

# MATHD022: Discrete Mathematics

Connor Petri

Spring 2025

# Contents

# 1. The Language of Mathematics

---

## 1.1 Variables

**Definition** A **variable** is a symbol that is used as a placeholder when:

- The quantity has one of more values, but is not known.
  - For example:  $2x^2 - x = 7$
- The quantity represents **any element** from a given set.
  - For example: The reciporical of any non-zero integer  $n$  is  $\frac{1}{n}$ .

**Writing Sentences using Variables** We can rewrite the following sentences using variables:

- Is there an integer  $n$  that has a remainder of 2 when it is divided by 5?
  - Is there an integer  $n$  such that  $n \% 5 = 2$ ?
- The cube root of any negative real number is negative.
  - For any real number  $s$ , if  $s < 0$ , then  $\sqrt[3]{s} < 0$ .

### Types of Statements

- A **universal statement** is a statement that is true always true.
  - For example: **All** positive numbers are greater than 0.
- A **conditional statement** is a statement that is true if a certain condition is met.
  - For example: **If** 378 is divisible by 18, **then** 378 is divisible by 6.
- A **universal conditional statement** is a statement that is both conditional and universal.

- For example: **For all** animals  $a$ , if  $a$  is a dog, **then**  $a$  is a mammal.
- As a universal statement: **For all** dogs  $a$ ,  $a$  is a mammal.
- As a conditional statement: **If**  $a$  is a dog, **then**  $a$  is a mammal.
- An **existential statement** gives a property that is true for at least one thing.
  - **There is** a prime number that is even.
- A **universal existential statement** is a statement where the first part is universal and the second part is existential.
  - **Every** real number **has** an additive inverse.
  - **For all** real numbers  $r$ , **there is** an additive inverse  $-r$ .
  - **For all** real numbers  $r$ , **there is** a real number  $s$  such that  $r + s = 0$ .
- An **existential universal statement** is a statement where the first part is existential and the second part is universal.
  - **There is** a positive integer that is less than or equal to **every** positive integer.
  - **There is** a positive integer  $m$  such that **every** positive integer is greater than or equal to  $m$ .
  - **There is** a positive integer  $m$  with the property that **for all** positive integers  $n$ ,  $m \leq n$ .

## 1.2 Sets

**Definition** A **set** is a collection of objects.

**Notation**

- $x \in S$ :  $x$  is an element of  $S$ .
- $x \notin S$ :  $x$  is not an element of  $S$ .
- $S = \{1, 2, 3, \dots\}$ : is **set roster notation**.

**Axiom of Extension** A set is determined by what its elements are. Orders of elements or repeated elements can't be determine the set.

For example:  $\{1, 2, 3\} = \{3, 2, 2, 1, 2, 3, 1\}$ . There are 3 elements in both sets.

**Common Sets**

- $\mathbb{R}$ : the set of all real numbers.
- $\mathbb{Z}$ :  $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  the set of all integers.
- $\mathbb{N}$ :  $\{1, 2, 3, \dots\}$  the set of all natural numbers.
- $\mathbb{Q}$ : the set of all rational numbers.
- $\emptyset = \{\}$ : the empty set, or null set.

The null set is a subset of every set.

**Set Builder Notation** Let  $S$  denote a set and let  $x \in S$  be and element in  $S$ .  $P(x)$  is a property that some elements of  $S$  satisfy.

$$A = \{x \in S | P(x)\}$$

$A$  constains elements in  $S$  such that  $(\text{---}) P(x)$  is true.

## Subsets

**Definition** Let  $A$  and  $B$  be sets.  $A$  is a **subset** ( $\subseteq$ ) of  $B$  if every element of  $A$  is also an element of  $B$ .

**Proper Subsets** Let  $A$  and  $B$  be sets.  $A$  is a **proper subset** ( $\subset$ ) of  $B$  if every element of  $A$  is also an element of  $B$ , **and** there is at least one element in  $B$  that is not in  $A$ .

**Example** Let  $A = \mathbb{Z}^+$ ,  $B = \{n \in \mathbb{Z} | 0 \leq n \leq 100\}$ , and  $C = \{100, 200, 300, 400, 500\}$ .

- $B \subseteq A$  is false.
- $C \subset A$  is true.
- $C \subseteq B$  is false.
- $C \subseteq C$  is true.

**Cartesian Product of sets** Let  $A$  and  $B$  be sets. The **Cartesian product** of  $A$  and  $B$ , denoted  $A \times B$ , is the set of all ordered pairs  $(a, b)$  such that  $a \in A$  and  $b \in B$ .

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

**Example** Let  $A = \{1, 2, 3\}$  and  $B = u, v$ .

$$A \times B = \{(1, u), (1, v), (2, u), (2, v), (3, u), (3, v)\}$$

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

### 1.3 Relations and Functions

**Relations** Let  $A$  and  $B$  be sets. A **relation** from  $A$  to  $B$  is a subset of the Cartesian product  $A \times B$ .

$$R \subseteq A \times B$$

- If  $(x,y) \in R$ , we say that  $x$  is related to  $y$  by  $R$ , denoted as  $xRy$ .
- **A** is in the **domain** of **R**
- **B** is the **codomain** of **R**

**Example** Let  $A = \{1, 2, 3\}$  and  $B = \{1, 2\}$  and define a relation  $R$  from  $A$  to  $B$  as follows:

$$(x, y) \in R \iff \frac{x+y}{2} \in \mathbb{Z}$$
$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1)\}$$
$$\text{Domain of } R = \{1, 2, 3\}$$
$$\text{Codomain of } R = \{1, 2\}$$

### Functions

**Definition** Let  $A$  and  $B$  be two sets. A function  $F$  from  $A$  to  $B$  is a relation with domain  $A$  and co-domain  $B$  that satisfies the following properties:

- For every element  $x \in A$ , there is an element  $y \in B$  such  $(x, y) \in F$
- For every element  $x \in A$  and  $y, z \in B$ :
  - If  $(x, y) \in F$  and  $(x, z) \in F$ , then  $y = z$

**Example** Let  $A = \{2, 4, 6\}$  and  $B = \{1, 3, 5\}$ . Which of the relations defined below are functions from A to B?

- $R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$ 
  - Not a function because 4 is related to 1 and 3. This is not a many-to-one relationship.
- For all  $(x, y) \in A \times B, (x, y) \in S \iff y = x + 1$ 
  - $S = \{(2, 3), (4, 5)\}$  is a function from A to B.
- $T = \{(2, 5), (4, 1), (6, 1)\}$ 
  - $T$  is a function from A to B as A has a many-to-one relationship with B.

### Equivalent Functions

Let A and B be two sets. Two functions  $f$  and  $g$  from A to B:

$$f = g \iff f(x) = g(x) \quad \forall \quad x \in A$$



## 2. The Logic of Compound Statements

### 2.1 Logical Form and Equivalence

---

#### Arguments

**Definition** 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.
- The statements that support the conclusion are called premises.
- If the premises are true, the conclusion must also be true.

