \iff \frac{1}{2} < \frac{4}{3}$ ✓

$P(k)$: Suppose $\sum_{i=1}^{k-1} \frac{i}{i+1} < \frac{k^2}{k+1}$. Prove $\sum_{i=1}^{k} \frac{i}{i+1} < \frac{(k+1)^2}{k+2}$

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

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

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

$$\therefore \sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \quad \forall\, n \geq 2$$

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 $a_1, a_2, \ldots, a_{n_0}$.

Exercise:

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

$a_3 = 5a_2 - 6a_1 = 5 \cdot 4 - 6 \cdot 1 = 14$

$a_4 = 5a_3 - 6a_2 = 5 \cdot 14 - 6 \cdot 4 = 46$

Exercise:

The Fibonacci numbers are the numbers in the famous sequence:

1, 1, 2, 3, 5, 8, 13, …

This sequence is defined by:

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

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

- Using induction

Strong Mathematical Induction

- Let $p(n)$ be defined for all $n \in \mathbb{N}$m let $a \in \mathbb{N}$ if:
  a) $p(1), p(2), \ldots, p(a)$ are true, AND
  b) For all $k \in \mathbb{N}, k \geq a, p(k)$ is true $\Rightarrow p(k+1)$ is true,
  Then $p(n)$ is true for all $n \in \mathbb{N}$.

Exercise:

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

a) $p(1)$: $f_1 : 1 < 2^1 = 2$ ✓

$p(2)$: $f_2 : 1 < 2^2 = 4$ ✓

$p(3)$: $f_3 : 2 < 2^3 = 8$ ✓

b) Suppose for $k \geq 3$, $f_1 < 2^1, f_2 < 2^2, \ldots, f_k < 2^k$.

Prove $f_{k+1} < 2^{k+1}$

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

$\therefore f_n < 2^n\ \forall n \in \mathbb{N}$

Exercise:

Let $a_1 = 2, a_2 = 4, a_n = 5a_{n-1} - 6a_{n-2}\ \forall\ n \geq 3$. Prove that $a_n = 2^n\ \forall\ n \in \mathbb{N}$.

① $a_1 = 2^1, a_2 = 2^2, a_3 = 5 \cdot 4 - 6 \cdot 2 = 8 = 2^3$. ✓

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

$a_{k+1} = 5a_k - 6a_{k-1} = 5 \cdot 2^k - 6 \cdot 2^{k-1}$

$= 5 \cdot 2^k - 3 \cdot 2^k = 2 \cdot 2^k = 2^{k+1}$ ✓

$\therefore a_n = 2^n\ \forall n \in \mathbb{N}$

Number Theory

- Let $n, d \in \mathbb{Z}, d \neq 0$ we say 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 $d \nmid n$

Definition - Transitivity of Divisibility:

If $a, b, c \in \mathbb{Z} \ni a|b$ AND $b|c$, then $a|c$

Proof:

$a|b \Rightarrow \exists d \in \mathbb{Z} \ni b = ad$

$b|c \Rightarrow \exists e \in \mathbb{Z} \ni c = be$

$\Rightarrow c = be = (ad)e = a(de), de \in \mathbb{Z}$

$\therefore a|c$

Definition – Divisibility by Primes:

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

Proof: (Strong Induction)

a) $2|2$

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

Case 1: $k + 1$ is a prime. Then $(k + 1)|(k + 1)$

Case 2: $k + 1$ is composite. Then $k + 1 = ab$ for some $a, b \in \mathbb{N}\{1\}$,

$a, b < k + 1$

By hypothesis, $\exists c\ Prime \ni c|a$. Since $c|a\ AND\ a|(k + 1)$, by transitivity $c|(k + 1)$

$\therefore$ Every $n \in \mathbb{N}\{1\}$ is divisible by a prime.

Exercise:

Find a prime factor:

a) 693 ← 3, 11

b) 1048

↑ 2

Theorem:
There are infinitely many primes.

Proof: (by contradiction)

Suppose there are finitely many Primes, $p_1, p_2, p_3, \dots, p_n$.
Construct a number p defined by $p = p_1 p_2 \dots p_n + 1$.

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), $p_1 | p_2$ ← Can be switched with any other prime

$$\frac{p}{p_1} = \frac{p_1 p_2 \dots p_n + 1}{p_1} = p_2 p_3 \dots p_n + \frac{1}{p_1} \notin \mathbb{Z}$$ ← a contradiction

Not an integer. Strictly less than 1.

∴ There are infinitely many primes.

Quotient-Remainder Theorem

- If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there exists a unique $q, r \in \mathbb{Z}$ such that:

  $n = dq + r \; AND \; 0 \leq r < d$

> *Definition*
>
> $\boldsymbol{n = dq + r \; AND \; 0 \leq r < d}$

Exercise:
Find $q, r \in n = dq + r, 0 \leq r < d$.

a) $n = 54, d = 4$
b) $n = -32, d = 7$
c) $n = 42, d = 70$

a) $54 = 4 \cdot 13 + 2$ ← unique representation
Could also say:
$54 = 4 \cdot 11 + 10$ ← however, doesn't satisfy $r < d$

b) $-32 = 7 \cdot (-5) + 3$ ← what neg. int. that is just below -32.
-5 gives -35, $r = +3$, $n = -32$.

c) $42 = 70 \cdot 0 + 42$

Fundamental Theorem of Arithmetic

- Every $a \in \mathbb{N}\{1\}$ can be factorized uniquely in the form:

  $a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$

  Where $k \in \mathbb{N}, \alpha_i \in \mathbb{N}\ \forall\ i, AND\ P_i\ is\ PRIME\ \forall\ i$

Proof:

The proof requires the following Lemma:

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

First, we show that every $a \in \mathbb{N}\{1\}$ is either a prime or a product of primes, by strong induction.

a) 2 is prime.
b) Suppose $2, 3, \dots, k$ are all either prime or product of primes.
   Prove that $k+1$ is either prime or product of primes.
   a. If $k+1$ is prime → there is nothing more to prove.
   b. If not, then it is a composite: $\exists\ Integers\ b, c \ni 1 < b \leq c < k+1\ and\ k+1 = bc$

      By hypothesis, $b = p_1 p_2 \dots p_j$ and $c = q_1 q_2 \dots q_m$ are products of primes.
      Then $k+1 = bc = p_1 p_2 \dots p_j q_1 q_2 \dots q_m$ is a product of primes.
      ∴ Ever $a \in \mathbb{N}\backslash\{1\}$ is either prime or a product of primes.

   Now we show uniqueness, by contradiction.
   Assume that $a > 1$ is the product of primes in two different ways:

   $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$

   Since $p_1|a$, Euclid's Lemma says p, divides one of the q_j. Without loss of generality, let $p_1|q_1$. Since q, is prime, its divisors are 1 and q. Hence, $p_1|q_1$, and:

   $$\frac{a}{p_1} = p_2 p_3 \dots p_m = q_2 q_3 \dots q_n$$

   By the same logic, p_2 must divide one of the remaining q_j, WLOQ $p_2|q_2$. Then

   $$\frac{a}{p_1 p_2} = p_3 p_4 \dots p_m = q_3 q_4 \dots q_n$$

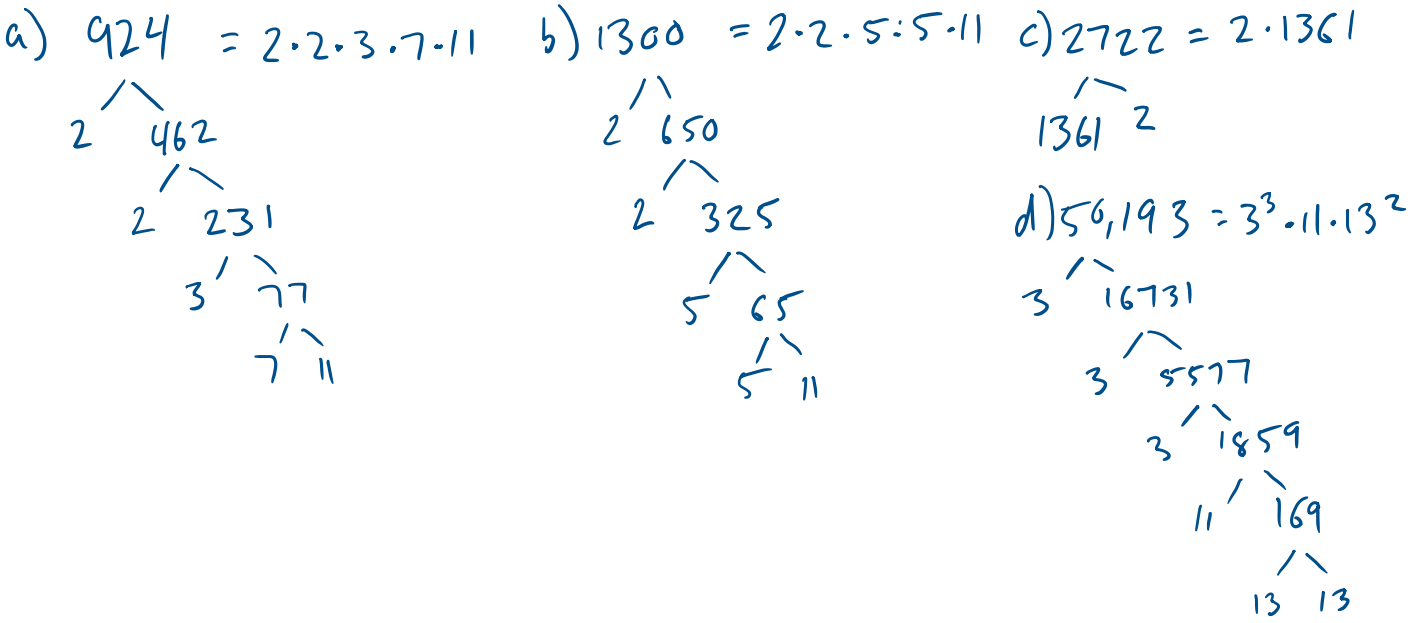
   Continuing like this, we find that $m \leq n$ and $p_i = q_i\ \forall\ i \in \{1, 2, \dots, m\}$.
   The same argument with the p primes and q primes reversed gives us that $n \leq m$ and $q_i = p_i\ \forall\ i \in \{1, 2, \dots, n\}$.
   Therefore, $m = n$ and we have that the two factorizations are the same.

Exercise:

Find the prime factorization.

NOTE: PRIMES = {2 3 5, 7, 11, 13, 17, 19, 23 29 31 37...}

a) 924
b) 1300
c) 2722
d) 50,193



Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$ with at least one of a, b nonzero.
- The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$ is the number c such that:
  - c is a common divisor of a and b: $c|a$ and $c|b$
  - If d is a common divisor of a and b, then $d \leq c$

Definition

$\boldsymbol{a, b \in \mathbb{Z}, a, b \neq 0,} \qquad \boldsymbol{gcd(a, b) = c}$

Exercise:
$\gcd(18, 12) = 6$, since $6|18$ and $6|12$, and there is no bigger integer that divides them both.

Note: $\gcd(18, 12) = \gcd(-18, 12) = \gcd(18, -12) = \gcd(-18, -12)$

- **Prime factorizations** can be used to find $gcd(a, b)$, if:

  $a = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ and $b = P_1^{\beta_1} \dots P_k^{\beta_k}$ (some α_i, β_i can be zero), then

  $\gcd(a, b) = P_1^{\gamma_1} \dots P_k^{\gamma_k}, where\ \gamma_i = \min\{\alpha_i, \beta_i\}$

Exercise:
Given that $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have:

$\gcd(3220, 1155) = 5 \cdot 7 = 35$

Least Common Multiples (LCM)

- Let $a, b \in \mathbb{Z}$ with at least one of a, b nonzero.
- The **least common multiple** of a and b, denoted by $lcm(a, b)$, is the number $c \in \mathbb{N}$ such that:
  - c is a common multiple of a and b, i.e., $a|b \; and \; b|c$.
  - If d is a common multiple of a and b, then $c \leq d$.

Exercise:

a) $lcm(12, 4) = 12$
b) $lcm(18, 15) = 90$

- We can use **prime factorization** to calculate $lcm(a, b)$, if:

  $a = P_1^{\alpha_1} \dots P_k^{\alpha_k} \; AND \; b = P_1^{\beta_1} \dots P_k^{\beta_k}$ (some α_i, β_i can be zero), then

  $lcm(a, b) = P_1^{\gamma_1} \dots P_k^{\gamma_k}, where \; \gamma_i = \max\{\alpha_i, \beta_i\}$

Exercise:

Given that $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ and $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, we have:

$lcm(3220, 1155) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 106,260$

Exercise:

a) Find $lcm(35100, 6975)$
b) Find $lcm(268944, \; 198466)$

a) lcm(35100, 6975)

$35100 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 13$

$6975 = 3^2 \cdot 5^2 \cdot 31$

$lcm(35100, 6975) = 2^2 \cdot 3^3 \cdot 5^2 \cdot 13 \cdot 31 = 1,088,100$

b) lcm(268944, 198466)

$268944 = 2^4 \cdot 3 \cdot 13 \cdot 431$

$198466 =$

$2 \; 99233$

The Euclidean Algorithm

- The Euclidean Algorithm is a process for finding the greatest common divisor.
- It works because of the Quotient-Remainder Theorem and the following two lemmas:

Lemma 1: For all $r \in \mathbb{N}, \gcd(r, o) = r$

Proof 1:

Lemma 2: Let $a, b \in \mathbb{Z}, b \neq 0, q, r \in \mathbb{N} \ni a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof 2:
Let $D = \{d \in \mathbb{Z}: d|a, d|b\}, \overline{D} = \{d \in \mathbb{Z}: d|b, d|r\}$, we will show that $D = \overline{D}$

$(\subseteq)$: *Let* $x \in D$, *then* $x|a$ *and* $x|b$, *we have*

$$a = bq + r$$
$$\Rightarrow a - bq = r$$
$$\Rightarrow \frac{a-bq}{x} = \frac{r}{x}$$
$$\Rightarrow \frac{a}{x} - \frac{bq}{x} = \frac{r}{x}$$

Since $\frac{a}{x}$ and $\frac{bq}{x}$ are integers, we have $\frac{r}{x} \in \mathbb{Z}$, so $x|r$.
Hence, $x \in \overline{D}$, and we have $D \subseteq \overline{D}$.

$(\supseteq)$: *Let* $x \in \overline{D}$, *then* $x|b$ *and* $x|r$, *we have*

$$a = bq + r$$
$$\frac{a}{x} = \frac{bq+r}{x}$$
$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}$$

Since $\frac{bq}{x}$ and $\frac{r}{x}$ are integers, we have $\frac{a}{x} \in \mathbb{Z}$, so $x|a$.
Hence, $x \in D$, and we have $\overline{D} \subseteq D$.

Therefore, $D = \overline{D}$. So, every common divisor of a and b is also a common divisor of b and r, and vice versa.

$\therefore \gcd(a, b) = \max_{d \in D} d = \max_{d \in \overline{D}} d = \gcd(b, r)$

Euclidean Algorithm

1) Let $a < b \leq 0$
2) Check if $b = 0$. If so, Lemma 1 says $\gcd(a, b) = a$
3) If $b \neq 0$, use Quotient-Remainder Theorem to find q, r with $0 \leq r < b$ such that $a = bq + r$. Lemma 2 says $\gcd(a, b) = \gcd(b, r)$.
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.

Exercise:

Find $\gcd(2772, 2310)$.

