CSE 191
Introduction to Discrete Structures

Dr. Eric Mikida
epmikida@buffalo.edu
208 Capen Hall

Functions and Relations
Outline

- Binary Relations
  - Intro
  - Partial Ordering
  - Equivalence Relations
- Functions
Binary Relations

A binary relation is a formal way to relate two objects, for example:

- **Student** $s$ is related to a course $c$ iff student $s$ is enrolled in course $c$
  - Defines a relation between students at UB and course at UB
- **Topic** $t$ is related to topic $s$ iff you need to learn $s$ before you learn $t$
  - Reading a chapter $t$ in the textbook related to $s$ requires reading $s$ first
- $x$ and $y$ are related iff they share a common divisor
A **binary relation** between two sets $A$ and $B$ is any set $R \subseteq A \times B$

A binary relation **from $A$ to $B$** is a set $R$ of ordered pairs, where the first element of each ordered pair comes from $A$ and the second from $B$

- For any $a \in A$ and $b \in B$ we say that $a$ is related to $b$ iff $(a,b) \in R$
- Denoted by $a R b$

**Note:** a relation is a binary predicate $R(a,b)$: "$a$ is related to $b$"
Example

Consider the set of student, \( S = \{ \text{Alice, Bob, Carol, Don} \} \), and the set of courses, \( C = \{ \text{CSE115, CSE116, CSE191} \} \)

Alice, Bob, and Carol are enrolled in CSE115

Don is enrolled in CSE116

Alice and Don are enrolled in CSE191
Example

Consider the set of students, \( S = \{ \text{Alice, Bob, Carol, Don} \} \), and the set of courses, \( C = \{ \text{CSE115, CSE116, CSE191} \} \).

Alice, Bob, and Carol are enrolled in CSE115.

Don is enrolled in CSE116.

Alice and Don are enrolled in CSE191.
Example

Consider the set of students, $S = \{ \text{Alice, Bob, Carol, Don} \}$, and the set of courses, $C = \{ \text{CSE115, CSE116, CSE191} \}$.

- Alice, Bob, and Carol are enrolled in CSE115.
- Don is enrolled in CSE116.
- Alice and Don are enrolled in CSE191.
Example

Consider the set of students, \( S = \{ \text{Alice, Bob, Carol, Don} \} \), and the set of courses, \( C = \{ \text{CSE115, CSE116, CSE191} \} \).

- Alice, Bob, and Carol are enrolled in CSE115.
- Don is enrolled in CSE116.
- Alice and Don are enrolled in CSE191.
Example

Consider the set of students, $S = \{ \text{Alice, Bob, Carol, Don} \}$, and the set of courses, $C = \{ \text{CSE115, CSE116, CSE191} \}$.

Alice, Bob, and Carol are enrolled in CSE115.

Don is enrolled in CSE116.

Alice and Don are enrolled in CSE191.
Consider the set of student, \( S = \{ \text{Alice, Bob, Carol, Don} \} \), and the set of courses, \( C = \{ \text{CSE115, CSE116, CSE191} \} \)

- Alice, Bob, and Carol are enrolled in CSE115
- Don is enrolled in CSE116
- Alice and Don are enrolled in CSE191

This is called an arrow diagram. It is a visual representation of a binary relation.
Example

Consider the set of students, \( S = \{ \text{Alice, Bob, Carol, Don} \} \), and the set of courses, \( C = \{ \text{CSE115, CSE116, CSE191} \} \).

Given the arrow diagram, we have the binary relation \( E \):

\[ E = \{(\text{Alice, CSE115}), (\text{Alice, CSE191}), (\text{Bob, CSE115}), (\text{Carol, CSE115}), (\text{Don, CSE116}), (\text{Don, CSE191})\} \]
Consider the set of students, $S = \{ \text{Alice, Bob, Carol, Don} \}$, and the set of courses, $C = \{ \text{CSE115, CSE116, CSE191} \}$.

We can also use **matrix representation** to describe $E$:

<table>
<thead>
<tr>
<th></th>
<th>CSE115</th>
<th>CSE116</th>
<th>CSE191</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Bob</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Don</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Consider the set of students, $S = \{ \text{Alice, Bob, Carol, Don} \}$, and the set of courses, $C = \{ \text{CSE115, CSE116, CSE191} \}$.