#### Example

- If student A is a math major or student A is a computer science major,
- Then student A will take Discrete Math.

#### Logical Statements

**Definition** A logical statement is a declarative sentence that is either true or false, but not both.

- Not  $p$ :  $\neg p$
- $p$  and/but  $q$ :  $p \wedge q$
- $p$  or  $q$ :  $p \vee q$
- Neither  $p$  nor  $q$ :  $\neg p \wedge \neg q$

**Example**  $h$  = healthy,  $w$  = wealthy,  $s$  = wise

- John is healthy and wealthy but not wise.
  - $(h \wedge w) \wedge \neg s$
- John is neither wealthy nor wise, but he is healthy
  - $(\neg w \wedge \neg s) \wedge h$

### Equivalent Statements

**Definition** Two logical statements are equivalent if they have the same truth tables, denoted:

$$p \equiv q$$

**De Morgan's Laws** The negation ( $\neg$ ) of an and statement is logically equivalent to the or statement of the negations. Similarly, the negation of an or statement is logically equivalent to the and statement of the negations.

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

### Tautological and Contradictory Statements

- A tautological statement is a statement that is always true.
- A contradictory statement is a statement that is always false.

## 2.2 Conditional Statements

---

**Definition** A Conditional statement is in the form "If  $p$ , then  $q$ " and is denoted as  $p \implies q$ . This is read as  $p$  implies  $q$ .

- $p$  is the **hypothesis** of the statement.
- $q$  is the **conclusion** of the statement.

### Order of Operations

- $()$ : parentheses
- $\neg$ : negation
- $\wedge/\vee$ : conjunction/disjunction
- $\implies$ : implication

### Equivalent of Conditional Statements

$$\begin{aligned} p \implies q &\equiv \neg p \vee q \\ \neg(p \implies q) &\equiv p \wedge \neg q \end{aligned}$$

**Example** Find the negation of the following statement: "If my car is in the repair shop then I cannot go to class".

- Hypothesis ( $p$ ): "My car is in the repair shop"
- Conclusion ( $q$ ): "I cannot go to class"
- Convert:  $p \implies q \equiv \neg p \vee q$
- Negation:  $\neg(p \implies q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$
- Convert back: "My car is in the repair shop and I can go to class"

**Negation vs Inverse** The negation of a statement is NOT the same as the inverse of the statement.

- Negation:  $\neg(p \implies q)$
- Inverse:  $\neg p \implies \neg q$

**Example** If  $p$  is a square, then  $p$  is a rectangle.

- Hypothesis ( $p$ ): "p is a square"
- Conclusion ( $q$ ): "p is a rectangle"
- Negation:  $\neg(p \implies q) \equiv p \wedge \neg q$
- Convert back: "p is a square and p is not a rectangle"
- Inverse:  $\neg p \implies \neg q \equiv p \vee \neg q$
- Convert: "If p is not a square, then p is not a rectangle"

**More statement types**

- Contrapositive of  $p \implies q \equiv \neg q \implies \neg p$
- Converse of  $p \implies q \equiv q \implies p$
- Inverse of  $p \implies q \equiv \neg p \implies \neg q$

**Example** If today is Easter then tomorrow is Monday.

- Hypothesis ( $p$ ): "Today is Easter"
- Conclusion ( $q$ ): "Tomorrow is Monday"
- Convert:  $p \implies q$
- Contrapositive:  $\neg q \implies \neg p \equiv$  If tomorrow is not Monday, then today is not Easter
- Converse:  $q \implies p \equiv$  If tomorrow is Monday, then today is Easter
- Inverse:  $\neg p \implies \neg q \equiv$  If today is not Easter, then tomorrow is not Monday

**Biconditional Statements** A biconditional statement is in the form "p if and only if q" and is denoted as  $p \iff q$ . This is read as  $p$  if and only if  $q$ .

$$p \iff q \equiv (p \implies q) \wedge (q \implies p) \quad (1)$$

**Sufficient and Necessary Conditions** If  $r$  and  $s$  are statements:

- $r$  is a **sufficient condition** for  $s$  if  $r \implies s$ .
- $r$  is a **necessary condition** for  $s$  if  $s \implies r$  or  $s \implies r$ .
- $r$  is a **necessary and sufficient condition** for  $s$  if  $r \iff s$ .

## 2.3 Valid and Invalid Arguments

---

**Definition** An **argument** is a sequence of statements, and an **argument form** is a sequence of statement form.

- The final statement or statement form is called the **conclusion**. The symbol  $\therefore$  (therefore) is used to denote the conclusion.
- All the preceding statements or statement forms are called **premises**, or assumptions or hypotheses.
- An argument form is **valid** means if all premises are true, then the conclusion must also be true.

**Example** Determine whether the following argument form is valid or invalid:

$$\begin{aligned}p &\implies q \vee \neg r \\q &\implies p \wedge r \\ \therefore p &\implies r\end{aligned}$$

$p$	$q$	$r$	$p \implies (q \vee \neg r)$	$q \implies (p \wedge r)$	$p \implies r$	Valid?
T	T	T	T	T	T	Valid
T	T	F	F	T	F	Invalid
T	F	T	T	F	T	Invalid
T	F	F	F	F	F	Invalid
F	T	T	T	F	T	Invalid
F	T	F	T	F	T	Invalid
F	F	T	T	F	T	Invalid
F	F	F	T	F	T	Invalid

Therefore the argument form is invalid.

## Syllogisms

**Definition** An argument form with two premises are called syllogism. The first and second premises are called the major premise and minor premise respectively.

**Modus Ponens** Modus Ponens is a valid argument form that can be expressed as:

$$\begin{array}{l} p \implies q \\ p \\ \therefore q \end{array}$$

This means that if  $p \implies q$  (if  $p$  then  $q$ ) is true, and  $p$  is true, then we can conclude that  $q$  must also be true.

**Example** If there are more pigeons than there are pigeonholes, then at least two pigeons roost in the same hole.

There are more pigeons than there are pigeonholes.

$\therefore$  At least two pigeons roost in the same hole.

**Modus Tollens** Modus Tollens is a valid argument form that can be expressed as:

$$\begin{array}{l} p \implies q \\ \neg q \\ \therefore \neg p \end{array}$$

This means that if  $p \implies q$  (if  $p$  then  $q$ ) is true, and  $q$  is false, then we can conclude that  $p$  must also be false.