$\gcd(a,b) = a$

$a = bq + r$

$2772 = 2310 \cdot 1 + 462$

$2310 = 462 \cdot 5 + 0$

$\therefore \gcd(2772, 2310) = 462$

Exercise:

Find $gcd(-243, 223)$.

$243 = 223 \cdot 1 + 20$ (Remember $\gcd(a,b) = \gcd(|a|,|b|)$)

$223 = 20 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\therefore \gcd(-243, 223) = 1$

Definition

Integers a, b are called coprime (relatively prime, mutually prime) if $gcd(a, b) = 1$.

Exercise:

True or false? For all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $\gcd(x, y) = 1$.

Bézout's Identity Theorem

- Let $a, b \in \mathbb{Z}\backslash\{0\}$, then $d = \gcd(a, b)$ exists, and there exists $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Corollary: if a and b are relatively prime, then there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

- How do we find m, n?
  - We use the Euclidean Algorithm in reverse.

Exercise:

Find $m, n \in \mathbb{Z}$ such that $\gcd(303, 156) = 330m + 156n$

① $\gcd(a,b) = a = bq + r$

$\Rightarrow 330 = 156 \cdot 2 + 18$

② $156 = 18 \cdot 8 + 12$

③ $18 = 12 \cdot 1 + 6$

④ $12 = 6 \cdot 2 + 0$

Now starting with the second-last line, isolate the gcd and use each previous line to substitute for other factors.

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 $18 = 330 - 156 \cdot 2 \Rightarrow 6 = -156 + (330 - 156 \cdot 2) \cdot 9$

$= \boxed{330 \cdot 9 - 156 \cdot 19}$

$\therefore m = 9, n = -19$

Exercise:

Find $m, n \in \mathbb{Z}$ such that $243m + 223n = 1$.

$243 = 223 \cdot 1 + 20$

$223 = 20 \cdot 11 + 3$

$20 = 3 \cdot 6 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\Rightarrow (3 = 2 \cdot 1 + 1) \Rightarrow 1 = 3 - 2$

$(2 = 20 - 3 \cdot 6) \Rightarrow 1 = 3 - (20 - 3 \cdot 6)$

$= -20 + 3 \cdot 7$

$(3 = 223 - 20 \cdot 11) \Rightarrow 1 = -20 + (223 - 20 \cdot 11) \cdot 7$

$= 223 \cdot 7 - 20 \cdot 78$

$(20 = 243 - 223 \cdot 1) \Rightarrow 1 = 223 \cdot 7 - (243 - 223 \cdot 1) \cdot 78$

$= \boxed{-243 \cdot 78 + 223 \cdot 85}$

$\therefore m = -78, n = 85$

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.

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.

Examples:

a) 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?
A: 4. The first 3 could possibly be all 3 different colours, but the fourth will match one or those (or else there's a previous pair).

b) In a room of 367 people (allowing for leap year), at least 2 of them share a birthday.

c) 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?

- Some formal equivalent statements to the pigeonhole principle:
  1) Let A be a set of n elements. If A is partitioned into k pairwise disjoint subsets, where k, n, then at least one subset contains more than one element.
  2) A function from one finite set to a smaller set cannot be one-to-one. There must be at least two elements that map to the same point.

Exercise:
In a group of 700 people, must there be two whose first names have the same first and last letters?

A: 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 names.
$\therefore$ A group of 700 people meets this condition.

- Problems of this sort involve figuring out how to form the pigeonholes properly (how to partition the set).

Exercise:
5 different numbers are selected from the set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Show that 2 of the selected numbers sum to 9.

A: Partition into pairs that sum to 9
$S = \{1, 8\} \cup \{2, 7\} \cup \{3, 6\} \cup \{4, 2\}$
There are 4 subsets, so its 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 numbers chosen belonging to the same subset.

Exercise:
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.

A: There are $3 \cdot 6 \cdot 4$ different combinations of meals.
$\therefore$ 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.

Exercise:

Show that in a group of 85 people, the first name of at least 4 of them must start with the same letter.

A: 85 pigeons, 26 pigeonholes

$85 = 26 \cdot 3 + 7$

So $85 > 26 \cdot 3 \Rightarrow m = 3$, and some pigeonholes contain at least $m + 1 = 4$ pigeons.

Exercise:

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.

A: 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 student each.

Then 40 people remain, for 9 classes.

Since $40 = 9 \cdot 4 + 4$, $m = 4$ and the principle says at least one of the 9 classes has 5 or more people in it. □

Modular Arithmetic

Definition:

- Let $n \in \mathbb{N}, a \in \mathbb{Z}$, we define $a \bmod n$ to be the remainder when a is divided by n.

Exercise:

a) $10 \bmod 4 = 2$ ← Since $\frac{10}{4} = 2$ w/ remainder of 2
b) $18 \bmod 3 = 0$
c) $-8 \bmod 6 = 4$ ← Since $x = qn + r$, $-8 = (-2 \cdot 6) + r$, $r = 4$
d) $10 \bmod 1 = 0$ ← anything mod 1 is always 0

- a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a - b)$
- Equivalently, $a \equiv b \pmod{n}$ IFF $a \bmod n = b \bmod n$

Modular Equivalences

- Let a, b and n be integers and suppose $n > 1$. The following statements are all equivalent:
  - $n|(a - b)$
  - $a \equiv b \pmod{n}$
  - $a = b + kn$ for some integer k
  - $a \bmod n = b \bmod n$

Exercise:

True or false?

a) $154 \equiv 56 \pmod{11}$

$11|(154-56) \Leftrightarrow 11|98$ False

b) $7 \equiv -9 \pmod{8}$

$8|(7-(-9)) \Leftrightarrow 8|16$ True

Exercise:

Find x such that $12 \equiv x \pmod{5}$.

$5|(12-x)$, $\therefore x$ is any of $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$

Exercise:

If $m \equiv 0 \pmod{2}$, what can we say about m?

$2|(m-0)$, $\therefore m$ 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) $(a - c) \equiv (c - d) (md\ n)$;
  3) $ab \equiv cd \pmod{n}$;
  4) $a^m \equiv c^m \pmod{n}\ \forall m \in \mathbb{N}$;

Proof:

$n \mid (a-c) \Rightarrow a - c = np,\ p \in \mathbb{Z}$

$n \mid (b-d) \Rightarrow b - d = nq,\ q \in \mathbb{Z}$

(1) $a + b = (np + c) + (nq + d) = n(p+q) + c + d$

$(a+b) \pmod n \equiv [\underbrace{n(p+q)}_{\text{mod } n \to 0} + c + d] \pmod n$

$\equiv (c+d) \pmod n$

(2) $a - b = (np + c) - (nq + d) = n(p-q) + (c-d)$

$(a-b) \pmod n \equiv [\underbrace{n(p-q)}_{\text{mod } n \to 0} + (c-d)] \pmod n$

$\equiv (c-d) \pmod n$

(3) $ab = (np + c)(nq + d) = n^2pq + npd + nqc + cd$

$= n(npq + pd + qc) + cd$

$ab \pmod n \equiv [\cancel{n(npq + pd + qc)} + cd] \pmod n$

$\equiv cd \pmod n$

(4) Induction

a) $m = 1$

$a^1 \equiv c^1 \pmod n$ ✓

b) Suppose $a^k \equiv c^k \pmod n$. 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) $a^k \cdot a \equiv c^k \cdot c \pmod n \Rightarrow a^{k+1} \equiv c^{k+1} \pmod n$

$\therefore a^m \equiv c^m \pmod n \ \forall m \in \mathbb{N}$

Exercise:

a) Given that $2064 = 1715 + 349$, find $2064 \pmod{17}$

b) Given that $713064 = 803 \cdot 888$, find $713064 \pmod{8}$

c) Find x such that $3^9 \equiv x \pmod{5}$

a) $(a+b) \equiv (c+d) \pmod{n}$

$1715 \equiv 15 \pmod{17}$ since $17 \mid (1715 - 15)$ and,

$349 \equiv 9 \pmod{17}$ since $17 \mid (349 - 9)$.

$(1715 + 349) \equiv (15 + 9) \pmod{17}$.

$2064 \equiv 7 \pmod{17}$ since $17 \mid (2064 - 7)$ □

b) $ab \equiv cd \pmod{n}$

$803 \equiv 3 \pmod{8}$ and $888 \equiv 0 \pmod{8}$

$713064 \pmod{8} \equiv (803 \cdot 888) \equiv (3 \cdot 0) \pmod{8} \equiv 0 \pmod{8}$

c) $ab \equiv cd \pmod{n}$

$3^9 = 3^4 \cdot 3^4 \cdot 3 = 81 \cdot 81 \cdot 3$

$81 \equiv 1 \pmod{5}$

$81 \cdot 81 \cdot 3 \pmod{5} \equiv 1 \cdot 1 \cdot 3 \pmod{5} \equiv 3 \pmod{5}$

$\therefore x = 3$

Exercise:

Find the remainder when 7^8 is divided by 16.

$a^m \equiv c^m \pmod{n} \; \forall \; m \in \mathbb{Z}$

?

$7^8 = (7^4)^2$

$(7^4)^2 \bmod 16 = (7^4 \bmod 16)^2 \bmod 16$

$= (2401 \bmod 16)^2 \bmod 16$

$= (1)^2 \bmod 16$ (because $\frac{2401}{16} = 150 \text{ r } 1$)

$= 1 \bmod 16$

Theorem (Cancellation Law):

- Let $n \in \mathbb{Z}, a, b, c \in \mathbb{Z}$
- If $\gcd(a, n) = 1$ and $ab = ac (mod\ n)$, then $b \equiv c\ (mod\ n)$.

Proof:

$$ab \equiv ac \pmod n$$
$$(ab - ac) \equiv 0 \pmod n$$
$$a(b-c) \equiv 0 \pmod n$$

$\Rightarrow a(b-c) \equiv kn$ for some $k \in \mathbb{Z}$ but a and n are coprime by ⊛, so the factor of n on LHS is contained in $(b-c)$. Hence,

$$(b-c) \equiv 0 \pmod n$$
$$b \equiv c \pmod n$$

- NOTE: ⊛ is essential.

Counterexample:

$$60 \equiv 90 \pmod{15}$$
$$10 \cdot 6 \equiv 10 \cdot 9 \pmod{15}, \text{ but}$$
$$6 \not\equiv 9 \pmod{15}$$

Since 10 and 15 are not coprime, the cancellation law does not apply.

Exercise:

Given $10904 \equiv 32\ (mod\ 9)$, find the smallest $x \in \mathbb{N}$ such that $x \equiv 1363\ (mod\ 9)$.

$10904 = 1363 \cdot 8$

$8 \cdot 1363 \equiv 8 \cdot 4 \pmod 9$

$1363 \equiv 4 \pmod 9$ (Since 8 and 9 are coprime)

$\therefore x = 4$ ($4 < 9$, so there are no smaller congruence > 0)

Congruence Classes modulo n

- The quotient-remainder theorem gives us the following:

Fact:

- Let $n \in \mathbb{Z}$.
- Every integer $x \in \mathbb{Z}$ is congruent modulo n to exactly one element in $\{0, 1, 2, \dots, n-1\}$
- 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 $[a] = \{x \in \mathbb{Z} : x \equiv a \ (mod\ n)\}$.

Exercise:

Write the congruence classes for $n = 4$. How many of them are there?

$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$ (since $4 \bmod 4 = 0$)
$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$ (since $5 \bmod 4 = 1$)
$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$ (since $-6 \bmod 4 = 2$)
$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$ (since $-5 \bmod 4 = 3$)

Note: $\underset{x}{-5} \bmod \underset{n}{4} = \underset{r}{3}$

$x = qn + r$

Theorem:

- Let $n \in \mathbb{N}$. There are exactly n distinct congruence classes: $[0], [1], \dots, [n-1]$.

Proof:

First, show that no two of $0, 1, \dots, n-1$ are congruent modulo n.
Let $0 \leq a < b < n, a, b \in \mathbb{N}$.
Then $b - a \in \mathbb{N}$ and $b - a < n$.
Thus, $n \nmid (b - a)$, so $b \not\equiv a \ (mod\ n)$.
Therefore, no two of $0, 1, \dots, n-1$ are congruent, and we have that $[0], [1], \dots, [n-1]$ are all distinct residues.

Next, show that every $x \in \mathbb{Z}$ is in one of these residues.
The Quotient-Remainder Theorem gives $x = nq + r, 0 \leq r < n$.
So, $r \in \{0, 1, \dots, n-1\}$, and $x - r = nq \Rightarrow x \equiv r \ (mod\ n)$.
Therefore, every $x \in \mathbb{Z}$ is in one of $[0], [1], \dots, [n-1]$.

Definition:

- Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set.

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

Exercise:
$\mathbb{Z}_3 = \{[0], [1], [2]\}$.
In $\mathbb{Z}_3$, we have
$[4] = [1]; [-1] = [2]; [30] = [0]$

Exercise:
In $\mathbb{Z}_n$,

a) $[0] \cup [1] \cup \dots \cup [n-1] = \mathbb{Z}$
b) $[0] \cap [1] \cap \dots \cap [n-1] = \emptyset$

↑ No two elements are the same.

Operations on $\mathbb{Z}_n$

- We want to define addition and multiplication on $\mathbb{Z}_n$.
- Since different numbers can give the same residue, we must be careful with the definitions.

Theorem:

- Let $n \in \mathbb{N}$.
  The operation $+$:

$$[a] + [b] = [a + b]$$

is well-defined addition on $\mathbb{Z}_n$, i.e. if $[a] = [c]$ and $[b] = [d]$, then $[a + b] = [c + d]$.

Similarly, the operation $\cdot$:

$$[a][b] = [ab]$$

is well-defined multiplication on $\mathbb{Z}_n$, i.e. if $[a] = [c]$ and $[b] = [d]$, then $[ab] = [cd]$.

Proof:

$[a] = [c] \Rightarrow a \equiv c \ (mod\ n) \Rightarrow \exists\, k_1 \in \mathbb{Z} \ni a = c + k_1 \cdot n$
$[b] = [d] \Rightarrow b \equiv d \ (mod\ n) \Rightarrow \exists\, k_2 \in \mathbb{Z} \ni b \equiv d + k_2 \cdot n$

$a + b = (c + k_1 n) + (d + k_2 n) = c + d + n(k_1 + k_2)$
$\Rightarrow (a + b) \equiv (c + d) \ (mod\ n)$
$\therefore [a + b] = [c + d]$

$ab = (c + k_1 n)(d + k_2 n) = cd + n(k_2 c + k_1 d + n k_1 k_2)$
$\Rightarrow ab \equiv cd \ (mod\ n)$
$\therefore [ab] = [cd]$

Exercise:

Write addition and multiplication tables for $\mathbb{Z}_3$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\swarrow [2]+[1] = 2+1 \pmod 3 = 0$

$\leftarrow [2]+[2] = 2+2 \pmod 3 = 1$

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\leftarrow [2]\cdot[1] = 2\cdot 1 \pmod 3 = 2$

$\leftarrow [2]\cdot[2] = 2\cdot 2 \pmod 3 = 1$

Properties of $\mathbb{Z}_n$

1) $+$ and $\cdot$ are closed (binary) operations.
2) $+$ and $\cdot$ are commutative
3) $+$ and $\cdot$ are associative
4) $\cdot$ is distributive over $+$
5) Identities are [0] under $+$, [1] under $\cdot$
6) The additive inverse of $[x]$ is $[n-x]$
7) Multiplicative inverses exist only for $x \ni \gcd(x,n) = 1$

Theorem:

- If a and n are coprime, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \ (mod\ n)$.
- We call b the multiplicative inverse of a *modulo* n.
- b is unique modulo n.
- We write $b = a^{-1} (mod\ n)$.