We can also use matrix representation to describe $E$:

\[
\begin{array}{ccc}
\text{Alice} & \text{Bob} & \text{Carol} & \text{Don} \\
\text{CSE115} & 1 & 1 & 0 \\
\text{CSE116} & 0 & 0 & 1 \\
\text{CSE191} & 1 & 0 & 0 \\
\end{array}
\]

Rows represent the first set, columns represent the second set. An entry is a 1 if the row and column are related, 0 otherwise.
Binary Relations over Infinite Sets

Consider the relation $L_1$ between $\mathbb{R}$ and $\mathbb{Z}$ to be: $x L_1 y$ iff $x + y \leq 1$

1. Is 5 related to 7?
2. Is 1 related to 0?
3. Which $x$ satisfy $10 L_1 x$?
4. Which $x$ satisfy $x L_1 7$?
Consider the relation $L_1$ between $\mathbb{R}$ and $\mathbb{Z}$ to be: $x L_1 y$ iff $x + y \leq 1$

1. Is 5 related to 7? \hspace{1cm} \textbf{No.} $5 \not\!L_1 7$, because $5 + 7 > 1$

2. Is 1 related to 0? 

3. Which $x$ satisfy $10 L_1 x$?

4. Which $x$ satisfy $x L_1 7$?
Binary Relations over Infinite Sets

Consider the relation $L_1$ between $\mathbb{R}$ and $\mathbb{Z}$ to be: $x L_1 y$ iff $x + y \leq 1$

1. Is 5 related to 7? No. $5 \not L_1 7$, because $5 + 7 > 1$
2. Is 1 related to 0? Yes. $1 L_1 0$, because $1 + 0 \leq 1$
3. Which $x$ satisfy $10 L_1 x$?
4. Which $x$ satisfy $x L_1 7$?
Consider the relation $L_1$ between $\mathbb{R}$ and $\mathbb{Z}$ to be: $x L_1 y$ iff $x + y \leq 1$

1. Is 5 related to 7? No. $5 \not L_1 7$, because $5 + 7 > 1$
2. Is 1 related to 0? Yes. $1 L_1 0$, because $1 + 0 \leq 1$
3. Which $x$ satisfy $10 L_1 x$? All $x \in \mathbb{Z}$ where $x \leq -9$
4. Which $x$ satisfy $x L_1 7$?
Consider the relation $L_1$ between $\mathbb{R}$ and $\mathbb{Z}$ to be: $x L_1 y$ iff $x + y \leq 1$

1. Is 5 related to 7? No. $5 \not L_1 7$, because $5 + 7 > 1$
2. Is 1 related to 0? Yes. $1 L_1 0$, because $1 + 0 \leq 1$
3. Which $x$ satisfy $10 L_1 x$? All $x \in \mathbb{Z}$ where $x \leq -9$
4. Which $x$ satisfy $x L_1 7$? All $x \in \mathbb{R}$ where $x \leq -6$
Binary Relations on a Set

The binary relation $R$ on a set $A$ is a subset of $A \times A$.

The set $A$ is called the domain of the binary relation.
Example

We can define the relation $R_1$ on the set of real numbers such that:

$$a R_1 b \text{ iff } a > b$$

1. Is 2 related to 3?
2. Is 5 related to 3?
3. For what values of $x$ is $x^2$ related to $2x$?
4. For what values of $x$ is $x$ related to $x$?
Example

We can define the relation $R_1$ on the set of real numbers such that:

$$a R_1 b \text{ iff } a > b$$

1. Is 2 related to 3?  
   No.
2. Is 5 related to 3?  
   Yes.
3. For what values of $x$ is $x^2$ related to $2x$?  
   $x^2 > 2x$ when $x > 2$
4. For what values of $x$ is $x$ related to $x$?  
   None
Special Properties of Binary Relations

For any binary relation, we can consider the following questions:

- Are all elements related to themselves?
- Does the relation hold in both directions?
- Does the relation only hold in one direction?
- If there is a chain of relations, does the relation also hold directly?
Special Properties of Binary Relations

For any binary relation, we can consider the following questions:

- Are all elements related to themselves?  **Reflexive**
- Does the relation hold in both directions?  **Symmetric**
- Does the relation only hold in one direction?  **Anti-Symmetric**
- If there is a chain of relations, does the relation also hold directly?  **Transitive**
A relation $R$ on set $A$ is called **reflexive** if every $a \in A$ is related to itself. Formally, $a R a$ for all $a \in A$.