**Rules of Inference** A rule of inference is a form of argument that is valid. Both modus ponens and modus tollens are rules of inference. The following are additional examples of rules of inference:

A <b>rule of inference</b> is a form of argument that is valid. Both modus ponens and modus tollens are rule of inference. The following are additional examples of rules of inference.			
Modus Ponens	$p \rightarrow q$ $p$ $\therefore q$	Elimination	a. $p \vee q$ $\sim q$ $\therefore p$ b. $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \sim p$	Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$
Generalization	a. $p$ $\therefore p \vee q$ b. $q$ $\therefore p \vee q$	Proof by Division into Cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore r$
Specialization	a. $p \wedge q$ $\therefore p$ b. $p \wedge q$ $\therefore q$		
Conjunction	$p$ $q$ $\therefore p \wedge q$	Contradiction Rule	$\sim p \rightarrow c$ (contradiction) $\therefore p$

Prove by Detachment  
Prove by contrapositive  
Disjunctive of syllogism  
Law of Syllogism

## Contradictions

**Definition** A contradiction is a statement that is always false.

$$\neg p \implies c$$

$$\therefore p$$



**2 column rule** The 2 column rule is a way to prove by contradiction. For example with knights and knaves. Knights always tell the truth and knaves always lie:

- A says B is a knight
- B says A and I are of opposite types

---

Suppose A is a knight:

What A says must be true	By the definition of a knight
B is a knight	by given (what A says)
What B says must be true	By the definition of a knight
A and B are of opposite types	by given (what B says)
Contradiction	A is not a knight or A is a knave
The supposition is false	by rule of contradiction
A is not a knight or A is a knave	by negation of supposition.

# 3. The Logic of Quantified Statements

## 3.1 Predicates and Quantified Statements (Part 1)

---

### Predicates

**Definition** A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. For example: " $P(x)$  :  $x$  is a positive integer" is a predicate. The statement  $P(3)$  is true, while  $P(-2)$  is false.

**Domain of a Predicate** The Domain of a predicate is the set of all values that can be substituted for the variable.

**Example** Let  $P(x)$  be the predicate " $x^2 > x$ ." The domain of  $P(x)$  is  $\mathbb{R}$ .

$$\begin{aligned} P\left(\frac{1}{2}\right) : \quad \left(\frac{1}{2}\right)^2 &> \frac{1}{2} && = \text{False} \\ P\left(-\frac{1}{2}\right) : \quad \left(-\frac{1}{2}\right)^2 &> -\frac{1}{2} && = \text{True} \\ P(2) : \quad 2^2 &> 2 && = \text{True} \end{aligned}$$

### Truth Sets

**Definition** If  $P(x)$  is a predicate with domain  $D$ , the truth set of  $P(x)$  is the set of all elements in  $D$  for which  $P(x)$  is true when they are substituted for  $x$ . The truth set of  $P(x)$  is denoted by:

$$\{x \in D \mid P(x)\} \subseteq D$$

**Example** Let  $P(x)$  be the predicate " $x^2 \leq 30$ " with domain  $\mathbb{Z}$ . The truth set of  $P(x)$  is:

$$\{x \in \mathbb{Z} \mid P(x)\} = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

## Quantified Statements

**Definition** A quantified statement is a statement that contains a quantifier. The two most common quantifiers are:

- **Universal Quantifier**  $\forall$  (for all)
- **Existential Quantifier**  $\exists$  (there exists)

**Universal Statements** Let  $P(x)$  be a predicate with domain  $D$ . A universal statement is a statement of the form " $\forall x \in D, P(x)$ " which is read as "for all  $x$  in  $D$ ,  $P(x)$  is true."

- It is defined to be true if and only if  $P(x)$  is true for all  $x$  in  $D$ .
- It is defined to be false if and only if  $P(x)$  is false for at least one  $x$  in  $D$ .
- The value of  $x$  for which  $P(x)$  is false is called a counterexample.

**Example** Let  $D = \{1, 2, 3\}$ , and show that the statement " $\forall x \in D, x^2 \geq x$ " is true.

$$\begin{aligned}1^2 &\geq 1 \text{ is true} \\2^2 &\geq 2 \text{ is true} \\3^2 &\geq 3 \text{ is true} \\\therefore \quad \forall x \in D, x^2 &\geq x \text{ is true.}\end{aligned}$$

**Existential Statements** Let  $P(x)$  be a predicate with domain  $D$ . An existential statement is a statement of the form " $\exists x \in D \ni P(x)$ " which is read as "there exists an  $x$  in  $D$  such that  $P(x)$  is true."

- It is defined to be true if and only if  $P(x)$  is true for at least one  $x$  in  $D$ .
- It is defined to be false if and only if  $P(x)$  is false for all  $x$  in  $D$ .
- The value of  $x$  for which  $P(x)$  is true is called a witness.

**Example** Show that the statement " $\exists x \in \mathbb{Z} \ni \frac{1}{x} = x$ " is true.

$$x = 1 : \frac{1}{1} = 1 \text{ is true}$$

$$\therefore \exists x \in \mathbb{Z} \ni \frac{1}{x} = x \text{ is true.}$$

**Universal Conditional Statements** A universal conditional statement is a statement of the form " $\forall x \in D, P(x) \implies Q(x)$ " which is read as "for all  $x$  in  $D$ , if  $P(x)$  is true, then  $Q(x)$  is true."

## 3.2 Predicates and Quantified Statements (Part 2)

---

### Negations of Quantified Statements

#### Negation of a Universal Statement

$$\neg(\forall x \in D, P(x)) \equiv \exists x \in D \ni \neg P(x)$$

#### Negation of an Existential Statement

$$\neg(\exists x \in D \ni P(x)) \equiv \forall x \in D, \neg P(x)$$

#### Negation of a Universal Conditional Statement

$$\neg(\forall x \in D, P(x) \implies Q(x)) \equiv \exists x \in D \ni P(x) \wedge \neg Q(x)$$

Consider the statement:  $\forall x \in D, P(x) \implies Q(x)$ .

It's contrapositive is:  $\forall x \in D, \neg Q(x) \implies \neg P(x)$

It's converse is:  $\forall x \in D, Q(x) \implies P(x)$

It's inverse is:  $\forall x \in D, \neg P(x) \implies \neg Q(x)$

### 3.3 Statements with Multiple Quantifiers

---

Consider the statement:  $\forall x \in D, \exists y \in E \ni P(x, y)$ . To show the truth of the statement, we must show that for every  $x$  in  $D$ , there exists a  $y$  in  $D$  such that  $P(x, y)$  is true.

**Example** Let  $D = \{1, 2, 3\}$  and  $P(x, y)$  be the predicate " $x + y = 4$ ". Show that the statement  $\forall x \in D, \exists y \in D \ni P(x, y)$  is true.

$$\begin{aligned}x = 1 : \quad & \exists y \in D \ni 1 + y = 4 \implies y = 3 \\x = 2 : \quad & \exists y \in D \ni 2 + y = 4 \implies y = 2 \\x = 3 : \quad & \exists y \in D \ni 3 + y = 4 \implies y = 1 \\\therefore \quad & \forall x \in D, \exists y \in D \ni P(x, y) \text{ is true.}\end{aligned}$$

Consider the statement:  $\exists x \in D \ni \forall y \in D, P(x, y)$ . To show the truth of the statement, we must show that there exists an  $x$  in  $D$  such that for every  $y$  in  $D$ ,  $P(x, y)$  is true.