Proof:

Consider the set $\{0, a, 2a, 3a, \dots, (n-1)a\}$.
If we can show that there are all distinct modulo n, then exactly one of them is equal to $1 \ (mod\ n)$.
Suppose the contrary: $\exists\ c, d \in \mathbb{N} \cup \{0\}, c, d < n \ni ca \equiv da \ (mod\ n), c \neq d$.
Then $(c-d)a \equiv 0 \ (mod\ n)$, so $\exists\ k \in \mathbb{Z} \ni (c-d)a = kn$.
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.

Exercise:

Find a multiplicative inverse of $43x$ *modulo* 60.

Given the theorem $ab \equiv 1 \pmod{n} \Rightarrow b = a^{-1} \pmod{n}$

Let $n = 60$, $b = 43$, $a = x$,

We need $x \in \mathbb{N} \ni 43x \equiv 1 \pmod{60}$

Notice that $43x$ must have a last digit of 1, since 60 is a multiple of 10. So any x such that $43x$ ends in 1 has last digit 7.

i.e. $61 \bmod 60 = 1$, $43 \cdot 7 = 301$ ← one option,
$43 \cdot 17 = 731$ ← another option

The possibilities are 7, 17, 27, 37, 47, 57,

$43 \cdot 7 = 301 \equiv 1 \pmod{60}$

$\therefore 43^{-1} = 7 \pmod{60}$

Exercise:

Find $3^{-1} (mod\ 40)$.

We need $x \in \mathbb{N} \ni 3x \equiv 1 \pmod{40}$ where $3^{-1} = x \pmod{40}$

$10 | 40 \rightarrow 3x$ must end in 1

$3 \cdot 7 = 21 \rightarrow x$ must end in 7

possibilities are 7, 17, 27, 37, 47.

$3 \cdot 7 = 21 \equiv 21 \pmod{40}$

$3 \cdot 17 = 51 \equiv 11 \pmod{40}$

$3 \cdot 27 = 81 \equiv 1 \pmod{40}$

$\therefore 3^{-1} = 27 \pmod{40}$

Application: Cryptography

- Cryptography is the study of methods for sending secrete 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** is one such public-key method.

RSA

1) Choose 2 large primes p, q.
2) Choose $e \in \mathbb{Z}$ that is coprime with $(p-1)(q-1)$.
3) Choose $d \in \mathbb{Z} \ni ed \equiv 1\ (mod\ (p-1)(q-1))$.
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 send 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 $C = M^e\ (mod\ pq)$.

Decryption Step:

- M is received by $M = C^d\ (mod\ pq)$.

- We will not see the proof.
- p and q are chosen to be several hundred digits long each, making it impossible for a computer to finds the factors $(p-1)(q-1)$ in reasonable time.
- We will see some examples with small primes.

Example:

Let $A = 1, B = 2, \ldots, Z = 26$, public key (3, 55). Encrypt and decrypt the message "HEY."

A: Given pub. key (e, pq), $pq = 55 \Rightarrow p = 5, q = 11$, $e = 3$ which is coprime with $(5-1)(11-1) = 40$.

$\gcd(3, 40) = 1$

Unencrypted method $H = 8$, $E = 5$, $Y = 25$.

Encryption: $C = M^e \pmod{pq}$

$8^3 = 64 \cdot 8 \equiv 9 \cdot 8 \pmod{55} = 72 \pmod{55} \equiv 17 \pmod{55}$

$5^3 = 125 \equiv 15 \pmod{55}$

$25^3 = 125 \cdot 125 \pmod{55} \equiv 15 \cdot 15 \pmod{55} = 225 \pmod{55} \equiv 5 \pmod{55}$

The encrypted message is 17, 15, 5

Decryption: $M = C^d \pmod{pq}$ or the inverse

From a previous example, $3^{-1} \pmod{40} = 27$.

$17^{27} = 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^6 \cdot 14 \cdot 17 \pmod{55} = 196^6 \cdot 238 \pmod{55}$

$\equiv 31^6 \cdot 18 \pmod{55} = 961^3 \cdot 18 \pmod{55} \equiv 26^3 \cdot 18 \pmod{55}$

$= 676 \cdot 468 \pmod{55} \equiv 16 \cdot 28 \pmod{55} = 448 \pmod{55}$

$\equiv 8 \pmod{55}$

So the decrypted 17 is 8, the original "H".

Similarly, 15 decrypts to 5, and 5 decrypts to 25.

Exercise:

Decrypt the message 41 83 36 that was encrypted with public key (5, 91).

$91 \quad pq = 91 \Rightarrow e = 5,\ p = 7,\ q = 13$

$7 \quad 13 \quad (13-1)(7-1) = 72$

$d = 5^{-1} \pmod{72} \leftarrow d \text{ s.t. } 5d \equiv 1 \pmod{72}$

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, and elements may be listed more than once without changing the set.
- Examples:

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

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 $\mathbb{R}$ is a set.

- Sets come from a **universe** of elements $\mathcal{U}$.
- 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.

$\{1, 2, 3\}; \{Susan, Robert\}; \{0, \{0\}, 1, \{0, 1\}\}; \{2, 4, 6, \dots\}; \{2, 4, 6, \dots, 30\}$

- Some important sets of numbers are:
  - $\mathbb{N} = \{1, 2, 3, \dots\}$ (NATURAL)
  - $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 3, \dots\}$ (INTEGER)
  - $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ (RATIONAL)
  - $\mathbb{R} = Set\ of\ all\ real\ numbers$ (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 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. This set is an internal, which can be denoted as $(-2, 5]$.

Exercise:
The set $\{x \in \mathbb{Z} : -2 < x \leq 5\}$ can be rewritten how?

A: $\{-1, 0, 1, 2, 3, 4, 5\}$ or $(-2, 5]$

Exercise:
The set $\{x \in \mathbb{R} : x^3 = x$ can be rewritten how?

A: $\{-1, 0, 1\}$

- The **empty set** is the set with no elements, denoted by ∅.
- It can be represented 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 $\{1, 2, \dots, n\}$.
- For a set S of this size, we write $|S| = n$ and say that S has **cardinality** n.
  - NOTE: $|\emptyset| = 0$
- A set that is not finite is said to be **infinite**.

Subsets

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.

> *Definition – Subsets:*
>
> $\boldsymbol{A \subseteq B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B}$

Supersets

Definition:

- If A is a subset of 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.

> *Definition – Supersets:*
>
> $\boldsymbol{A \not\subseteq B \Leftrightarrow \exists x \ni x \in A \wedge x \notin B}$

Exercise:

Decide true or false.

a) $\{1, 2\} \subseteq \{1, 2, 3\}$ T
b) $\{0, 2\} \subseteq \{1, 2, 3\}$ F
c) $-1 \in \{x \in \mathbb{N} : x^2 = 1$ F (-1, not element of $\mathbb{N}$)
d) $\{1\} \in \{x \in \mathbb{N} : x^2 = 1\}$ F (Not an element)
e) *For all sets* $A, \emptyset \subseteq A$ T

Proper Subsets

Definition:

- A subset $A \subset B$ is **proper** if $\exists x \in B \ni x \notin A$.
  - We write $A \subset B$
  - For example, $\{1\} \subseteq \{1,2\}$ and $\{1,2\} \subseteq \{1,2\}$, but $2 \in \{1,2\}$ and $2 \notin \{1\}$, so actually $\{1\} \subset \{1,2\}$.

> *Definition – Proper Subsets:*
>
> $\boldsymbol{A \subset B, \exists\, x \in B \ni x \notin A}$

Exercise:
Order the sets $\mathbb{R}, \mathbb{N}, \mathbb{Q}, \emptyset, \mathbb{Z}$ in terms of subsets. Are any of these proper subsets?

$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ - They are all proper

Exercise:
True or false? Let $A = \{1,2,3\}$.

a) $A \subset A$ F
b) $\emptyset \in A$ F
c) $\emptyset \subseteq A$ T
d) $\{\emptyset\} \subseteq A$ F
e) $2 \in A$ T
f) $\{2\} \in A$ F
g) $2 \subseteq A$ F
h) $\{2\} \subseteq A$ T
i) $\{2\} \subseteq \{\{1\},\{2\}\}$ F
j) $\{2\} \in \{\{1\},\{2\}\}$ T

Definition:

- Let A and B be sets.
- We say A **equals** B, written $A = B$, if and only if, A contains B and B contains A.

> *Definition – Set Equality*
>
> $\boldsymbol{A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A}$

- To prove two sets are equal, prove the two contentions, $A \subseteq B$ and $B \subseteq A$.

Exercise:

Prove that $A = \{n \in \mathbb{N} : n \text{ is even}\}$ and $B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$ are equal.

($\subseteq$) Let $n \in A$. Then $n = 2k$ for some $k \in \mathbb{N}$.
$n^2 = n \cdot n = (2k)(2k) = 2(2k^2), 2k^2 \in \mathbb{N} \Rightarrow n^2 \text{is even} \Rightarrow n \in B$.

($\supseteq$) Let $n \in B$, so n^2 is even.
Suppose that n is odd, $n = 2k + 1$ for some $k \in \mathbb{N}$.
Then $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is a *contradiction*
Hench, n is even and $n \in A$.
$\therefore B \subseteq A$

$\therefore A = B$

Exercise:

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 $A = B$? T
b) Is $A = D$? F
c) Is $A = C$? T

Proof by case:
($\subseteq$): Let $p = 0$, $p \in \mathbb{Z}$
$n = 2(0) = 0$, $n \in \mathbb{Z}$,
($\supseteq$): Let $r = 0$, $r \in \mathbb{Z}$
$k = 3(0) + 1 = 1$, $k \notin A$

Operations on Sets

- Let A, B be subsets pf a universe $\mathcal{U}/$

1) The **union** of A and B,written $A \cup B$, is the set of all elements that are in A or in B.

$A \cup B = \{x \in \mathcal{U} : x \in A \vee x \in B\}$

2) The **intersection** of A and B, written $A \cap B$, is the set of all elements that are in A and in B.

$A \cap B = \{x \in \mathcal{U} : x \in A \wedge x \in B\}$

3) The **complement** of A, written $\overline{A}$ or $\mathcal{U} \backslash A$, is the set of all elements that are not in A.

$\overline{A} = \mathcal{U} \backslash A = \{x \in \mathcal{U} : x \notin A\}$

4) The **difference** of B minus A, written $B - A$, is the set of all elements that are in B and not in A.

$B - A = \{x \in \mathcal{U} : x \in B \wedge x \notin A\}$

Power Set

Definition:

- The **power set** of a universe $\mathcal{U}$, denoted by $P(\mathcal{U})$, is the set of all subsets of $\mathcal{U}$.

Exercise:

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

$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$

- If $|A| = n$, then $|P(A)| = 2^n$
- The operations of set theory are equivalent to their counterpart connectives of logic, as follows:

Set Operation	Name	Connective
$\setminus$	**Complement**	$\sim$
$\cup$	**Union**	$\vee$
$\cap$	**Intersection**	$\wedge$
$\subseteq$	**Subset**	$\Rightarrow$
$=$	**Equality**	$\Leftrightarrow$

Exercise:

Let $\mathcal{U} = \mathbb{Z}$. Write down $\overline{A}$ for the following.

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

$\overline{A} = \{x \in \mathbb{Z} : 1 < x < 3\}$ or $\{x \in \mathbb{Z} : x \neq 1, 2, 3\}$

b) $A = \{x \in \mathbb{Z} : x \text{ is even}\}$

$\overline{A} = \{x \in \mathbb{Z} : x \text{ is odd}\}$

c) $A = \{x \in \mathbb{Z} : x > 0 \vee x < 0\}$

$A = \{0\}$

Exercise:

Let $\mathcal{U} \in \mathbb{R}$. Write down $A \cup B$ for the following, and $A \cap B$.

a) $A = \{1\}, B = \{2\}$

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

$A \cap B = \emptyset$

b) A is the set of even integers, B is the set of odd integers.

$A \cup B = \mathbb{Z}$

$A \cap B = \emptyset$

c) $A = \{x \in \mathbb{R} : 0 \leq x \leq 2\}$ and $B = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$

$A \cup B = [0, 3]$

$A \cap B = [1, 2]$

Exercise:

Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$.

A: $[(A \Rightarrow C) \wedge (B \Rightarrow C)] \Rightarrow [(A \vee B) \Rightarrow C]$

Use a truth table, or suppose the main connective is false.

$[(A \Rightarrow C) \wedge (B \Rightarrow C)] \Rightarrow [(A \vee B) \Rightarrow C]$

F

T F

T T T F

C:T? A:T C:F?

The contradiction is C cannot be false for LHS to be true.

$\therefore (A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cup B \subseteq C$ □

Exercise:

Prove or disprove: $(A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cap B \subseteq C$

A: $[(A \Rightarrow C) \wedge (B \Rightarrow C)] \Rightarrow [(A \cap B) \Rightarrow C]$

F

T F

T T T F

C:T? A:T, B:T C:F? (!)

$\therefore (A \subseteq C) \wedge (B \subseteq C) \Rightarrow A \cap B$

Exercise:

Let $\mathcal{U} = \mathbb{R}, A = \{1, 2, 3\}, B = \{2\}, C = \{2, 3, 4\}. D = [0,1]$.

a) $A - C =$ $\{1\}$

b) $B - C =$ $\emptyset$

c) $D - B =$ D

d) $D - A =$ $[0, 1)$

e) $A - D =$ $\{2, 3\}$

Disjoints

Definition:

- The sets A and B are **disjoints** if $A \cap B = \emptyset$.

Exercise:

Let $\mathcal{U} = \mathbb{R}$. Write down some sets that are disjoint to the following.

a) $A = \{x \in \mathbb{Z} : x \text{ is even}\}$ $B = \{x \in \mathbb{Z} : x \text{ is odd}\}$

b) $A = \{x \in \mathbb{R} : x^2 - 5x + 6 \geq 0\}$ $B = \{x \in \mathbb{R} : x < 0\}$

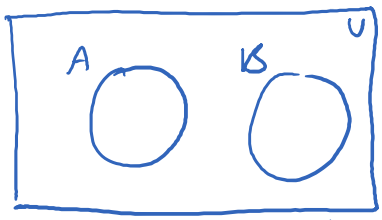
c) $A = \mathbb{Q}$ $B = \mathbb{R} \setminus \mathbb{Q}$

Definition (Addition Rule):

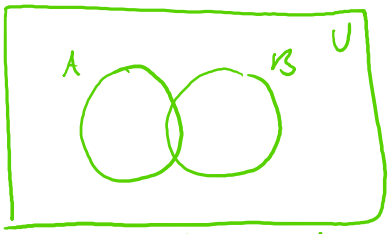
- Let A, B be finite, disjoint sets.
- Then $A \cup B$ is finite and $|A \cup B| = |A| + |B|$.

Venn Diagrams

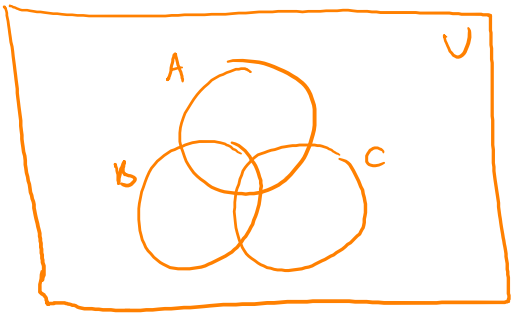
- If we represent sets as regions in the plane, then the relationships among sets can be represented by drawing called **Venn diagrams**.