**Example:** Consider the $\leq$ relation on $\mathbb{Z}$.
Special Properties of Binary Relations

A relation $R$ on set $A$ is called **symmetric** if for every $a R b$, we also have that $b R a$.

**Example:** Consider the $=$ relation on $\mathbb{Z}$

A relation $R$ on set $A$ is called **anti-symmetric** if for all $a, b \in A$: $a R b$ and $b R a$ implies that $a = b$.

**Example:** Consider the $\leq$ relation on $\mathbb{Z}$
A relation $R$ on set $A$ is called **transitive** if for all $a, b, c \in A$: $a R b$ and $b R c$ implies $a R c$.

**Example:** Consider the $<$ relation on $\mathbb{Z}$
Consider the following relations on the set \{1,2,3\}

\[ R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,3)\} \]

\[ R_2 = \{(1,1), (1,3), (2,2), (3,1)\} \]

\[ R_3 = \{(2,3)\} \]

\[ R_4 = \{(1,1), (1,3)\} \]

What are the special properties of each relation?
Exercise

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,3)\}$

Reflexive?
Symmetric?
Anti-Symmetric?
Transitive?
Exercise

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,3)\}$

- Reflexive? Yes.
- Symmetric? No... 3 $R_1 1$ but 1 $\not R_1 3$
- Anti-Symmetric? No... 2 $R_1 1$ and 1 $R_1 2$ but 1 $\neq$ 2
- Transitive? No... 3 $R_1 1$ and 1 $R_1 2$ but 3 $\not R_1 2$
Exercise

\( R_2 = \{(1,1), (1,3), (2,2), (3,1)\} \)

Reflexive?  
Symmetric?  
Anti-Symmetric?  
Transitive?
Exercise

\[ R_2 = \{(1,1), (1,3), (2,2), (3,1)\} \]

Reflexive? **No**...\(3 \not R_2 3\)

Symmetric? **Yes**. \(x R_2 y \rightarrow y R_2 x\)

Anti-Symmetric? **No**...\(1 R_2 3\) and \(3 R_2 1\) but \(1 \neq 3\)

Transitive? **No**. \(3 R_2 1\) and \(1 R_2 3\) but \(3 \not R_2 3\)
Exercise

$R_3 = \{(2,3)\}$

Reflexive?
Symmetric?
Anti-Symmetric?
Transitive?
Exercise

\( R_3 = \{(2,3)\} \)

Reflexive? No.

Symmetric? No.

Anti-Symmetric? Yes.

Transitive? Yes. Can't pick \(a, b, c\) s.t. \(a R_3 b\) and \(b R_3 c\)
Exercise

\[ R_4 = \{(1,1), (1,3)\} \]

Reflexive?
Symmetric?
Anti-Symmetric?
Transitive?
Exercise

\[ R_4 = \{(1,1), (1,3)\} \]

Reflexive? **No.**

Symmetric? **No.**

Anti-Symmetric? **Yes.**

Transitive? **Yes.** \( 1 R_4 1 \) and \( 1 R_4 3 \) \( \rightarrow \) \( 1 R_4 3 \)
Outline

- Binary Relations
  - Intro
  - Partial Ordering
    - Equivalence Relations
- Functions
A relation $R$ on a set $A$ is called a \textbf{partial order} if it is reflexive, transitive, and antisymmetric.

$a R b$ is denoted $a \leq b$ for partial ordering $R$

- We read $a \leq b$ as "$a$ is at most $b$" or "$a$ precedes $b$"
- A domain, $A$, with a partial ordering $\leq$ can be treated as the object $(A, \leq)$
  - $(A, \leq)$ is called a \textbf{partially ordered set} or \textbf{poset}
Partial Ordering Example

Consider the relation $R$ on the set $\mathbb{Z}$, where:

$x R y$ if and only if $x \leq y$

Is $(\mathbb{Z}, R)$ a poset?
Partial Ordering Example

Consider the relation $R$ on the set $\mathbb{Z}$, where:

$x R y$ if and only if $x \leq y$

Is $(\mathbb{Z}, R)$ a poset? Yes.