**Example** Let  $D = \{1, 2, 3\}$  and  $P(x, y)$  be the predicate " $x + y = 4$ ". Show that the statement  $\exists x \in D \ni \forall y \in D, P(x, y)$  is false.

$$\begin{aligned}x = 1 : \quad & \forall y \in D, 1 + y = 4 \implies y = 3 \\x = 2 : \quad & \forall y \in D, 2 + y = 4 \implies y = 2 \\x = 3 : \quad & \forall y \in D, 3 + y = 4 \implies y = 1 \\\therefore \quad & \exists x \in D \ni \forall y \in D, P(x, y) \text{ is false.}\end{aligned}$$

#### Negation of Multiply-Quantified Statements

$$\begin{aligned}\neg(\forall x \in D, \exists y \in E \ni P(x, y)) &\equiv \exists x \in D \ni \forall y \in E, \neg P(x, y) \\\neg(\exists x \in D, \forall y \in E, P(x, y)) &\equiv \forall x \in D, \exists y \in E \ni \neg P(x, y)\end{aligned}$$

### 3.4 Arguments with Quantified Statements

---

#### Universal Model Ponens (Direct Proof)

$\forall x, P(x) \implies Q(x)$	If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true.
$P(a)$	Input $a$ makes $P(a)$ true.
$\therefore Q(a)$	Therefore $a$ makes $Q(a)$ true.

**Example** Let  $P(x)$  be the predicate " $x$  is a prime number" and  $Q(x)$  be the predicate " $x$  is an odd number".

$\forall x, P(x) \implies Q(x)$	If $x$ is a prime number, then $x$ is an odd number.
$P(3)$	3 is a prime number,
$\therefore Q(3)$	therefore 3 is an odd number.

#### Universal Modus Tollens (Prove by Contradiction)

$\forall x, P(x) \implies Q(x)$	If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true.
$\neg Q(a)$	Input $a$ makes $Q(a)$ false.
$\therefore \neg P(a)$	Therefore $a$ does not make $P(a)$ true.

**Example** Consider the statement "All irrational numbers are real numbers.":

$\forall x \in \mathbb{R} - \mathbb{Q}, x \in \mathbb{R}$	If $x$ is an irrational number, then $x$ is a real number.
$\frac{1}{0} \notin \mathbb{R}$	$\frac{1}{0}$ is not a real number,
$\therefore \frac{1}{0} \notin \mathbb{R} - \mathbb{Q}$	therefore $\frac{1}{0}$ is not an irrational number.

#### Converse and Inverse Errors

##### Converse Error

$\forall x, P(x) \implies Q(x)$	$Q(a) \therefore P(a)$ (Invalid Argument)
---------------------------------	---

### **Inverse Error**

$$\forall x, P(x) \implies Q(x) \quad \neg P(a) \therefore \neg Q(a) \text{ (Invalid Argument)}$$



# 4. Elementary Number Theory and Methods of Proof

## 4.1 Direct Proof and Counterexample

---

**Definitions** Let  $P(n)$  be the predicate "n is an even number".

$$\begin{aligned}\forall n \in \mathbb{Z}, P(n) &\iff \exists k \in \mathbb{Z} \ni n = 2k. \\ \forall n \in \mathbb{Z}, \neg P(n) &\iff \exists k \in \mathbb{Z} \ni n = 2k + 1.\end{aligned}$$

**Example** Is -301 even or odd?

$$-301 = 2k + 1 \text{ for } k = -151$$

**Example** If  $a, b \in \mathbb{Z}$ , is  $6a^2b$  even?

$$\begin{aligned}\exists a, b \in \mathbb{Z} \ni 6a^2b &= 2(k) + 1 \\ 6a^2b &= 2(3a^2b) \text{ for } k = 3a^2b \\ \therefore 6a^2b &\text{ is even.}\end{aligned}$$

**Prime and Composite Number Definition** Let  $P(n)$  be the predicate "n is a prime number".

$$\begin{aligned}\forall n \in \mathbb{Z}_{>1}, P(n) &\iff \forall r, s \in \mathbb{Z}_{>1}, n = rs \implies r = n \vee s = n \\ \forall n \in \mathbb{Z}_{>1}, \neg P(n) &\iff \exists r, s \in \mathbb{Z}_{>1} \ni n = rs \wedge 1 < r < n \wedge 1 < s < n\end{aligned}$$

### Constructive Proof of Existential Statement

$$\exists x \text{ in } D \ni Q(x)$$

- Find an  $x$  in  $D$  that makes  $Q(x)$  true.
- Give a set of directions for finding such an  $x$  in  $D$

**Example** Prove there is an even integer  $n$  such that  $n$  can be written in two ways as a sum of two prime numbers.

Let  $n = 10$ ,

$$10 = 3 + 7$$

$$10 = 5 + 5$$

$\therefore$  the statement is true.

### Disproving Universal Statement by Counterexample

$$\forall x \in D, P(x) \implies Q(x)$$

- Find an  $x$  in  $D$  that makes  $P(x)$  true, but  $Q(x)$  false.

### Method of Exhaustion of Proving Universal Statement

$$\forall x \in D, P(x) \implies Q(x)$$

- Check all  $x$  in  $D$  to make sure that when  $P(x)$  is true,  $Q(x)$  is false.

### Direct Proof of Universal Statement

$$\forall x \in D, P(x) \implies Q(x)$$

- Suppose  $x$  is an arbitrary element in  $D$  for which the hypothesis  $P(x)$  is true.
- Using definitions or previously established results and rules to conclude  $Q(x)$  is true.

**Example** Prove the statement "the sum of any two even integers is even."

Suppose  $a$  and  $b$  are two even integers

$$\therefore a = 2k, \exists k_1 \in \mathbb{Z}$$

$$\therefore b = 2k, \exists k_2 \in \mathbb{Z}$$

$$\therefore a + b = 2k_1 + 2k_2$$

$$\therefore a + b = 2(k_1 + k_2)$$

$$\therefore a + b \text{ is even}$$

## 4.2 Skipped

---

## 4.3 Rational Numbers

---

### Definitions

- A real number  $r$  is rational if and only if  $\exists a, b \in \mathbb{Z}$  such that  $r = \frac{a}{b} \wedge b \neq 0$ .
- A real number that is not rational is irrational.

**Example** Is 320.5492492492... a rational number? (The 492 repeats). We can split the number into two parts: 320.5 and 0.0492492...