2 disjoint sets



2 intersecting sets - $A \cap B$



3 intersecting sets - $A \cap B \cap C$

Algebra on Sets

- There are many rules that govern set theory and the relationships among sets.
- All the following statements can be proved using the definitions we have seen so far.

Theorem:

- Let $\mathcal{U}$ be a set, and A, B, C be element of $P(\mathcal{U})$. Then…

1) $(A \subseteq B \wedge B \subseteq) \Rightarrow A \subseteq C$
   $A \subseteq A \cup B; B \subseteq A \cup B$
   $A \cap B \subseteq A; A \cap B \subseteq B$
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) **Commutative Laws:**
   $A \cup B = B \cup A$
   $A \cap B = B \cap A$
5) **Associative Laws:**
   $(A \cup B) \cup C = A \cup (B \cup C)$
   $(A \cap B) \cap C = A \cap (B \cap C)$
6) **Distributive Laws:**
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
7) **De Morgan's Laws:**
   $\overline{A \cup B} = \overline{A} \cap \overline{B}$
   $\overline{A \cap B} = \overline{A} \cup \overline{B}$
8) $\overline{(\overline{A})} = A$
   $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$
   $A - B = A \cap \overline{B}$
   $\overline{\mathcal{U}} = \emptyset$
   $\overline{\emptyset} = \mathcal{U}$
9) $A \cap \mathcal{U} = A; A \cup \emptyset = A$
   $A \cap \emptyset = \emptyset; A \cup \mathcal{U} = \mathcal{U}$
   $A \cap \overline{A} = \emptyset; A \cup \overline{A} = \mathcal{U}$
10) $(A \subseteq C \wedge B \subseteq C) \Leftrightarrow (A \cup B) \subseteq C$
    $(A \subseteq B \wedge A \subseteq C) \Leftrightarrow A \subseteq (B \cap C)$

Exercise:

Prove (7) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

($\subseteq$) Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \in \overline{A}$ and $x \in \overline{B}$

$\Rightarrow x \in \overline{A} \cap \overline{B}$

($\supseteq$) Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A}$ and $x \in \overline{B}$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \notin A \cup B$

$\Rightarrow x \in \overline{A \cup B}$

$\therefore \overline{A \cup B} = \overline{A} \cap \overline{B}$

Exercise:

Prove (2) $A \subseteq B \Leftrightarrow A \cup B = B$.

($\Rightarrow$) Let $A \subseteq B$

($\subseteq$) Let $x \in A \cup B$. Then $x \in A$ or $x \in B$

Since $A \subseteq B$, if $x \in A$ then $x \in B$.

$\Rightarrow x \in B$

$\therefore x \in A \cup B \Rightarrow x \in B$ i.e. $A \cup B \subseteq B$

($\supseteq$) Let $x \in B$. Then $x \in A \cup B$

$\therefore B \subseteq A \cup B$

$\therefore A \subseteq B \Rightarrow A \cup B = B$

($\Leftarrow$) Let $A \cup B = B$

Let $x \in A$. Then $x \in A \cup B$. But $A \cup B = B$, so $x \in B$

$\Rightarrow A \subseteq B$

$\therefore A \cup B = B \Rightarrow A \subseteq B$

$\therefore A \subseteq B \Leftrightarrow A \cup B = B$

Exercise:

Prove that the difference operator is not commutative.

A: Show that $A-(B-C) \neq (A-B)-C$

① $A-(B-C) = A-(B \cap \overline{C})$ (8) $A-B = A \cap \overline{B}$

$= A \cap \overline{(B \cap \overline{C})}$ (8) $A-B = A \cap \overline{B}$

$= A \cap (\overline{B} \cup C)$ (7) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (De Morgan's)

$= (A \cap \overline{B}) \cup (A \cap C)$ (6) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distrib.)

② $(A-B)-C = (A \cap \overline{B})-C$ (8)

$= A \cap \overline{B} \cap \overline{C}$ (8)

Let $x \in A \cap C$. Then by ①, $x \in A-(B-C)$, and since $x \in A$ and $x \in C$, we have $x \notin \overline{C}$. So by ②, $x \notin (A-B)-C$

$\therefore A-(B-C) \neq (A-B)-C$

Pairwise Disjoint

Definition:

- The sets $A_1, A_2, \ldots, A_k$ are **pairwise disjoint** if $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Theorem (Extension of Addition Rule):

- Let $A_1, A_2, \ldots, A_k$ be finite, pairwise disjoint sets.
- Then $A_1 \cup A_2 \cup \ldots \cup A_k$ is finite and $|A_1 \cup A_2 \cup \ldots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|$.

Combinatorics

Sequences and Words

- A **sequence** is an ordered list of objects, with repetitions of the same objects allowed (as opposed to a set).
- The objects of a sequence are called **terms**.
- A sequence may be finite:

  $(1, 2, 3, 4)$; $(a, b, \dots, z)$;

  Or infinite

  $(2, 4, 6, \dots)$; $(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots)$

- The order matters;
- $(1, 2, 3)$ is a different sequence than $(3, 2, 1)$.
- If all terms of a sequence are from a set U, the sequence is a **sequence in U** or a **U-sequence**.
- For example, $(1, 2, 3)$ is a sequence in $\mathbb{N}$.
  - It's also a sequence in $\{0, 1, 2, 3, 4\}$, in $\mathbb{Q}$, in $\mathbb{Z}$, and in $\mathbb{R}$.
- A sequence can also be called a **word** in the alphabet U.
- The sequence $(t_1, t_2, \dots, t_k)$ with n_i possible values for each t_i. Then:

  $s = n_1 n_2 \dots n_k$

Corollary:

- Let $|A| = n$.
- Then there are n^k sequences of length k in A.

Exercise:

How many 3-letter words can be formed with the English alphabet?

Term 1 2 3

$26 \cdot 26 \cdot 26 = 17576$. The words are AAA, AAB, AAC, ..., ZZZ

↑ 26 letter options in alphabet

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 objects is called a **permutation of n objects taken k at a time**.
- If $k = n$, we just say **permutations of n objects.**

Exercise:

Let $S = \{1, 2, 3, 4, 5, 6\}$. The following words in S are permutations of 6 objects taken 3 at a time.

$$s_1 = \{1, 4, 6\}, s_2 = \{3, 2, 4\}, s_3 = \{5, 3, 1\}$$

The following words in S are permutations of 6 objects.

$$s_4 = \{1, 2, 3, 4, 5, 6\}, s_5 = \{1, 3, 2, 6, 4, 5\}, s_6 = \{6, 5, 1, 3, 2, 4\}$$

- There are $P_k^n = \frac{n!}{(n-k)!}$ Permutations of n objects taken k at a time.
- Notice that $\frac{(n!)}{(n-k)!} = \frac{1 \cdot 2 \cdot \ldots \cdot n}{1 \cdot 2 \cdot \ldots \cdot k} = n(n-1) \ldots (n-k+1)$.
- This has a shorter notation called **"falling factorial"** $n^{\underline{k}}$, which is also used for $k > n$.
- When $k \leq n$, we have:

$n^{\underline{k}} = \frac{n!}{(n-k)!}$, and when $k > n, n^{\underline{k}} = 0$

Exercise:

Let $n = 7, k = 10$.

$7^{\underline{10}} = 7 \cdot 6 \cdot \ldots \cdot 1 \cdot 0 \cdot (-1) \cdot (-2) = 0$

Theorem:

- For all $n, k \in \mathbb{N}$, there are $n^{\underline{k}}$ permutations of n objects taken k at a time.

Proof:

If $k > n$, there is no way to permute n objects k at a time, so the answer must be zero.
If $k \leq n$, there are n choices for the 1st element, then $(n-1)$ choices for the 2nd, etc.
So the possibilities are:

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) = n^{\underline{k}} = \frac{n!}{(n-k)!} \blacksquare$$

Corollary:

- For all $n \in \mathbb{N}$, there are $n!$ permutations of n objects.

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:

$\_\ \_\ \_\ \cdots\ \_$
$1\ \ 2\ \ 3\ \ \ \ k$

- Fill each slot one at a time, with the number of possible values for each term, given the restrictions of the properties.

$\underset{1}{n_1}\ \underset{2}{n_2}\ \underset{3}{n_3}\ \cdots\ \underset{k}{n_k}$

- By multiplication rule, there are $n_1 n_2 n_3 \ldots n_k$ possible sequences.

Exercise:

There are 2 highways from Brisbane to Sydney, and 3 highways from Sydney to Adelaide. How many different round trips from Brisbane to Adelaide via Sydney are there? How many are there without taking the same highway twice?

A: 1st problem: $\underset{B\text{-}S}{2} \cdot \underset{S\text{-}A}{3} \cdot \underset{A\text{-}S}{3} \cdot \underset{S\text{-}B}{2} = 36$

2nd problem: $\underset{B\text{-}S}{2} \cdot \underset{S\text{-}A}{3} \cdot \underset{A\text{-}S}{2} \cdot \underset{S\text{-}B}{1} = 12$

↳ one less to avoid same highway.

- You don't necessarily have to start with the 1st position.
- Start where it's most convenient.

Exercise:

How many 5-digit odd numbers with no repeated digits are there?

$\underset{\text{Next}}{8} \cdot 8 \cdot 7 \cdot 6 \cdot \underset{\text{Last digit must be odd to be an odd number.}}{5}$

Next cannot be one chosen from digit 5

Start here with options 1, 3, 5, 7, 9

Can't include 1st digit chosen but can include last.

- Sometimes, we need to break a problem up into subproblems.

Exercise:
How many 5-digit even numbers with no repeated digits are there?

① If last digit is 0
9 8 7 6 1
② If last digit is not 0
8 8 7 6 4

There's the same restriction on digit 5, but the restriction on digit 1 is different if digit 5 is zero

Required Adjacency
- For a required adjacency, treat the adjacency as a single object, then multiple by the number of arrangements of the adjacency.

Exercise:
Three single people and a married couple are to be seated in a row of chairs. In how many ways can it be done such that the spouses sit together?

4 3 2 1 = 24 total arrangements with n = 4 because H-W must sit together.

24 · 2 = 48
↳ The permutations of required adjacency i.e. (W-H), (H-W)

Forbidden Adjacency
- For a forbidden adjacency, calculate it as a required adjacency, and then subtract from the total possible arrangements.

Exercise:
In how many ways can you align a cow, a goat, a fox, and a chicken such that the fox and the chicken are not next to each other.

Required adjacency (CH-FX): 3 · 2 · 1 = 6
6 · 2 = 12
CH-FX FX-CH

Total permutations w/out adjacency: 4 · 3 · 2 · 1 = 24

Forbidden adjacency: 24 − 12 = 12 □

Binomial Coefficients

- Recall the power set of x: $P(x) = \{A : A \subseteq X\}$.

  $P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

- Another notation for $P(X)$ is 2^X. This is because of the following.

Theorem:

- Let $|X| = n \in \mathbb{N}U\{0\}$
- Then X has 2^n subsets, i.e. $|P(X)| = 2^{|X|}$

Proof:

With induction.

a) Let $n = 0$, then $X = \emptyset$, and $P(X) = \emptyset$, so $|P(X)| = 1 = 2^0$

b) Let $k \in \mathbb{N}$, suppose $|X| = k$ and $|P(X)| = 2^k$. Define

$Y = X \cup \{y\} = \{x_1, x_2, \dots, x_k, y\}$.

The subsets of Y are those that contain y, and those that do not. Those that do not 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 too. Therefore, $|Y| = 2^k + 2^k = 2^{k+1}$.

$\therefore |P(X)| = 2^{|X|}\ \forall X\ finite$ ■

- 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.

  $$\binom{n}{k} = |\{A : A \subseteq X\ and\ |A| = k\}|$$

- The symbol $\binom{n}{k}$ Is read **"n choose k"** or **"the k^{th} BINOMIAL COEFFICIENT of order n"**
- Some $\binom{n}{k}$ are obvious:

  $\binom{n}{0} = 1$, since the only subset of cardinality 0 is $\emptyset$.
  $\binom{n}{n} = 1$, since X is the only subset of X with n elements.
  If $k > n$, then $\binom{n}{k} = 0$, as it's impossible to have a subset of X with cardinality larger than that of 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've 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.

Exercise:

How many different poker hands are there?

A: There are 5 cards in a poker hand.
Order is not important.
They are taken from a deck of 52 cards.
$\binom{52}{5} = \frac{52!}{5!(52-5)!} = 2,598,960$ poker hands

Theorem:

- For all $n, k \in \mathbb{N} \cup \{0\} \ni 0 \leq k \leq n, \binom{n}{k} = \binom{n}{n-k}$

Proof:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)!]} = \binom{n}{n-k}$$

Theorem:

- For all $n, k \in \mathbb{N} \cup \{0\} \ni 0 \leq k \leq n,$
  a) $\binom{n}{0} = 1$
  b) $\binom{0}{k} = 0$
  c) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Proof:

The Binomial Theorem

- Motivation:
  - In how many ways can 3 red marbles and 4 blue marbles be arranged in a row? (Or a more practical example: how many binary words are there with 3 zeros and 4 ones?). The multiplication rule isn't very helpful here; there are too many cases. However, considering the 7 slots:

Notice that once you choose slots for the red marbles, the placement of the blue ones is automatic. So the question is, how many ways are there to choose 3 of the 7 slots? We know the answer is $\binom{7}{3} = 35$. Similarly, if you choose 4 slots for the blue marbles first, there are $\binom{7}{4} = 35$ ways to do it. The answer is the same, because $\binom{7}{3} = \binom{7}{4} = \frac{7!}{3!4!}$

Theorem:

- The number of words of length n consisting of n_1 letters of one sort, and $n_2 = n - n_1$, letters of a second 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 $\{x, y\}$.
Similarly,

$$(x + y)^3 = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$

is the sum of all words of length 3 in the alphabet $\{x, y\}$.
By 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 in $\mathbb{N}$.

Theorem (Binomial 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 (before simplification) the sum of all 2^n words of length n in the alphabet $\{x, y\}$.
The number of such words that consist of k $x's$ and $(n - k)$ $y's$ is $\binom{n}{k}$ by the previous theorem.

The binomial theorem as written gives the expansion in ascending powers of x:

$$(x + y)^n = y^n + n \cdot xy^{n-1} + \binom{n}{2} x^2 y^{n-2} + \binom{n}{3} x^3 y^{n-3} + \cdots + n \cdot x^{n-1} y + x^n$$

Equivalently, it can be written in reverse:

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = x^n + n \cdot x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + n \cdot xy^{n-1} + y^n$$

We can substitute values for x and y to obtain identities.

Exercise:
Let $x = y = 1$. Then the binomial theorem gives:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Exercise:
Let $x = -1, y = 1$. Then the binomial theorem gives:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0;$$
$$\binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots;$$
$$\sum_{k \text{ even}}^{n} \binom{n}{k} = \sum_{k \text{ odd}}^{n} \binom{n}{k}$$

- Sometimes, a useful trick is to use the fact that $x = x \cdot 1$.

Exercise:
Simplify $\sum_{k=0}^{n} \binom{n}{k} a^k$.

A:

$$\sum_{k=0}^{n} \binom{n}{k} a^k = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot 1^{n-k} = (a + 1)^n$$

Exercise:

Simplify $\sum_{k=1}^{17}(-1)^k\binom{17}{k}13^{17-k}$

A:

$$\sum_{k=1}^{17}\binom{17}{k}13^{17-k}(-1)^k = \sum_{k-0}^{17}\binom{17}{k}13^{17-k}(-1)^k - \binom{17}{0}13^{17-0}(-1)^0$$
$$= (13-1)^{17} - 1\cdot 13^{17}\cdot 1$$
$$= 12^{17} - 13^{17}$$

Relations and Functions

Cartesian Product

- 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 internal $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ uses the same notation, but context makes it clear.
- The **Cartesian product** of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) with $a \in A, b \in B$.