$R$ is reflexive ($x \leq x$ for all $x \in \mathbb{Z}$), $R$ is antisymmetric ($x \leq y$ and $y \leq x \rightarrow x = y$) and $R$ is transitive ($x \leq y$ and $y \leq z \rightarrow x \leq z$)
Elements $x$ and $y$ are **comparable** if $x \leq y$ or $y \leq x$ (or both)

A partial order is a **total order** if every pair of elements in the domain are comparable.

In our previous example, $(\mathbb{Z}, R)$ is a total order

- It is a partial order, and for every $x, y \in \mathbb{Z}$, $x R y$ or $y R x$
- We say that $R$ is a total ordering of $\mathbb{Z}$
What does it look like when elements cannot be compared?

Let the operator \( \preceq \) be \( \subseteq \), where \( A \preceq B \) iff \( A \subseteq B \), and let \( S = \mathcal{P}\{a,b,c\} \)

We have no way to compare \( \{a,b\} \) and \( \{b,c\} \)

\[ \{a,b\} \not\preceq \{b,c\} \]
\[ \{b,c\} \not\preceq \{a,b\} \]
\[ \text{Therefore, } \{a,b\} \text{ and } \{b,c\} \text{ are incomparable} \]

Is \( (S, \preceq) \) a partial ordering of \( S \)?

Is \( (S, \preceq) \) a partial ordering of \( S \)?
Partial vs Total Ordering

What does it look like when elements cannot be compared?

Let the operator \(\preceq\) be \(\subseteq\), where \(A \preceq B\) iff \(A \subseteq B\), and let \(S = \mathcal{P}\{a,b,c\}\).

We have no way to compare \(\{a,b\}\) and \(\{b,c\}\):  
- \(\{a,b\} \not\preceq \{b,c\}\)  
- \(\{b,c\} \not\preceq \{a,b\}\)  
- Therefore, \(\{a,b\}\) and \(\{b,c\}\) are incomparable

Is \((S, \preceq)\) a partial ordering of \(S\)? Yes. \(\preceq\) is reflexive, anti-symmetric, transitive

Is \((S, \preceq)\) a partial ordering of \(S\)? No. There exist incomparable elements of \(S\).
Given a poset, we can draw a **Hasse Diagram** to visualize the relation:

- If $x \leq y$, then $x$ appears lower in the drawing than $y$.
- There is a line from $x$ to $y$ iff $x \leq y$ or $y \leq x$.
- Omit line between $x$ and $z$ if $x \leq z$ but $\exists y$ s.t. $x \leq y \leq z$.

Consider $(S, \subseteq)$ where $S = \mathcal{P}\{a,b,c\}$.
Another Example

Consider the set $H$

$$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$$
Consider the set $H$

$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$

I could organize these movies in a tier list based on my preferences:

**A-tier:** Halloween, Get Out, Friday the 13th

**B-tier:** It, Descent, Chucky

**C-tier:** Hereditary
Another Example

Consider the set $H$

$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$

I could organize these movies in a tier list based on my preferences:

**A-tier:** Halloween, Get Out, Friday the 13th

**B-tier:** It, Descent, Chucky

**C-tier:** Hereditary

Is this a partial or total ordering?
Is (Hereditary, Chucky) in the relation?
Is (Hereditary, Halloween)?
Is (Halloween, Get Out)?
Another Example

Consider the set $H$

$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$

I could organize these movies in a tier list based on my preferences:

**A-tier:** Halloween, Get Out, Friday the 13th

**B-tier:** It, Descent, Chucky

**C-tier:** Hereditary

Is this a partial or total ordering? partial

Is (Hereditary, Chucky) in the relation? Yes

Is (Hereditary, Halloween)? Yes (transitivity)

Is (Halloween, Get Out)? No (incomparable)
Another Example

Consider the set $H$

$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$
Another Example

Consider the set $H$

$$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$$

I could also rank these movies based on my preferences:

1. Halloween
2. Get Out
3. Friday the 13th
4. Descent
5. It
6. Chucky
7. Hereditary

Is this a partial or total ordering?
Is (Hereditary, Chucky) in the relation?
Is (Hereditary, Halloween)?
Is (Halloween, Get Out)?
Another Example

Consider the set $H$

$H = \{ \text{Halloween, It, Hereditary, Get Out, Descent, Chucky, Friday the 13th} \}$

I could also rank these movies based on my preferences:

1. Halloween
2. Get Out
3. Friday the 13th
4. Descent
5. It
6. Chucky
7. Hereditary

Is this a partial or total ordering? total

Is (Hereditary, Chucky) in the relation? Yes

Is (Hereditary, Halloween)? Yes (transitivity)

Is (Halloween, Get Out)? No
Outline

- Binary Relations
  - Intro
  - Partial Ordering
  - Equivalence Relations
- Functions
A relation $R$ on a set $A$ is called an **equivalence relation** if it is reflexive, transitive, and symmetric.