First we rewrite 320.5 as a fraction:

$$320.5 = \frac{3205}{10}$$

Then we rewrite 0.0492492... as a fraction:

$$10000(0.0492492...) - 10(0.0492492...) = 492.492... = 0.492492... = 492$$

$$\Rightarrow 10000x - 10x = 492$$

$$\Rightarrow 9990x = 492$$

$$\Rightarrow x = \frac{492}{9990}$$

Now we can combine the two fractions:

$$320.5492492... = \frac{3205}{10} + \frac{492}{9990}$$

$$\Rightarrow \frac{3205 \cdot 999}{10 \cdot 999} + \frac{492 \cdot 1}{9990}$$

$$\Rightarrow \frac{3205 \cdot 999 + 492}{9990}$$

$$\Rightarrow \frac{3199995 + 492}{9990}$$

$$\Rightarrow \frac{3200487}{9990}$$

$\therefore$  320.5492492... is rational.

## Zero Product Property

**Theorem** If neither of two real numbers is zero, then their product is non-zero. The contrapositive of this theorem is also true: If the product of two real numbers is zero, then at least one of the two numbers is zero.

Let  $a, b \in \mathbb{Q}$

If  $ab = 0 \Rightarrow a = 0 \vee b = 0$

If  $ab \neq 0 \Rightarrow a \neq 0 \wedge b \neq 0$

### Example

Let  $a, b \in \mathbb{Q}$  :

$\therefore a = \frac{n_1}{d_1}, \exists n_1, d_1 \in \mathbb{Z} \wedge d_1 \neq 0$       Definition of rational numbers.

$\therefore b = \frac{n_2}{d_2}, \exists n_2, d_2 \in \mathbb{Z} \wedge d_2 \neq 0$

$\therefore a + b = \frac{n_1}{d_1} + \frac{n_2}{d_2}$       Substitution principle.

$\therefore a + b = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}$

$\therefore d_1 d_2 \neq 0$       Zero product property

$\therefore a + b$  is rational

## Corollaries

**Definition** A corollary is a statement whose truth can be immediately deduced from a theorem that has already been proven.

**Example** Prove that the product of two rational numbers is rational.

Let  $a, b \in \mathbb{Q}$  :

$$\therefore a = \frac{n}{m}, \exists n, m \in \mathbb{Z} \wedge m \neq 0 \quad \text{Definition of rational numbers.}$$

$$\therefore b = \frac{s}{t}, \exists s, t \in \mathbb{Z} \wedge t \neq 0$$

$$\therefore a \cdot b = \frac{n}{m} \cdot \frac{s}{t}, m \neq 0 \wedge t \neq 0$$

$$\therefore ab = \frac{ns}{mt}, mt \neq 0 \quad \text{Zero product property.}$$

$$\therefore ab \in \mathbb{Q}$$

**Example** Prove or disprove by counterexample the following statement:  
"The quotient of any 2 rational numbers is rational."

$$\forall p, q \in \mathbb{Q}, \frac{p}{q} \in \mathbb{Q} \quad \text{Statement}$$

$$\text{Let } p = 1, q = 0$$

$$\therefore \frac{p}{q} \notin \mathbb{Q}$$

$$\therefore \exists p, q \in \mathbb{Q} \ni \frac{p}{q} \notin \mathbb{Q}$$

**Example** Prove or disprove by counterexample the following statement:  
 $\forall a, b \in \mathbb{R}, a < b \implies a < \frac{a+b}{2} < b$ .

$$\therefore a < b \implies a + b < 2b$$

$$\therefore \frac{1}{2} > 0$$

$$\therefore a < b \wedge \frac{1}{2} > 0 \implies \frac{a+b}{2} < \frac{b}{2}$$

$$\therefore a < b \implies 2a < b + a$$

$$\therefore \frac{1}{2} > 0$$

$$\therefore a < b \wedge \frac{1}{2} > 0 \implies a < \frac{a+b}{2}$$

$$\therefore a < \frac{a+b}{2} \wedge \frac{a+b}{2} < b \equiv a < \frac{a+b}{2} < b$$

## 4.4 Divisibility

---

**Definitions** If  $n$  and  $d$  are integers and  $d \neq 0$ , then  $n$  is divisible by  $d$  if and only if  $n = dk$  for some integer  $k$ .

- Notation:  $d|n$  is read "d divides n".
  - $d|n \iff \exists k \in \mathbb{Z} \ni n = dk$
  - Note that the factor comes first in this notation.

It is equivalent to the following statements:

- $n$  is a multiple of  $d$
- $d$  is a factor of  $n$
- $d$  is a divisor of  $n$
- $d$  divides  $n$

**Example** Prove the following statement:  $\forall a, b, c \in \mathbb{Z}, a|b \wedge a|c \implies a|(b + c)$ .

Suppose  $a, b, c \in \mathbb{Z} \wedge a|b \wedge a|c$

$\therefore b = ak, \exists k \in \mathbb{Z}$  Definition of Divisibility

$\therefore c = am, \exists m \in \mathbb{Z}$

$\therefore b + c = a(k + m)$  Substitution and distributive

$\therefore k + m \in \mathbb{Z}$  Integers are closed under addition

$\therefore a|(b + c)$  Def. of divisibility

### Divisibility Theorems

#### Positive Divisor of a Positive Integer Theorem

$$\forall a, b \in \mathbb{Z}, a > 0 \wedge b > 0 \wedge a|b \implies a \leq b.$$

**Divisors of 1 Theorem** The only divisors of 1 are 1 and -1.

### Transitivity of Divisibility Theorem

$$\forall a, b, c \in \mathbb{Z}, a|b \wedge b|c \implies a|c$$

**Divisible by a Prime Theorem** Any integer  $n \neq 1$  is divisible by a prime number.

**Unique Factorization of Integers Theorem** Given any integer  $n \neq 1$ , there exists  $k$  many distinct prime numbers  $(p_1, \dots, p_k)$  and  $k$  many positive integers  $(e_1, \dots, e_k)$ , where  $k$  is a positive integer, such that:

$$n = \prod_{i=1}^k p_i^{e_i}$$

**Example** If  $a = \prod_{i=1}^k p_i^{e_i}$ , find the standard factored form of  $a^2$ :

$$\begin{aligned} a^2 &= \prod_{i=1}^k p_i^{e_i} \cdot \prod_{i=1}^k p_i^{e_i} \\ &= (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \cdot (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\ &= p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k} \\ &= \prod_{i=1}^k p_i^{2e_i} \end{aligned}$$



## 4.5 The Quotient-Remainder Theorem

### Theorem

$$\forall n \in \mathbb{Z}, \forall d \in \mathbb{Z}^+, \exists q, r \in \mathbb{Z} \ni n = dq + r \wedge 0 \leq r < d$$

**Definition** Given any integer  $n$  and any positive integer  $d$ :

$$\begin{aligned} n \div d &= q \\ n \bmod d &= r \end{aligned}$$

**Example** If today is tuesday, what day of the week will it be in 365 days?

$$365 \bmod 7 = 1 \text{Tuesday} + 1 \text{ day} = \text{Wednesday}$$

### The Parity Property

**Definition** We call the fact that any integer is either even or odd the parity property.

( Method of Proof by Division Into Cases) To prove a statement of the form  
"If  $A_1 \text{ or } A_2 \dots \text{ or } A_n$ , then  $C$ ."