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

Exercise:
Let $A = B = \mathbb{R}$. What is $A \times B$?

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

Exercise:
Let $A = \{3\}, B = \{2, 3\}$. What is $A \times B$?

$A \times B = \{(3,2), (3,3)\}$

Exercise:
Let $A = \{x, y\}, B = \{1, 2, 3\}, C = \{a, b\}$. What are $A \times B$ and $(A \times B) \times C$?

$A \times B = \{(x,1), (x,2), (x,3), (y,1), (y,2), (y,3)\}$

$(A \times B) \times C = \{(x,1,a), (x,1,b), (x,2,a), (x,2,b), (x,3,a), (x,3,b),$
$(y,1,a), (y,1,b), (y,2,a), (y,2,b), (y,3,a), (y,3,b)\}$

Exercise:
Let $A = \{1, 2\}, B = \{\pi, e\}$. Is $A \times B = B \times A$?

No.

Relations

- 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 of A.**
- We say that a is related to b by R if $(a, b) \in R$.
- This is denoted by aRb.

Exercise:

Let $X = \{0, 1, 2, 3\}, R = \{(x, y): \exists\, z \in \mathbb{N} \ni x + z = y\}$

a) What is an easier way of expressing R?

b) List all the elements of R.

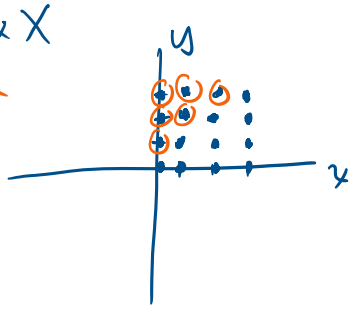
c) Sketch $X \times X$ and circle the elements of R.

a) $\{(x,y) : y - x \in \mathbb{N}\}$; $\{(x,y) : y > x\}$

b) $R = \{(0,1), (0,2), (0,3), (1,2), (1,3), (2,3)\}$

c) $X \times X$

R



Exercise:

Let R *on* $\mathbb{Z}\backslash\{0\}$ be given by $R = \{(x, y): \exists\, z \in \mathbb{Z} \ni xz = y\}$.

a) Describe the relation R.

b) True or false?

a) It's the set $\{(x,y) : x \text{ is a divisor of } y\}$

b) $(2, -4) \in R \longrightarrow 2 \mid -4$ ✓ T

$-3 R 0 \longrightarrow -3 \mid 0$ × F

$(3,5) \in R \longrightarrow z = \frac{y}{x}, \; z \in \mathbb{Z}$

$= \frac{5}{3}, \; z \in \mathbb{Z}$ □ ✓ T

Exercise:

Let R *on* $\mathbb{Z}$ be given by $R = \{(m,n) : m - n \text{ is even}\}$

a) Give another description of R.

b) Which are elements of R?

   a. $(0,3)$
   b. $(-5,-6)$
   c. $(2,-11)$
   d. $(17,1)$

c) Prove that n *odd* $\Rightarrow nR1$.

a) $\{(m,n)$: m and n have the same parity$\}$

i.e. $4-2=2$, 2 is even

$2-4=-2$, -2 is also even

b) $(17,1)$

c) Let $m=1$, and $n=3$

$1-3=-2$

-2 is even

$\therefore$ n odd $\Rightarrow nR1$

Union and Intersection of Relations

- Relations are sets, so the set operations apply.

Exercise:

Let R_1, R_2 *on* $\mathbb{R}$ by given by $R_1 = \{(x,y) : x = y\}, R_2 = \{(x,y) : x = -y\}$.

Write expressions for $R_1 \cup R_2$ and $R_1 \cap R_2$.

$R_1 \cup R_2 = \{(x,y) : x = y \vee x = -y\}$

$R_1 \cap R_2 = \varnothing$

Definition (Domain and Range)

- Let R be a relation from A to B.
- The **domain** of R and the **range** of R, denoted respectively by $domR$ and $ranR$, are defined:

$$dom\ R = \{x : \exists\ y \ni xRy\}$$
$$ran\ R = \{y : \exists\ x \ni xRy\}$$

- Note that $dom\ R \subseteq A$ and $ran\ R \subseteq B$.

Exercise:

Let $A = \{0, 1, 2, 3\}, R = \{(0,0), (0,1), (0,2), (3,0)\}$. Write $dom\ R$ and $ran\ R$.

$dom\ R = \{0, 3\}$

$ran\ R = \{0, 1, 2\}$

Exercise:

Find domain and range of R *on* $\mathbb{Z} \times \mathbb{Q}, R = \{(x, y): x \neq 0 \wedge y = \frac{1}{x}\}$.

$dom\ R = \mathbb{Z} \setminus \{0\}$

$ran\ R = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\} \cup \{-1, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}, \ldots\}$

Exercise:

Find domain and range of R *on* $\mathbb{Z}, R = \{(x, y) : xy \neq 0\}$.

$dom\ R = \{x : x \neq 0\}$

$ran\ R = \{y : y \neq 0\}$

The Inverse of a Relation

- If R is on $A \times B$, then a relation R^{-1}on $B \times A$ can be defined by interchanging the elements of the ordered pairs of R.

Definition:

- Let R be on $A \times B$. The inverse relation of R is:

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$$

- Note that $dom\ R^{-1} = ran\ R$ and $ran\ R^{-1} = dom\ R$.

Exercise:

Let $A = \{a, b, c\}, B = \{1, 2, 3, 4\}, R = \{(a, 1), (b, 2), (c, 3), (a, 4)\}$. Find R^{-1}.

$R^{-1} = \{(1, a), (2, b), (3, c), (4, a)\}$

Exercise:

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}.

$R = \{(1, 2), (2, 4), (3, 6), \ldots\}$

$R^{-1} = \{(2, 1), (4, 2), (6, 3), \ldots\}$

$R^{-1} = \{(y, x) : x = 2y\}$

Exercise:

The identity relation on $\mathbb{R}$ is $R = \{(x, x) : x \in \mathbb{R}\}$. What is R^{-1}?

$R = R^{-1}$

Properties of Relations

- Let R be a relation on A. Then:
  1) R is **reflexive** on A IFF $\forall x \in A, (x, x) \in R$.
  2) R is **symmetric** on A IFF $\forall\, x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$.
  3) R is **transitive** on A IFF $\forall\, x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.

Exercise:

Which properties do the following relations satisfy?

a) On $\mathbb{N}$, $R = \{(x, y) : x \text{ is a factor of } y\}$ – reflexive, transitive
b) On $\mathbb{R}$, the identity relation – all 3
c) On $\mathbb{Z}$, $R = \{(x, y) : x < y\}$ – transitive
d) On $\mathbb{R}$, $R = \{(x, y) : y = x^2\}$ – None
e) On the set of all people, $R = \{(x, y) : x \text{ is in the family of } y\}$ – symmetric, reflexive
f) On the set of all people, $R = \{(x, y) : x \text{ loves } y\}$ – reflexive

Equivalence Relations

Definition

- Let R be a relation on A. Then R is an equivalence relation of A IFF R is *reflexive*, *symmetric*, and *transitive* on A.

Exercise:

Prove or disprove that the identity relation on $\mathbb{R}$ is an equivalence relation.

Reflexive: by definition of the identity relation on $\mathbb{R}$,
$x R x \;\forall\, x \in \mathbb{R}$

Symmetric: $\forall\, x, y \in \mathbb{R}$, $x R y \Rightarrow x = y \Rightarrow y R x$

Transitive: $\forall\, x, y, z \in \mathbb{R}$, $x R y \Rightarrow x = y$
$y R z \Rightarrow y = z$
$\Rightarrow x = z$

$\therefore (x, z) \in R$

$\therefore$ The identity relation on $\mathbb{R}$ is an equivalence relation because it satisfies reflexivity, symmetric, and transitivity.

Exercise:

On $\mathbb{Z}$, prove that $R = \{(a, b) : a \equiv b \ (mod\ n)\}$ is an equivalence relation.

$a \equiv b \pmod n$

$n \mid (b-a)$

For example, suppose $x = 13$, $(13, 13) \in R$

$n \mid (13-13) = n \mid 0$, $\frac{0}{n} = 0$, $0 \in \mathbb{Z}$

Reflexive ✓

$n \mid (b-a)$, $n \mid (a-b) \Rightarrow n \mid (-1)(a-b) \Rightarrow n \mid (b-a)$

Symmetric ✓

If (a, b) and $(b, c) \in R$, then prove $(a, c) \in R$

$(a, b) \in R \Rightarrow n \mid (b-a) \Rightarrow b - a = np,\ p \in \mathbb{Z}$

$(b, c) \in R \Rightarrow n \mid (c-b) \Rightarrow c - b = nq,\ q \in \mathbb{Z}$

$(a, c) \in R \Rightarrow n \mid (c-a) \Rightarrow c - a + b - b = (c-b) + (b-a) = np + nq$

add zero; rearrange

$= n(p+q)$

transitive ✓

- To disprove an equivalence relation, you only need to show that one of the properties does not hold.

Exercise:

On $\mathbb{Z}$, prove that $R = \{(a, b) : ab = 0\}$ is not an equivalence relation.

Given $a = 2$, $2 \cdot 2 \neq 0$, $\therefore (a, a) \notin R$ $\therefore$ NOT reflexive

Equivalence Classes

Definition

- Let R be an equivalence relation on A. For each $a \in A$, the **equivalence class** of a, denoted $[a]$, is the set:

$$[a] = \{x \in A : xRa\}$$

- Equivalence classes have the following properties:
  1) For any $a, b \in A$, we have either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
  2) All distinct equivalence classes form a **partition** of A
     a. The *union* of all classes is A, and the *intersection* of any 2 classes is empty.

Exercise:

Let $A = \{0,1,2\}, R = \{(0,0),\ (1,1),\ (2,2),\ (0,1),\ (1,0)\}$. Find [0], [1], [2].

$[0] = \{0,1\}$

$[1] = \{1,0\}$

$[2] = \{2\}$

Exercise:

What do the equivalence classes of the identity relation on $\mathbb{R}$ look like?

$[1] = \{1\}$

$[\frac{2}{5}] = \{\frac{2}{5}\}$

Exercise:

Let R *on* $\mathbb{Z}$ be defined by $R = \{(a,b) : a \equiv b\ (mod\ 3)\}$. Find [0], [1], [2].

$3 \mid (b-0) \Rightarrow [0] = \{\ldots,-3,0,3,6,\ldots\}$

$3 \mid (b-1) \Rightarrow [1] = \{\ldots,-5,-2,1,4,7,\ldots\}$

$3 \mid (b-2) \Rightarrow [2] = \{\ldots,-7,-4,-1,2,5,\ldots\}$

Relations and Functions

Functions

Definition:

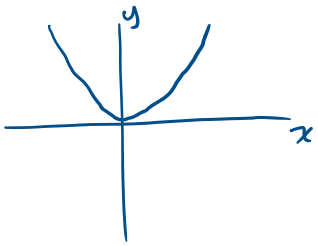
- A relation F from A to B is a **function** from A to B IFF:
  1) $dom\ F = A$, and
  2) For each $x \in A$ there is at most **one** $y \in B$ such that $(x, y) \in F$.
     a. Then B is the **codomain** of F.
- A function from A to B is denoted by $f: A \to B$.
- The equation $y = f(x)$ means $(x, y) \in f$.
- In that case, y is the **image** of x under f.
- 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 graph at most once.

Exercise:

Sketch the relations and determine which are functions.

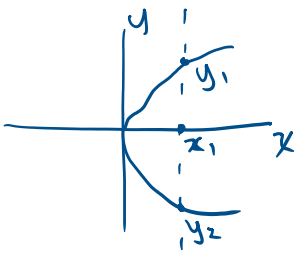
a) On $\mathbb{R}$, $R = \{(x, y): y = x^2\}$
b) On R, $R = \{(x, y): x = y^2\}$
c) On $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$, $R = (x, y): x = y^2\}$
d) On $\mathbb{R}$, $R = \{(x, y): y = \sqrt{x}\}$

a)



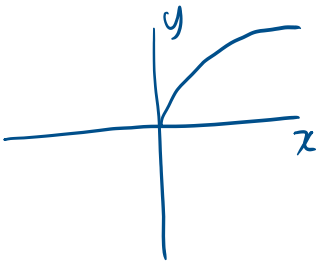
Yes function

b)



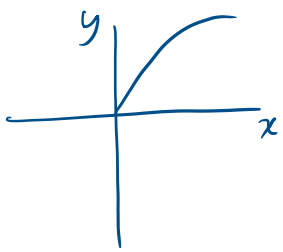
Not a function.
Fails vertical line test.
x_1 has two values y_1, y_2.

c)



Yes function.

d)



Yes function.

Exercise:

Which are functions?

a) The identity relation on $A = \{1,5,10\}$. → Yes

b) $A = \{2,4,6\}, B = \{1,3,5\}, R\ on\ A \times B, R = \{(x,y): x + 1 = y\}$ → No, Let $x = 6 \Rightarrow y = 7$, 7 ∉ codomain B

c) On $\mathbb{Z}, F = \{(x,y): x + 1 = y\}$ → Yes

d) On $\mathbb{R}, R = \{(x,y): y = 1\}$ →  Yes

Definition (Injective):

- Let $f: A \to B$ be a function.
- We say that f is **one-to-one (injective)** IFF for all $x_1, x_2 \in A$.

$$f(x_1) = f(x_2) = x_1 = x_2$$

- That is, each element of the range is the image of only **one** element of the domain.

Exercise:

Let $A = \{0,1,2,3\}, f: f(A) \to \mathbb{N}, f(A_i)$ is the number of elements in A_i. Prove or disprove that f is one-to-one.

Let $A_1 = 1$, $A_2 = 2$, $A_1 \neq A_2$

$f(\{1\}) = 1$

$f(\{2\}) = 1$

$f(A_1) = f(A_2)$

∴ This function is not one-to-one.

Exercise:

Which are one-to-one?

a) On $A = \{1,2,3\}, F = \{(1,2),(2,3),(3,1)\}$ → Yes

b) On $A = \{1,2,3\}, F = \{(1,2),(2,1),(3,1)\}$ → No → $f(2) = f(3) = 1$

c) On $\mathbb{Z}, F = \{(x,y): y = 2x\}$ → Yes

d) On $\mathbb{Z}\backslash\{0\} \to \mathbb{R}, F = \{(x,y): y = \sqrt{x^2 - 1}\}$ → No → for $x_1 = 3$, $x_2 = -3$, $y = 2.8$

Definition (Surjective):

- A function $f: A \to B$ is **onto (surjective)** IFF $ran\ f = B$.
- That is, for all $y \in B$, there exists $x \in A$ such that $f(x) = y$.