$a R b$ is denoted $a \sim b$ for an equivalence relation $R$.

- We read $a \sim b$ as "$a$ is equivalent to $b$"
Example

Consider the relation $R$ on $P = \{ \text{all people} \}$, where $a R b$ iff $a$ and $b$ have the same birthday.

Is $R$ an equivalence relation?
Example

Consider the relation $R$ on $P = \{ \text{all people} \}$, where $a R b$ iff $a$ and $b$ have the same birthday.

Is $R$ an equivalence relation? Yes.

Reflexive: Any person, $a$, has the same birthday as themselves.

Transitive: If person $a$ and $b$ have the same birthday, and $b$ and $c$ have the same birthday, then $a$ and $c$ also have the same birthday.

Symmetric: If $a R b$, then $b R a$. 
We can partition the domain of an equivalence relation into equivalent elements. These partitions are called **equivalence classes**.

If $e \in D$ then the equivalence class containing $e$ is denoted $[e]$

$[e] = \{ x \mid x \in D, x \sim e \}$
Examples

Consider the birthday equivalence relation from the previous example, $R$

Suppose Alice's birthday is March 12

- If Alice $R$ Bob, then Bob's birthday is also March 12
- Under the relation $R$ Alice and Bob are equivalent (Alice $\sim$ Bob)
- $[\text{Alice}] = \{ \text{Alice, Bob, ...} \} = \{ \text{all people born on March 12} \}$
- $[\text{Alice}] = [\text{Bob}]$ since both represent people born on March 12
Examples

Consider the birthday equivalence relation from the previous example, $R$

Suppose Alice's birthday is March 12

- If Alice $R$ Bob, then Bob's birthday is also March 12
- Under the relation $R$ Alice and Bob are equivalent (Alice $\sim$ Bob)
- $[\text{Alice}] = \{ \text{Alice, Bob, ...} \} = \{ \text{all people born on March 12} \}$
- $[\text{Alice}] = [\text{Bob}]$ since both represent people born on March 12

Do the equivalence classes form a partition of the domain?
Consider the birthday equivalence relation from the previous example, $R$

Suppose Alice's birthday is March 12

- If Alice $R$ Bob, then Bob's birthday is also March 12
- Under the relation $R$ Alice and Bob are equivalent (Alice $\sim$ Bob)
- $[\text{Alice}] = \{ \text{Alice, Bob, ...} \} = \{ \text{all people born on March 12} \}$
- $[\text{Alice}] = [\text{Bob}]$ since both represent people born on March 12

Do the equivalence classes form a partition of the domain? Yes
Outline

- Binary Relations
- **Functions**
  - Introduction to Functions
  - Function Equality
  - Function Properties
  - Floor/Ceiling Functions
  - Division of Modular Arithmetic
  - Composition of Functions
Function Definition

Consider a relation of students to letter grades:

- Alice ➔ A
- Bob ➔ B
- Carly ➔ C
- Devon ➔ D
- Eustace ➔ E

We may want to be able to input a student's name and get their grade.
(A function is a different take on binary relations)
Let $A$ and $B$ be nonempty sets. A function, $f$, from $A$ to $B$ is an assignment of exactly one element of $B$ to each element of $A$.

Denoted by $f: A \rightarrow B$

We write $f(a) = b$ if $b$ is the unique element of $B$ assigned by $f$ to the element $a$ of $A$.

The set $A$ is the **domain** of $f$.