**Example** The product of two consecutive integers is even.

$$\exists n \in \mathbb{Z}$$

Case 1:  $2|n$

$$\begin{aligned} \therefore 2|n &\implies \exists k \in \mathbb{Z} \ni n = 2k \implies n + 1 = 2k + 1 \\ \therefore n(n + 1) &= 2k(2k + 1) = 2(2k^2 + k) \\ \therefore k \in \mathbb{Z} &\implies 2k^2 + k \in \mathbb{Z} \\ \therefore n(n + 1) &= 2(2k^2 + k) \wedge 2k^2 + k \in \mathbb{Z} \implies [2|n(n + 1)] \end{aligned}$$

Case 2:  $\neg(2|n)$

$$\begin{aligned} \therefore \neg(2|n) &\implies \exists k \in \mathbb{Z} \ni n = 2k + 1 \implies n + 1 = 2k + 2 \\ \therefore n(n + 1) &= (2k + 1)(2k + 2) = 2(2k^2 + 3k + 1) \\ \therefore k \in \mathbb{Z} &\implies 2k^2 + 3k + 1 \in \mathbb{Z} \\ \therefore n(n + 1) &= 2(2k^2 + 3k + 1) \wedge 2k^2 + 3k + 1 \in \mathbb{Z} \implies [2|n(n + 1)] \\ \therefore [2|n(n + 1)] \end{aligned}$$

## Absolute Value

**Definition** For any real number  $x$ , the absolute value of  $x$ , delotes  $|x|$ , is defined as:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

**Lemma**

$$\begin{aligned} \forall r \in \mathbb{R}, -|r| &\leq r \leq |r| \\ \forall r \in \mathbb{R}, |-r| &= |r| \end{aligned}$$

## The Triangle Inequality

$$\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$$

## 4.6 Skipped

## 4.7 Contradiction and Contraposition

---

### Method of Proof by Contradiction

- Suppose the opposite of the to-be proved conclusion.
- Show that this supposition leads logically to a contradiction (a statement that is always false).
- Conclude that the statement to be proved is true.

**Example** Prove the theorem by contradiction: "There is no greatest integer."

Suppose:  $\exists m \in \mathbb{Z} \ni \forall n \in \mathbb{Z}, n \leq m$       Opposite of theorem  
 $\therefore \exists n \in \mathbb{Z} \ni n = m + 1$   
 $\therefore \nexists m \in \mathbb{Z} \ni \forall n \in \mathbb{Z}, n \leq m$

**Example** Prove the theorem by contradiction: "The square root of any irrational number is irrational."

Theorem: $\forall n \notin \mathbb{Q}, \sqrt{n} \notin \mathbb{Q}$	Theorem
Suppose: $\forall n \notin \mathbb{Q}, \sqrt{n} \in \mathbb{Q}$	Opposite of theorem
$\therefore \sqrt{n} \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z} \ni \sqrt{n} = \frac{a}{b} \wedge b \neq 0$	Definition of rational numbers
$\therefore \sqrt{n} = \frac{a}{b} \implies n = \frac{a^2}{b^2}$	Squaring both sides
$\therefore a, b \in \mathbb{Z} \implies a^2, b^2 \in \mathbb{Z}$	Integers are closed under squaring
$\therefore n = \frac{a^2}{b^2} \wedge a^2, b^2 \in \mathbb{Z} \implies n \in \mathbb{Q}$	Definition of rational numbers
$\therefore n \in \mathbb{Q} \wedge n \notin \mathbb{Q}$	Contradiction
$\therefore$ The assumption is false, and the theorem is true.	

**Example** Prove the theorem by contradiction: "The sum of any rational number and any irrational number is irrational."

Theorem:  $\forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \notin \mathbb{Q}$

Suppose:  $\forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \in \mathbb{Q}$

Opposite of theorem

$\therefore n + b \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z} \ni n + m = \frac{a}{b} \wedge b \neq 0$  Definition of rational numbers

$\therefore m = \frac{a}{b} - n$

$\therefore n \in \mathbb{Q} \implies \exists x, y \in \mathbb{Z} \ni n = \frac{x}{y} \wedge y \neq 0$  Definition of rational numbers

$\therefore m = \frac{a}{b} - \frac{x}{y}$

$\therefore m = \frac{ay - bx}{by} \implies m \in \mathbb{Q}$

$\therefore m \in \mathbb{Q} \wedge m \notin \mathbb{Q}$

Contradiction

$\therefore \forall n \in \mathbb{Q}, \forall m \notin \mathbb{Q}, n + m \notin \mathbb{Q}$

The theorem is true.

### Method of Proof by Contraposition

- Express the given statement in the form of " $\forall x \in D, P(x) \implies Q(x)$ ".
- Rewrite in contrapositive form: " $\forall x \in D, \neg Q(x) \implies \neg P(x)$ ".
- Prove the contrapositive by direct proof.
  - Suppose  $\exists x \in D \ni \neg Q(x)$ .
  - Prove  $\neg P(x)$ .

**Example** Prove the statement by contraposition: "For all integers m and n, if mn is even then m is even or n is even."

Theorem:  $\forall m, n \in \mathbb{Z}, 2|mn \implies 2|m \vee 2|n$

Contrapositive:  $\forall m, n \in \mathbb{Z}, \neg(2|m) \wedge \neg(2|n) \implies \neg(2|mn)$

Suppose:  $\exists m, n \in \mathbb{Z} \ni \neg(2|m) \wedge \neg(2|n)$

$\therefore \neg(2|m) \wedge \neg(2|n) \implies \exists k, l \in \mathbb{Z} \ni m = 2k + 1 \wedge n = 2l + 1$

$\therefore mn = (2k + 1)(2l + 1)$

$\implies mn = 4kl + 2k + 2l + 1 \implies mn = 2(2kl + k + l) + 1$

$\therefore k, l \in \mathbb{Z} \implies 2kl + k + l \in \mathbb{Z}$

$\therefore mn = 2(2kl + k + l) + 1 \wedge 2kl + k + l \in \mathbb{Z} \implies \neg(2|mn)$

# 5. Sequences, Induction, and Recursion

## 5.1 Sequences

---

**Definition** A sequence is a function whose **domain** is either all the **integers** between two given integers or all the integers greater than or equal to a given integers.