Exercise:

Let $A = \{1,2,3,4,5\}, B = \{a,b,c,d\}$. Which are onto?

a) $f: A \to B, f = \{(1,a),(2,c),(3,c),(4,d),(5,d)\}$ → No, no b element

b) $f: A \to B, f = \{(1,a),(2,b),(3,c),(4,d),(5,a)\}$ → Yes

c) $f: \mathbb{R} \to \mathbb{R}, f(x) = 4x - 1$

d) $f: \mathbb{Z} \to \mathbb{Z}, f(x) = 4x - 1$

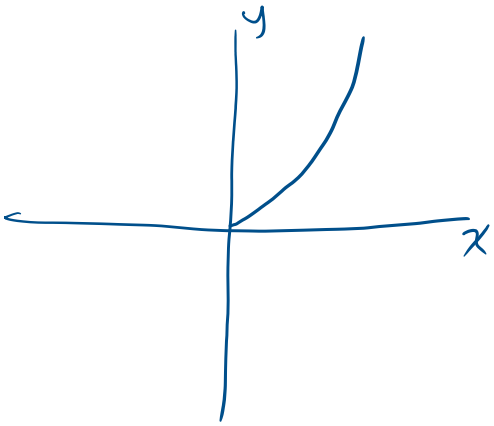
Theorem (Inverse):

- The **inverse** of a function f, written f^{-1}, is also a function IFF f is one-to-one and onto **(bijective)**.

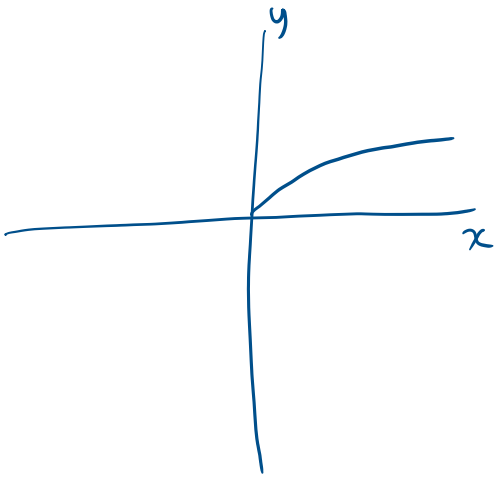
Exercise:

Sketch $f: \mathbb{R}_+ \to \mathbb{R}, f = \{(x, y): y = x^2\}$. Find and sketch f^{-1}. Is f^{-1} a function?

f:



f^{-1}:



$f^{-1}: y = \sqrt{x}$

f^{-1} is also a function

Graph Theory

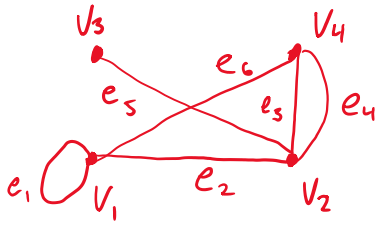
- Many real-world problems concern objects and relations, e.g. people with friendships, cities connected by highways, web pages linked to others, etc.
- The mathematical abstraction of these situations is the study of graph theory.
- A **graph** is a collection of points and curves.

Definition:

- A **graph** G consists of a pair of finite sets:
  - A nonempty set of V of **vertices** and a set of 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**.
- 2 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 edges are incident is called **isolated**.
- 2 vertices connect by an edge are called **adjacent**.

Exercise:

Write down V and E for the following graph. List any loops and parallel edges.

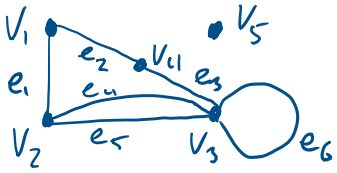


$V = \{v_1, v_2, v_3, v_4\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

Exercise:

Draw a graph that has 5 vertices include 1 isolated, 1 loop, and 1 pair of parallel edges.



$V = \{v_1, v_2, v_3, v_4, v_5\}$

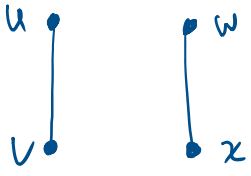
$E = \{(v_1, v_2), (v_1, v_4), (v_4, v_3), (v_3, v_2), (v_3, v_2), (v_3, v_3)\}$

Definition (Simple Graph):

- A **simple graph** is one that does not have loops nor parallel edges.

Exercise:

Draw a simple graph with $V = \{u, v, w, x\}$ and 2 edges, one of which has endpoints u and v.

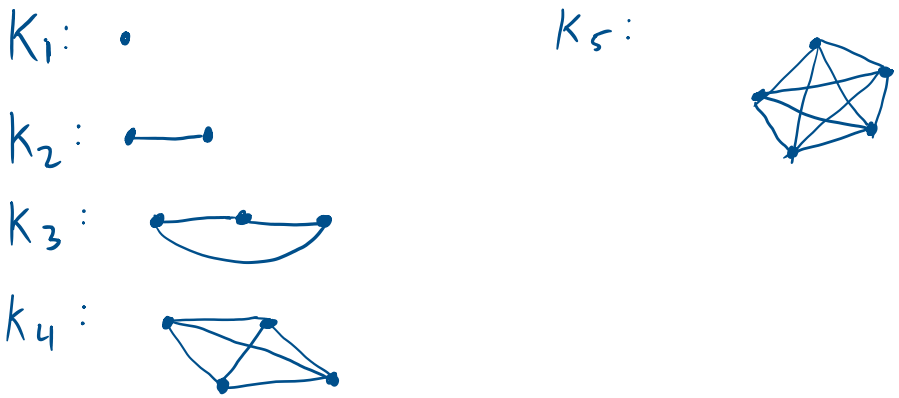


Definition (Complete Graph):

- A **complete graph** on n vertices, denoted by K_n, is a simple graph with n vertices whose edge set contains exactly one edge for every pair of distinct vertices.

Exercise:

Draw K_1, K_2, K_3, K_4, K_5.

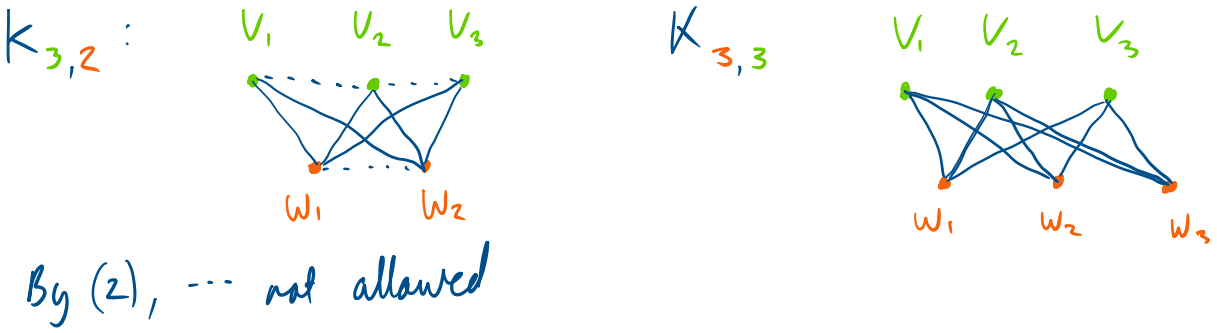


Definition (Complete Bipartite Graph):

- A **complete bipartite graph** on (m, n) vertices, denoted by K_{m_1,n_1} is a simple graph with $V = \{V_1, \dots, V_m, W_i, \dots, W_n\}$ 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 other V_k;
  3) No edge from any W_j to any other W_l

Exercise:

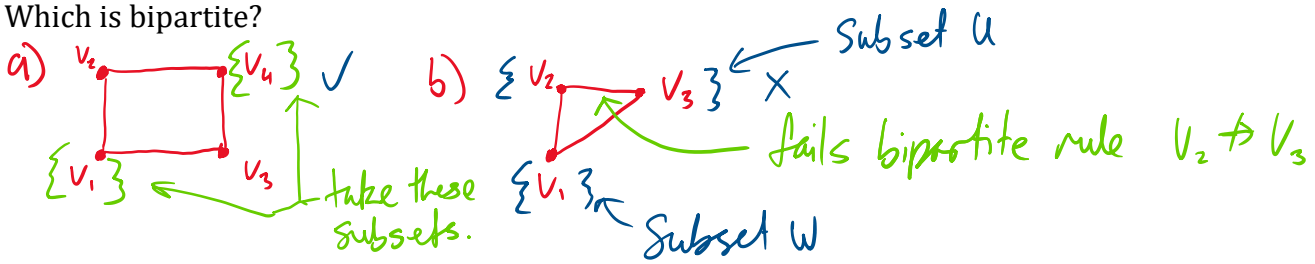
Draw $K_{3,2}, K_{3,3}$.



- A simple graph is **bipartite** if there exists $\mathcal{U} \subseteq V$ and $W \subseteq V$ such that:
  1) $\mathcal{U} \cup W = V$ and $\mathcal{U} \cap W = \emptyset$;
  2) Every edge connects to a vertex of $\mathcal{U}$ with a vertex of W.

Exercise:

Which is bipartite?

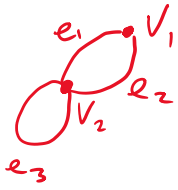


Definition (subgraph):

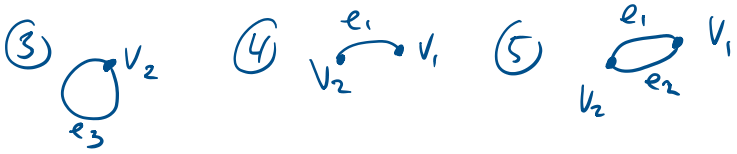
- A graph H is a **subgraph** of a graph G if
  - Every vertex in H is in G;
  - Every edge in H is in G; and
  - Every edge in H has the same endpoints in G.

Exercise:

Draw all the subgraphs of

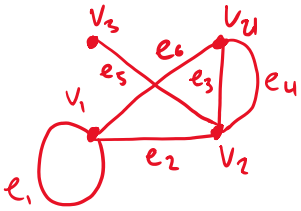


Subgraphs: ① V_1 ② V_2 ③ V_1 V_2

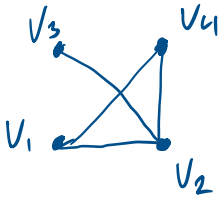


Exercise:

Draw 2 subgraphs containing 2 vertices each, one simple and one not.



① Simple H_1



② NOT Simple

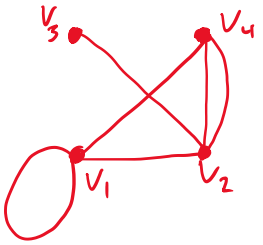
Definition (Degree):

- Let G 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 $v \in V$.

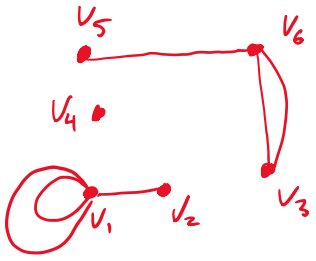
Exercise:

Find the degree of G_1 and G_2.

G_1 :



G_2 :



$\delta(V_1) = 4$

$\delta(V_2) = 4$

$\delta(V_3) = 1$

$\delta(V_4) = 3$

$\delta(G_1) = 4 + 4 + 1 + 3 = 12$

$\delta(G_2) =$ number of edges $\times 2$

$= 6 \cdot 2$

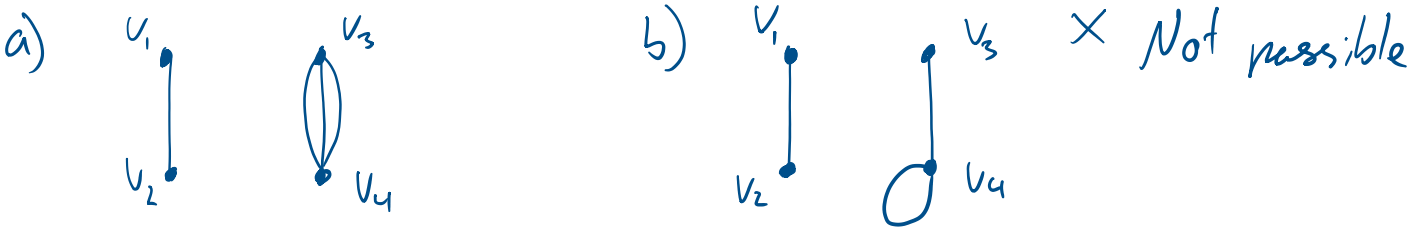
$= 12$

Exercise:

Draw graphs with $|V| = 4$ and vertices of degree:

a) 1, 1, 3, 3;

b) 1, 1, 2, 3

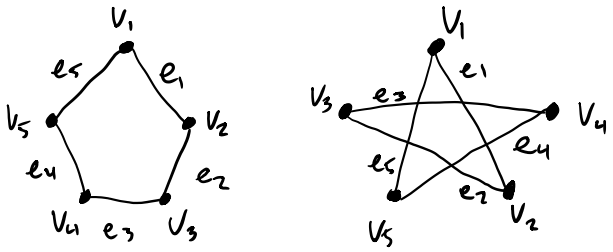


The Hand Shake Theorem:

- The degree of a graph is twice the number of its edges.
- This holds because each edge always has 2 endpoints.
- So, the degree of a graph is always even, and a graph with 4 vertices of degree 1, 1, 2, 3 is impossible.

Isomorphic Graphs

Is there any difference between these graphs?

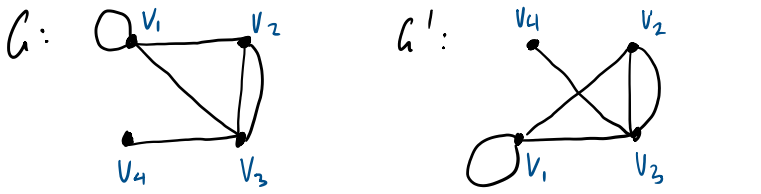


Definition:

- Let G, G' be graphs $G = (V, E), G'(V', E')$.
- We say G is **isomorphic** to G' if there exist bijective functions $f: V \to V', h: E \to E'$ that preserve adjacency, i.e. V is an endpoint of $e \Leftrightarrow f(v)$ is an endpoint of $h(e)$.

Exercise:

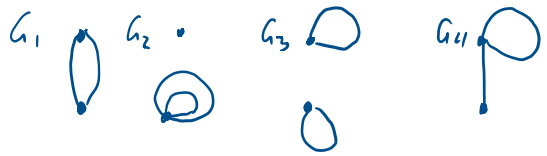
Show that G and G' are isomorphic.



$f: \{v_1, v_2, v_3, v_4\} = \{w_1, w_2, w_3, w_4\}$

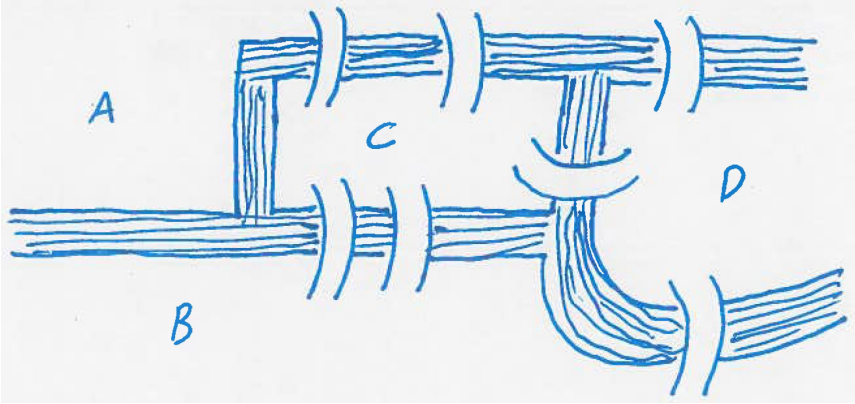
Exercise:

Draw all possible graphs (up to isomorphism) with $|V| = |E| = 2$.



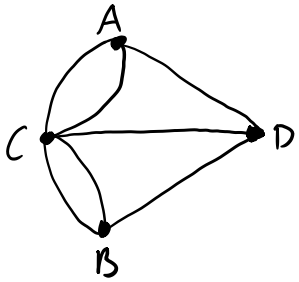
The Königsberg Bridge Problem

- In 1736, Leonhard Euler introduced graph theory by solving the following problem.