**Notation**

$$\begin{aligned}a_1 &= f(1) \\&\dots \\a_{n-1} &= f(n-1) \\a_n &= f(n) \\a_{n+1} &= f(n+1)\end{aligned}$$

**Example** Write the first three terms of the sequence whose **explicit** or **general formula** is given:

$$\begin{aligned}a_n &= \frac{(-1)^n}{2^n + 1} \text{ for } n \geq 1 \\a_1 &= \frac{(-1)^1}{2^1 + 1} = -\frac{1}{3} \\a_2 &= \frac{(-1)^2}{2^2 + 1} = \frac{1}{5} \\a_3 &= \frac{(-1)^3}{2^3 + 1} = -\frac{1}{9}\end{aligned}$$

## Summation Notation

**Definition** If  $m$  and  $n$  are integers and  $m \leq n$ , then a **series** can be notated as:

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + \cdots + a_n$$

- **Read as** “the summation from  $i = m$  to  $n$  of  $a$ -sub- $i$ ”
- $i$  is called the **index** of the Summation
- $m$  is called the **lower limit** of the Summation
- $n$  is called the **upper limit** of the summation

**Example** Expand and evaluate the following:

$$\begin{aligned}\sum_{i=2}^6 (i-1)^2 \\&= 1 + 4 + 9 + 16 + 25 \\&= 55\end{aligned}$$

**Re-indexing a Summation** Re-indexing a summation involves changing the index variable or the limits of summation, often to simplify the expression or to match another sum’s index.

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i^2} \\&= \sum_{i=1}^n \frac{1}{i^2} + \frac{1}{(n+1)^2}\end{aligned}$$



**Example** If  $j = i + 1$ , transform the following summation by rewriting it in terms of  $j$ :  $\sum_{i=4}^{k-1} i(i-1)$

$$i = 4 \implies j = 4 + 1 = 5 \quad \text{Rewrite lower limit.}$$

$$i = k - 1 \implies j = k - 1 + 1 = k \quad \text{Rewrite upper limit}$$

$$j = i + 1 \implies i = j - 1 \quad \text{Rewrite i in terms of j}$$

$$\sum_{j=5}^k (j-1)(j-2) \quad \text{Rewrite sum}$$

## Product Notation

**Definition** If  $m$  and  $n$  are integers and  $m \leq n$ , then a **series** can be notated as:

$$\prod_{i=m}^n a_i = a_m \cdot a_{m+1} \cdot \cdots \cdot a_n$$

- **Read as** “the product from  $i = m$  to  $n$  of  $a$ -sub- $i$ ”
- $i$  is called the **index** of the product
- $m$  is called the **lower limit** of the product
- $n$  is called the **upper limit** of the product

**Example** Expand and evaluate the following:

$$\begin{aligned} & \prod_{k=2}^5 \frac{k}{k+1} \\ &= \frac{2}{2+1} \cdot \frac{3}{3+1} \cdot \frac{4}{4+1} \cdot \frac{5}{5+1} \\ &= \frac{1}{3} \end{aligned}$$

**Theorem** Given sequences  $\{a\}$  and  $\{b\}$  and  $c \in \mathbb{R}$ , the following equations hold:

$$\begin{aligned}\sum_{i=m}^n a_i + \sum_{i=m}^n b_i &= \sum_{i=m}^n (a_i + b_i) \\ c \cdot \sum_{i=m}^n a_i &= \sum_{i=m}^n c \cdot a_i \\ \prod_{i=m}^n a_i \cdot \prod_{i=m}^n b_i &= \prod_{i=m}^n (a_i b_i)\end{aligned}$$

## Factorials

$$n! = n \cdot (n - 1) \cdot \dots \cdot 2 \cdot 1$$

## Binomial Coefficient

**Definition** Let  $n$  and  $r$  be integers with  $0 \leq r \leq n$ , the binomial coefficient is notated as:

$${}_nC_r = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

It presents the number of combinations of choosing  $r$  items from  $n$  choices.

**Example** Evaluate:

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

## 5.2 Mathematical Induction 1: Proving Formulas

---

### Method of Proof by Induction

**Definition** Induction proof explores the **patterns** we recognize from a list of unknown terms.

**Method** Consider the statement  $\forall n \in \{a \in \mathbb{Z} : n \geq a\}, P(n)$

- Step 1: (**basis step**): Show that  $P(a)$  is true.
- Step 2: (**inductive step**): Show that if we suppose  $P(k)$  is true, then  $P(k+1)$  is true.

**Example** Use the formula to evaluate  $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ .

$$\begin{aligned}\text{Suppose } n &= 50 \\ 1 + 2 + \cdots + 50 &= \frac{50(50 + 1)}{2} \\ &= \frac{50(51)}{2} \\ &= \frac{2550}{2} \\ &= 1275\end{aligned}$$

**Definition** If a sum with a variable number of terms is shown to equal an expression that does not contain either an ellipsis or a summation sign, we can say that the sum is written in **closed form**.

**Example** Use the formula to evaluate  $1 + 2 + \cdots + n$

### Geometric Series

**Definition** If  $r \in \mathbb{R} \wedge r \neq 1$ , the sum of the first  $n$  terms of a geometric series is given by:

$$\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}$$

**Example** Use the above formula to evaluate  $1 + 3 + \cdots + 3^{m-2}$

$$\begin{aligned}
 r &= 3, n = m - 2 \\
 1 + 3 + \cdots + 3^{m-2} &= \sum_{i=0}^{m-2} 3^i \\
 &= \frac{3^{m-1} - 1}{3 - 1} = \frac{3^{m-1} - 1}{2}
 \end{aligned}$$

**Example**  $3^2 + 3^3 + \cdots + 3^m$

$$\begin{aligned}
 3^2 + 3^3 + \cdots + 3^m &= 1 + 3 + 3^2 + 3^3 + \cdots + 3^m - (1 + 3) \\
 \implies [3^0 + 3^1 + 3^2 + 3^3 + \cdots + 3^m] - 4 &= \sum_{i=0}^m 3^i - 4 \quad (r = 3, n = m) \\
 \implies \sum_{i=0}^m 3^i - 4 &= \frac{3^{m+1} - 1}{3 - 1} - 4 = \frac{3^{m+1} - 9}{2}
 \end{aligned}$$

## 5.3 Mathematical Induction 2

---

### Deduction and Induction

#### Definitions

- **Deduction** is to infer a conclusion from general principles using laws of logical reasoning.
- **Induction** is to infer a general principle from specific examples.