Is it possible for someone to walk in Königsberg, starting and ending at the same point, and crossing each of 7 bridges exactly once?

- This 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 a vertex and traverses each edge exactly once?

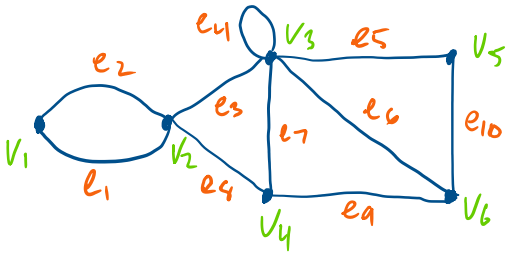
Walks, Paths, and Circuits

- **Walk:** from vertex V to vertex W in G is a finite alternating sequence of adjacent vertices and edges of G that starts at V and ends at W:

$$v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n, where\ v_o = v\ and\ v_n = w$$

  - **Length:** of a walk is the number of edges in the sequence.
  - If it is not ambiguous, a walk can be denoted by a sequence of only vertices or only edges.
- **Trail:** a walk that does not contain a repeated *edge*.
- **Path:** a trail that does not contain a repeated *vertex*.
- **Circuit:** a walk whose first and last vertices are the same.
- **Simple circuit:** a trail whose first and last vertices are the same.

Exercise:



Are the following walks, trails, paths, circuits, or simple circuits?

1) $v_1e_1v_2e_3v_3e_4v_3e_5v_5$
2) $e_1e_3e_4e_4e_6$
3) $v_2v_3v_4v_6$
4) $v_2v_3v_4v_2$
5) $v_1e_1v_2e_1v_1$
6) v_1

Definition (Connected):

- 2 vertices v, w in G are **connected** if there exists a walk from v to w.
- G is connected if there is a walk between every pair of vertices.
- Otherwise, G is **disconnected**.

Example:

CONNECTED GRAPHS

G_1 :

G_2 :

DISCONNECTED GRAPHS

G_3 :

G_4 :

Definition (Connect Component):

- A graph H is a **connected component** of G if:
  1) H is a subgraph of G
  2) H is connected
  3) No connected subgraph of G has H as a subgraph and contains vertices or edges that are outside of H.

Example:

G : v_1 e_1 v_2 e_2 v_3

v_4

e_3

$(\{v_1, v_2, v_3\}, \{e_1, e_2\})$ is a CONNECTED COMPONENT of G

$(\{v_1, v_2\}, \{e_1\})$ is NOT.

Definition (Eulerian Circuit):

- An **Eulerian circuit** of G is a simple circuit that contains every vertex and every edge of G.
- If an Eulerian circuit exists, G is an **Eulerian Graph**.
- An **Eulerian path** from v to w is a path from v to w that passes through every vertex in G at least once, and every edge in G exactly once.

Theorem:

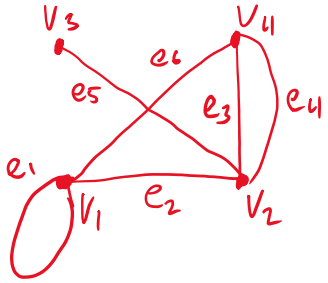
- If G is an Eulerian graph, then every vertex of G has an even degree.
- Equivalently, if some vertex of G has an odd degree, then G is not Eulerian.

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, it uses 2 edges; one arriving to the vertex and one leaving it. Each edge is used once, so each vertex uses an event number of incident edge endpoints. The starting point v is of even degree as well, since the circuit begins by leaving v, then using v an even number of times, then arriving at v. ■

Exercise:

Does the following have an Eulerian circuit? An Eulerian path?



Not an Eulerian circuit, because V_3 and V_4 have an odd degree.

Yes, an Eulerian path if you start or end at V_3 or V_4.

Euler's Theorem:

- In a connected graph, the degree of every vertex is even and positive IFF the graph is Eulerian.

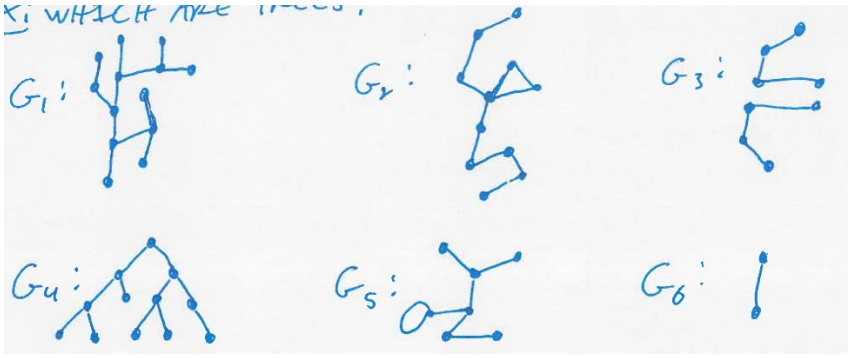
Tree

Definition:

- A graph is a **tree** if it is connected and has no circuits.

Example:

Which are trees?



A: G_1, G_4, G_6

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.

Exercise:

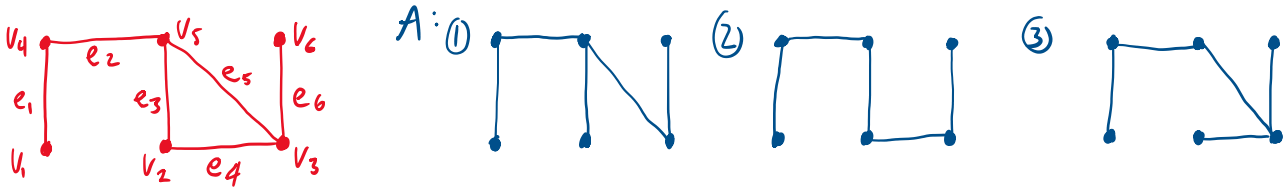
Draw a tree with 5 vertices and 4 edges. Draw a graph with 5 vertices and 4 edges that is not a tree.

Definition (Spanning Tree):

- 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 2 spanning trees for a graph have the same number of edges.

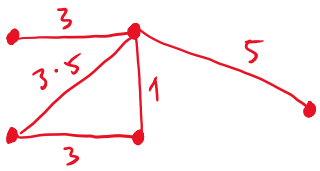
Exercise:

Find all spanning trees.



Exercise:

Let the edges represent phone lines, the number represent the cost (in thousands) of installing the lines.



Find the spanning tree and determine the minimum cost.

3 + 1 + 3 + 5 = 12

Definition (Weighted Graph):

- 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.

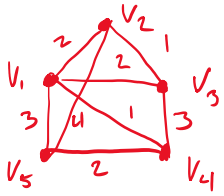
- A **minimum spanning tree** for a connected, weighted graph is a spanning tree that has the least possible weight.
- NOTE: minimum spanning trees are not necessarily unique.
- We use $w(e)$ and $w(G)$ for the weights of edge e and graph G.

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 what will be the minimum spanning tree, one does not create a circuit.

Example:

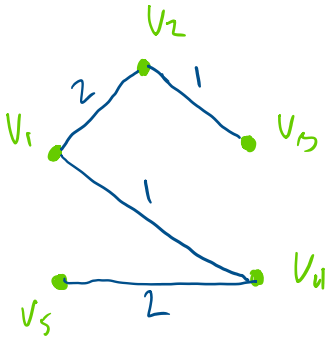
Find a minimum spanning tree.



A: First, put the edges in order by weight.

Edge	Weight	Will adding edge make a circuit?	Action	Cumulative Weight
v_2v_3	1	No	Add	1
v_1v_4	1	No	Add	2
v_1v_3	2	No	Add	4
v_2v_3	2	Yes	Skip	4
v_4v_5	2	No	Add	6
v_3v_4	3	Yes	Skip	6
v_1v_5	3	Yes	Skip	6
v_2v_5	4	Yes	Skip	6

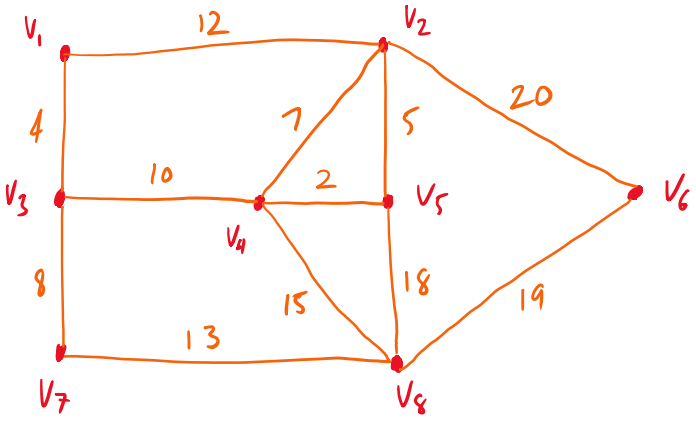
MST:

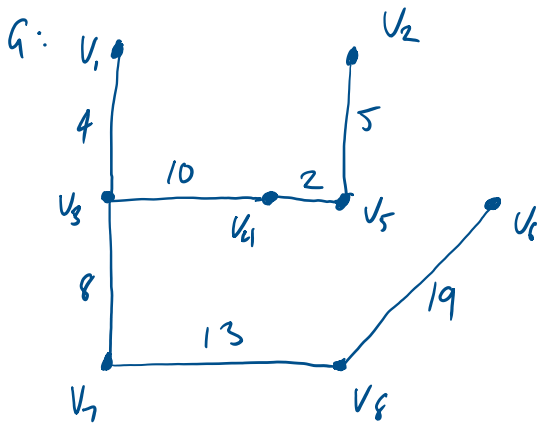


$\therefore\ w(G) = 6$

Exercise:

Find a minimum spanning tree.





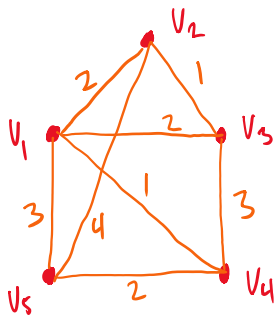
Edge	Weight	Circuit?	Action	Cumulative Weight
V_4V_5	2	No	Add	2
V_1V_3	4	No	Add	6
V_2V_5	5	No	Add	11
V_2V_4	7	Yes	Skip	11
V_3V_7	8	No	Add	19
V_3V_4	10	No	Add	29
V_1V_2	12	Yes	Skip	29
V_7V_8	13	No	Add	42
V_4V_8	15	Yes	Skip	42
V_5V_8	18	Yes	Skip	42
V_6V_8	19	No	Add	61
V_2V_6	20	Yes	Skip	61

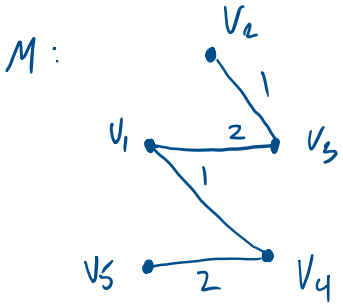
$\therefore\ w(G) = 61$

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:



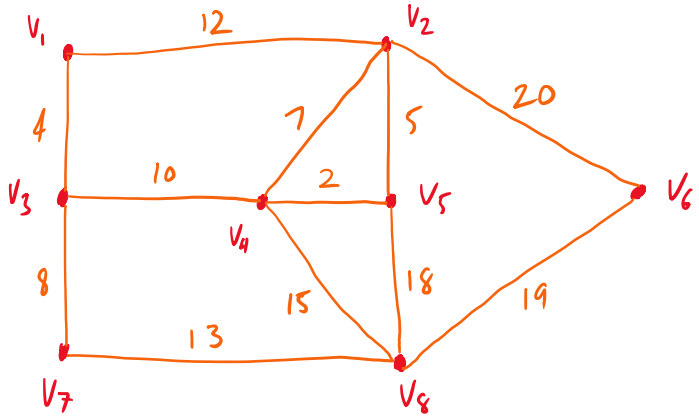


A: Start with (arbitrarily) V_1.

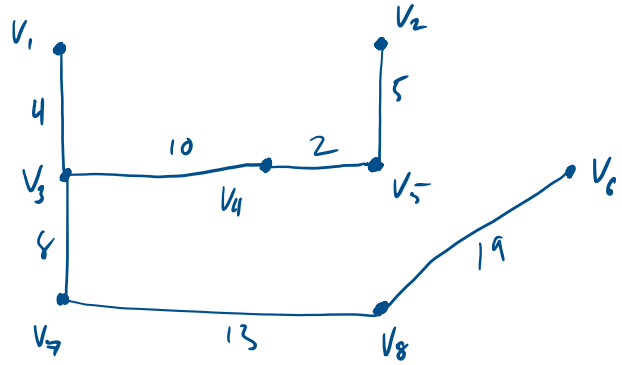
Vertex Added	Edge Added	Weight	Cumulative Weight
V_4	V_1V_4	1	1
V_3	V_1V_3	2	3
V_2	V_2V_5	1	4
V_5	V_4V_5	2	6

Exercise:

Find the MST with Prim's algorithm.



A: Start with V_4:



$V_5 \to V_4V_5 : 2$
$V_2 \to V_2V_5 : 5$
$V_3 \to V_3V_4 : 10$
$V_1 \to V_1V_3 : 4$
$V_7 \to V_3V_7 : 8$
$V_8 \to V_7V_8 : 13$
$V_6 \to V_6V_8 : 19$

$\therefore w(G) = 61$

Probability

Definition:

- **Random** phenomenon**:** cannot be predicted with certainty in advance.
- **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.
- 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.
  $P(\emptyset) = 0$, as $\emptyset$ contains no possibilities.

- Some probabilities can be calculated, others can be found experimentally as long run proportions.
- They can be added, provided they are disjoint (mutually exclusive).

Example:

The probability that a random student obtains grades in MATH223 are:

F	P	C	D	HD
0.2	0.35	0.2	0.15	0.1

Let E denote the event $\{C, D, HD\}$ ("credit or better").

$P(E) = 0.2 + 0.15 + 0.1 = 0.45$

This is valid because events $\{C\}$, $\{D\}$, and $\{HD\}$ are disjoint (non-overlapping).

- If all outcomes are equally likely, then:

  $P(A) = \frac{|A|}{|S|}$, where $|X|$ is the number of outcomes in set X

Example:

A coin is tossed twice. The sequence of heads and tails is record. $S = \{HH, HT, TH, TT\}$. Let $E = \{HH, TT\}$ denote the event "same result for both tosses." Since all 4 outcomes have equal probability,

$$P(E) = \frac{|E|}{|S|} = \frac{2}{4} = \frac{1}{2}$$

Exercise:

2 fair dice are rolled. What is the probability that the sum of faces is 4?

A:

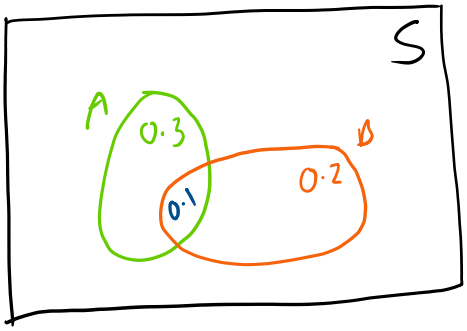
	1	2	3	5	6	TOTAL
1	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
2	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
3	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
4	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
5	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
6	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{6}$
TOTAL	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	1

All 36 events have equal probability, and 3 of them meet our needs.
Let $B = \{(1,3), (2,2), (3,1)\}$. Then,

$$P(B) = \frac{|B|}{|S|} = \frac{3}{36} = \frac{1}{12}$$

Venn Diagrams

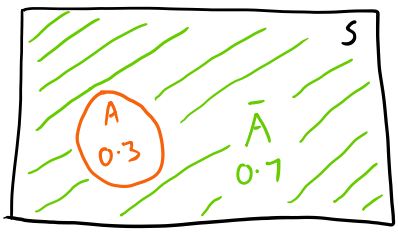
- A Venn Diagram represents the sample space and all events.
- Probabilities are represented as areas.



Complement

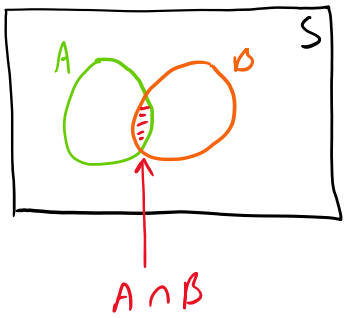
- The complement of A, denoted by A^c or $\overline{A}$, is the set of all outcomes not in A.

$$P(\overline{A}) = 1 - P(A)$$



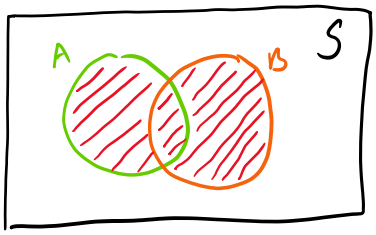
Intersection

- The intersection $A \cap B$ is the event that both A and B occur.



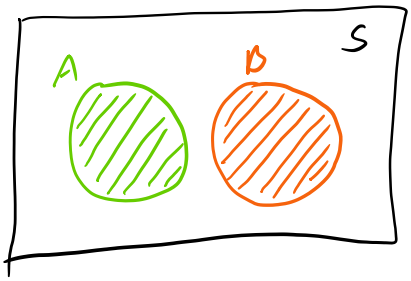
Union

- The union $A \cup B$ is the event that A or B (or both) occurs.



Disjoint

- Two events A and B are **disjoint** (cannot occur simultaneously) if $A \cap B = \emptyset$.



- For disjoint events A and B

$$P(A \cup B) = P(A) + P(B)$$
$$P(A \cap B) = 0$$

Conditional Probability

- The conditional probability of event A given that 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 one happens.
- This gives us a formula for conditional probability:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Example:
What is the probability of A ("doubles") given B (sum of 2 dice is 4)?

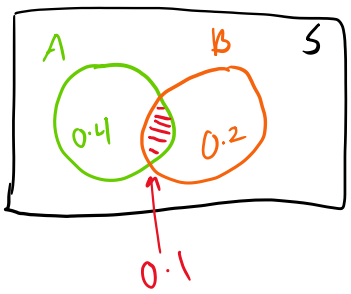
A: For a double to occur, A ("doubles") has to occur and B (sum of 2 dice is 4) has to occur.

$$P(A \cap B) = \frac{1}{36}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{36}}{\frac{3}{36}} = \frac{1}{3}$$

- Notice that this is different from the unconditional probability $P(A) = \frac{6}{36} = \frac{1}{6}$.
- If you use Venn diagrams to calculate $P(A|B)$, $\overline{B}$ is discarded and B becomes the new sample space.

$$P(A|B) = \frac{0.1}{0.1 + 0.2} = \frac{1}{3}$$



Probability Rules

1) $P(S) = 1, P(\emptyset) = 0$
2) $P(E) \geq 0$ for any event $E \subseteq S$
3) If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$
4) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
5) $P(\overline{A}) = 1 - P(A)$
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.

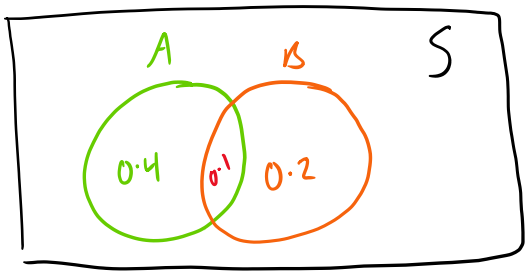
	B	$\overline{B}$	TOTAL
A	$P(A \cap B)$	$P(A \cap \overline{B})$	$P(A)$
$\overline{A}$	$P(\overline{A} \cap B)$	$P(\overline{A} \cap \overline{B})$	$P(\overline{A})$
TOTAL	$P(B)$	$P(\overline{B})$	1

Example:
Using the previous Venn diagram:

	B	$\overline{B}$	TOTAL
A	0.1	0.4	0.5
$\overline{A}$	0.2	0.3	0.5
TOTAL	0.3	0.7	1

- To find conditional probabilities using a two-way table, divide the intersection value by the row or column total.

	B	$\overline{B}$	TOTAL
A	0.1	0.4	0.5
$\overline{A}$	0.2	0.3	0.5
TOTAL	0.3	0.7	1



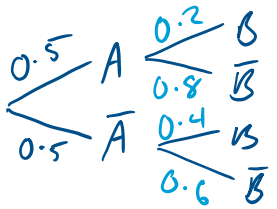
$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{0.1}{0.5} = \frac{1}{5}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{0.1}{0.3} = \frac{1}{3}$$

Tree Diagrams

- Conditional probabilities correspond to second-level (or higher) branches in a tree diagram.
- Multiply probabilities of all branches along a path to find it's probability.
- Add probabilities of all paths leading to an event to find it's probability.

Example:
Based on the previous two-way table:



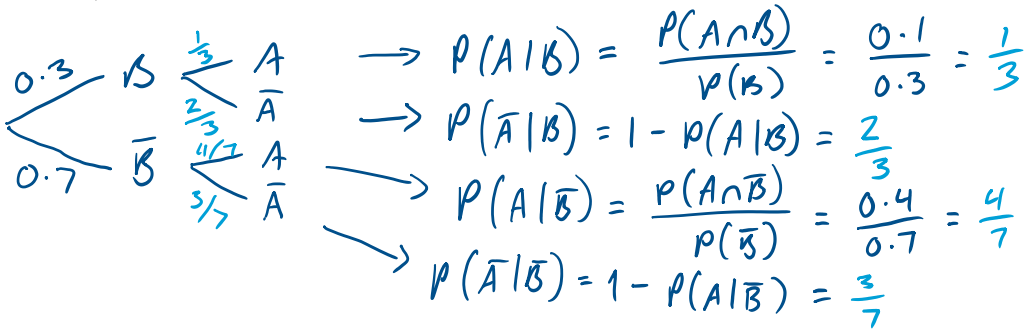
$(0.5)(0.2) = 0.1 = P(A \cap B)$ → $P(A \cap B) = P(A)P(B|A) = 0.1$

$(0.5)(0.8) = 0.4 = P(\overline{A} \cap B)$ $= (0.5) \cdot P(B|A) = 0.1$

$(0.5)(0.4) = 0.2 = P(\overline{A} \cap B)$ $= P(B) = \frac{0.1}{0.5} = 0.2$

$(0.5)(0.6) = 0.3 = P(\overline{A} \cap \overline{B})$

Exercise:
Same table, branch from B first.



Law of Total Probability

- $P(A)$ can be found by decomposing A into disjoint pieces.
- Then using the sum and product rules:

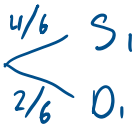
$$\begin{aligned} P(A) &= P(A \cap B) + P(A \cap \overline{B}) \\ &= P(B)P(A|B) + P(\overline{B})P(A|\overline{B}) \end{aligned}$$

Example:
For the previous example,

$$P(A) = (0.3) \cdot \frac{1}{3} + (0.7) \cdot \frac{4}{7} = 0.5$$

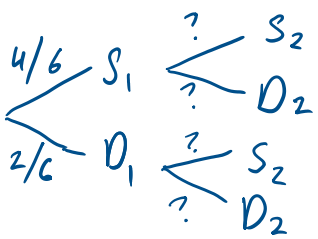
Exercise:
2 items are randomly selected without replacement from a batch of 6. The batch contains 2 defective items. Let S_i denote the event that item i inspected is satisfactory. Let D_i denote the event that item i inspected is defective. What is the probability that at least one defective item is found?

Step 1: Inspect the first item.



Step 2: Given step 1, inspect the second item.

One item selected that is satisfactory, so 3/5 choices



Intersections:
$P(S_1 \cap S_2) = \frac{4}{6} \cdot \frac{3}{5} = \frac{2}{5}$
$P(S_1 \cap D_2) = \frac{4}{6} \cdot \frac{2}{5} = \frac{4}{15}$
$P(D_1 \cap S_2) = \frac{2}{6} \cdot \frac{4}{5} = \frac{4}{15}$
$P(D_1 \cap D_2) = \frac{2}{6} \cdot \frac{1}{5} = \frac{1}{15}$

$P(\text{At least one defective}) = P(D_1 \cap D_2) + P(S_1 \cap D_2) + P(D_1 \cap S_2) = \frac{1}{15} + \frac{4}{15} + \frac{4}{15} = \frac{3}{5}$
OR $1 - P(\text{No defectives}) = 1 - P(S_1 \cap S_2) = \frac{3}{5}$

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.**
- We have that $P(A|B) = \frac{P(A \cap B)}{P(B)}$, so A and B are independent IFF:

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

Examples:

- Successive coin tosses are not affected by previous results, so the results of different tosses are independent.
- The events "drug present" and "positive test result are not independent, as a drug test is much more likely to be positive if the drug is present.

Exercise:

Events A and B are independent, $P(A) = 0.4, P(B) = 0.5$. Construct a two-way table and a tree diagram.

Start with what you know, and use $P(A \cap B) = P(A)P(B)$.

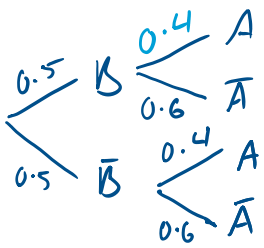
	B	$\overline{B}$	TOTAL
A	0.2	0.2	0.4
$\overline{A}$	0.3	0.3	0.6
TOTAL	0.5	0.5	1

$P(A \cap B) = (0.4)(0.5) = 0.2$

$P(\overline{A} \cap B) = P(B) - P(A) = 0.5 - 0.2 = 0.3$

$P(A \cap \overline{B}) = P(A) - P(B) = 0.4 - 0.2 = 0.2$

. . .



$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{0.2}{0.5} = 0.4$

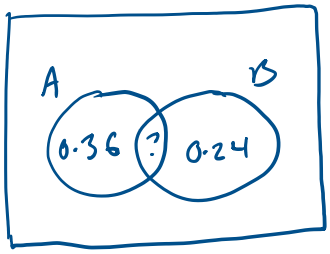
. . .

Exercise:

If $P(A \cap \overline{B}) = 0.36, P(\overline{A} \cap B) = 0.24, P(A|B) = 0.5$. Then A and B are:

a) Disjoint and independent.
b) Disjoint and not independent.
c) Independent and not disjoint.
d) Not independent and not disjoint.

A:



Recall that disjoint means $P(A \cap B) = 0$

$P(B) = P(\bar{A} \cap B) + P(A \cap B)$

$= 0.24 + P(A \cap B)$

$P(A|B) = \frac{P(A \cap B)}{P(B)} \Rightarrow 0.5 = \frac{P(A \cap B)}{P(A \cap B) + 0.24}$

$\Rightarrow 0.5(P(A \cap B) + 0.24) = P(A \cap B)$

$\Rightarrow 0.5(P(A \cap B)) + 0.12 = P(A \cap B)$

$\Rightarrow 0.12 = P(A \cap B) - 0.5(P(A \cap B))$

$\Rightarrow 0.12 = P(A \cap B)(1 - 0.5)$

$\Rightarrow P(A \cap B) = 0.24 \neq 0$

$\therefore$ A and B are not disjoint

$P(A) = 0.36 + 0.24 = 0.6$; $P(B) = 0.24 + 0.24 = 0.48$

Recall that independence means $P(A \cap B) = P(A)P(B)$

$P(A)P(B) = (0.6)(0.48) = 0.288 \neq P(A \cap B)$

$\therefore$ A and B are not independent

Bayes' Rule

- For events A and B, Bayes' rule provides a way to reverse the order of conditional probabilities.

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|\overline{B})P(\overline{B})}$$

- This comes directly from the definition of conditional probability, the product rule (numerator) and the law of total probability (denominator).

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

- In terms of a tree, the numerator defines one path, the denominator is the sum of paths that lead to A.

Exercise:

A drug test has 0.96 chance of positive result if the drug is present, 0.93 chance of negative result if the drug is present, 0.93 chance of negative result if the drug is not present. The unconditional probability of the drug being present is 0.007. Given a positive result, what is the probability that the drug is present?

Let A = "positive test result", B = "drug is present"

$$P(A|B) = 0.96;\ P(\bar{A}|\bar{B}) = 0.93;\ P(B) = 0.007.$$

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|\bar{B})P(\bar{B})}$$

$$= \frac{(0.96)(0.007)}{(0.96)(0.007) + (1-0.93)(1-0.007)}$$

$$= 0.08815$$

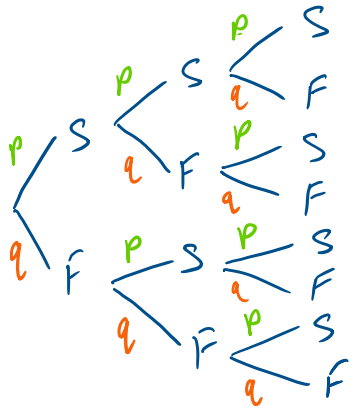
Positive test result is 91% likely to be false!

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 success.
- Notation:
  - $n = number\ of\ indenpendent\ trials$
  - $p = probability\ of\ success\ for\ a\ single\ trial. 0 < p < 1$
  - $q = 1 - p = probability\ of\ failure$
  - $x = number\ of\ successes$

For small n, a tree diagram can be used to work out probabilities:

x	0	1	2	3	Total
Prob.	q^3	$3pq^2$	$3p^2q$	p^3	1



- Recall the Binomial Coefficient, the number of ways to select k objects out of n (order is not important) is:

$$\binom{n}{k} = C_k^n = \frac{n1}{k1(n-k)!}$$

Example:

$\binom{3}{2} = \frac{3!}{2!(3-2)!} = 3$, so there are 3 different ways of choosing 2 items from a set of 3 times.

- An alternative interpretation is that there are $\binom{n}{x}$ ways of arranging n objects, x of one type (success) and $(n-x)$ of another type (failure): $\binom{3}{2}$ → SSF, SFS, FSS.
- Since the binomial scenario events are independent, the probability of x successes and $(n-x)$ failures in n trials (single path) is:

$$\underbrace{p \cdot p \cdot \ldots \cdot p}_{x \text{ times}} \underbrace{q \cdot q \cdot \ldots \cdot q}_{(n-x) \text{ times}} = p^x q^{n-x}$$

- The number of such path is $C_x^n = \binom{n}{x}$
- So the probability of x success is:

$$\binom{n}{x} p^x q^{n-x}$$

- NOTE: that the sum of all binomial probabilities is 1, as it must be.
- We see this by the binomial expansion theorem.

$$\binom{n}{0} q^n + \binom{n}{1} pq^{n-1} + \binom{n}{2} p^2 q^{n-2} + \cdots + \binom{n}{n} p^n$$

$$= \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} = (q+p)^n = (1-p+p)^n = 1$$

Example:

The probability that an email delivered to a certain account is junk is 0.25, independently of all other messages. What is the probability that exactly 5 out of the 20 most recent messages are junk?

A: $n = 20$ is far too large for a tree diagram, so use the binomial probability formula with:

$$n = 20, x = 5, p = 0.25$$

$$P(5) = \binom{20}{5} 0.25^5 0.75^{20-5} = 0.2023$$