**Example** Use mathematical induction to prove  
 $\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, 3|(2^{2n} - 1)$ :

Step 0: Identify the property  $P(n)$

$$P(n) \equiv 3|(2^{2n} - 1)$$

Step 1: Prove  $P(0)$

$$2^{2(0)} - 1 = 2^0 - 1 = 1 - 1 = 0$$

$$3|0$$

$$\therefore 3|(2^{2(0)} - 1)$$

Step 2: Suppose  $P(k)$  is true for  $k \geq 0$ , then prove  $P(k+1)$

$$\text{Suppose } 3|(2^{2k} - 1)$$

$$\implies \exists m \in \mathbb{Z} \ni 2^{2k} - 1 = 3m$$

$$\implies 2^{2(k+1)} - 1 = 2^{2k} \cdot 2^2 - 1$$

$$\implies 2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1$$

$$\implies 2^{2(k+1)} - 1 = 4(2^{2k} - 1) + 3$$

$$\implies 2^{2(k+1)} - 1 = 4(3m) + 3$$

$$\therefore 3|(2^{2(k+1)} - 1)$$

**Example** Use mathematical induction to prove

$$\forall n \in \{x \in \mathbb{Z} : x \geq 5\}, n^2 < 2^n$$

Base Step:  $n = 5$

$$5^2 < 2^5 = 25 < 32$$

Inductive Step: Suppose  $\forall k \in \{x \in \mathbb{Z} : x \geq 5\}, k^2 < 2^k$  then prove  $(k+1)^2 < 2^{k+1}$

$$\text{LHS} = (k+1)^2$$

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

$$k^2 < 2^k \implies k^2 + 2k + 1 < 2^k + [2k + 1]$$

$$\text{RHS} = 2^{k+1}$$

$$2^{k+1} = 2^k \cdot 2^1 = 2^k + [2^k]$$

Prove  $(k+1)^2 < 2^{k+1}$  for  $k \geq 5$  :

$$2 \cdot 5 + 1 = 11 < 32 = 2^5$$

$$2 \cdot 6 + 1 = 13 < 64 = 2^6$$

$$2 \cdot 7 + 1 = 15 < 128 = 2^7$$

and so on.

$$\therefore \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, 2k + 1 < 2^k$$

$$\therefore \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, (k+1)^2 < 2^{k+1}$$

$$\therefore \forall k \in \{x \in \mathbb{Z} : x \geq 5\}, k^2 < 2^k$$

## Recursion

**Definition** A **recursion** is a function that is defined in terms of itself. A recursive function is a function that calls itself.

**Example**  $a_k = 5a_{k-1}$  for all integers  $k \geq 2$ .

## 5.4 Strong Mathematical Induction

---

### Principle of Strong Mathematical Induction

Let  $P(n)$  be a property that is defined for integers  $n$ , and let  $a$  and  $b$  be fixed integers with  $a \leq b$ .

- Basis Step: Show that  $P(a), P(a+1), \dots, P(b)$  are all true.
- Inductive Step: Show that for every integer  $k \geq b$ , if  $P(a), P(a+1), \dots, P(k)$  are all true, then  $P(k+1)$  is true.

**Example** Define a sequence:

$$\begin{aligned}S_0 &= 0 \\S_1 &= 4 \\ \forall k \in \{x \in \mathbb{Z} : x \geq 2\}, S_k &= 6S_{k-1} - 5S_{k-2}\end{aligned}$$

Prove  $\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, S_n = 5^n - 1$ :

Let  $G = \{x \in \mathbb{Z} : x \geq 0\}$

Basic step:

$$\begin{aligned}S_0 &= 5^0 - 1 = 1 - 1 = 0 \\S_1 &= 5^1 - 1 = 5 - 1 = 4\end{aligned}$$

Inductive step:

$$\begin{aligned}&\text{Suppose } \forall k \in G, S_k = 5^k - 1 \\ \implies S_{k+1} &= 6S_k - 5S_{k-1} = 6(5^k - 1) - 5(5^{k-1} - 1) = 6(5^k) - 6 + 5(5^{k-1}) + 5 \\ &= 6(5^k) - (5^{k-1+1}) - 1 = (6 - 1)5^k - 1 = 5 \cdot 5^k - 1 = 5^{k+1} - 1 \\ \therefore S_{k+1} &= 6S_k - 5S_{k-1}\end{aligned}$$

$$\therefore \forall n \in \{x \in \mathbb{Z} : x \geq 0\}, S_n = 5^n - 1$$

## Well-Ordering Principle for the Integers

**Definition** Let  $S$  be a **non-empty** set of **integers**. If all elements in  $S$  are greater than some fixed integers, then  $S$  has a **least element**. For the well-ordering principle to work:

- The set must be integers.
- The set must be non-empty.
- The set must be greater than some fixed integers.



## 5.5 Skipped

## 5.6 Solving Recurrence relations by Iteration

---

**Method** Starting from the initial conditions, calculate the successive terms of sequences from the recurrence formula until a pattern emerges. Then, use the pattern to find a closed form for the sequence.

**Example**

$$a_n = \begin{cases} 1, & n = 0 \\ a_{n-1} + 2, & \forall n \in \mathbb{Z}^+ \end{cases}$$

Solve the recurrence relation.

$$\begin{aligned} \forall n \in \mathbb{Z}^+, a_k &= a_{k-1} + 2 \\ a_n &= (a_{n-1} + 2) + 2 \\ a_n &= (a_{n-2} + 2) + 2(2) \\ &\dots \\ a_n &= a_{n-k} + k(2) \\ \therefore \forall n \in \mathbb{Z}^+, a_n &= a_0 + 2n \\ \therefore \forall n \in \mathbb{Z}^+, a_n &= 1 + 2n \end{aligned}$$

### Arithmetic Sequence

**Definition** A sequence is arithmetic if there is a constant  $d$  such that:

$$\forall k \in \mathbb{Z}^+, a_k = a_{k-1} + d$$

**General Formula**

$$\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, a_n = a_0 + nd$$

### Geometric Sequence

**Definition** A sequence is geometric if there is a constant  $r$  such that:

$$\forall k \in \mathbb{Z}^+, a_k = a_{k-1}r$$

### General Formula

$$\forall n \in \{x \in \mathbb{Z} : x \geq 0\}, \quad a_n = a_0 r^n$$

**Example** Use iteration to find the explicit formula of the following sequence:

$$e_k = \begin{cases} 2, & k = 0 \\ 4e_{k-1} + 5, & k \geq 1 \end{cases}$$

$$e_0 = 2$$

$$e_1 = 4(2) + 5$$

$$e_2 = 4(4(2) + 5) + 5 = 4^2(2) + 4(5) + 5$$

$$e_3 = 4(4^2(2) + 4(5) + 5) + 5 = 4^3(2) + 4^2(5) + 4(5) + 5$$

...

$$e_k = 4^k(2) + 4^{k-1}(5) + 4^{k-2}(5) + \cdots + 4(5) + 5$$

$$= 4^k(2) + 5 \sum_{i=0}^{k-1} 4^i = 4^k(2) + 5 \left( \frac{4^{k-1+1} - 1}{4 - 1} \right)$$

$$e_k = 4^k(2) + 5 \left( \frac{4^k - 1}{3} \right)$$