The set $B$ is the **codomain** of $f$. 
Function Examples

Consider the sets $X_1 = \{1, 2, 3\}$, $Y_1 = \{1, 2, 3\}$, and the mapping $f_1: X_1 \rightarrow Y_1$:

$$f_1(x) = x$$

1. Is $f_1$ a function?
2. What is the domain of $f_1$?
3. What is the codomain of $f_1$?
Function Examples

Consider the sets $X_1 = \{1, 2, 3\}$, $Y_1 = \{1, 2, 3\}$, and the mapping $f_1 : X_1 \rightarrow Y_1$:

$$f_1(x) = x$$

1. Is $f_1$ a function? **Yes.** Every element in $X_1$ maps to a unique elem of $Y_1$
2. What is the domain of $f_1$?
3. What is the codomain of $f_1$?
Consider the sets $X_1 = \{1, 2, 3\}$, $Y_1 = \{1, 2, 3\}$, and the mapping $f_1 : X_1 \rightarrow Y_1$:

$$f_1(x) = x$$

1. Is $f_1$ a function? Yes. Every element in $X_1$ maps to a unique elem of $Y_1$
2. What is the domain of $f_1$? $X_1$
3. What is the codomain of $f_1$?
Consider the sets $X_1 = \{1, 2, 3\}$, $Y_1 = \{1, 2, 3\}$, and the mapping $f_1 : X_1 \rightarrow Y_1$:

$$f_1(x) = x$$

1. Is $f_1$ a function? **Yes.** Every element in $X_1$ maps to a unique elem of $Y_1$
2. What is the domain of $f_1$? $X_1$
3. What is the codomain of $f_1$? $Y_1$
Consider the sets $X_1 = \{1, 2, 3\}$, $Y_1 = \{1, 2, 3\}$, and the mapping $f_1 : X_1 \to Y_1$:

$$f_1(x) = x$$

1. Is $f_1$ a function? **Yes.** Every element in $X_1$ maps to a unique elem of $Y_1$
2. What is the domain of $f_1$? $X_1$
3. What is the codomain of $f_1$? $Y_1$

We can also write $f_1 = \{(1,1), (2,2), (3,3)\}$
Consider the sets $X_2 = \mathbb{Z}$, $Y_2 = \{1, 2, 3\}$, and the mapping $f_2: X_2 \rightarrow Y_2$:

$$f_2(x) = x$$

1. Is $f_2$ a function?
Consider the sets $X_2 = \mathbb{Z}$, $Y_2 = \{1, 2, 3\}$, and the mapping $f_2 : X_2 \to Y_2$:

$$f_2(x) = x$$

1. Is $f_2$ a function? **No.** Problem: $f_2(4) = ???$
Function Examples

Consider the sets $X_2 = \mathbb{Z}$, $Y_2 = \{1, 2, 3\}$, and the mapping $f_2: X_2 \rightarrow Y_2$:

$$f_2(x) = x$$

1. Is $f_2$ a function? **No.** Problem: $f_2(4) = ???$

We could fix this by defining a new mapping:

$$f'_2(x) = \begin{cases} 
  x & \text{if } 1 \leq x \leq 3 \\
  1 & \text{if } x < 1 \text{ or } x > 3 
\end{cases}$$
Consider the sets $X_2 = \mathbb{Z}$, $Y_2 = \{1, 2, 3\}$, and the mapping $f_2 : X_2 \rightarrow Y_2$:

$$f_2(x) = x$$

1. Is $f_2$ a function? **No.** Problem: $f_2(4) = \text{??}$

We could fix this by defining a new mapping:

$$f'_2(x) = \begin{cases} 
  x & \text{if } 1 \leq x \leq 3 \\
  1 & \text{if } x < 1 \text{ or } x > 3
\end{cases}$$

$$f'_2 = \{(1,1), (2,2), (3,3) \cup \{(x, 1) \mid x \in \mathbb{Z}, x < 1 \text{ or } x > 3\}$$
Consider the sets $X_3 = \mathbb{Z}$, $Y_3 = \mathbb{Z}$, and the mapping $f_3 : X_3 \rightarrow Y_3$:

$$f_3(x) = \begin{cases} 
  x & \text{if } x \text{ is odd} \\
  x^2 & \text{if } x \geq 0 \\
  |x| & \text{if } x < 0 
\end{cases}$$

Is $f_3$ a function?
Consider the sets $X_3 = \mathbb{Z}$, $Y_3 = \mathbb{Z}$, and the mapping $f_3 : X_3 \rightarrow Y_3$:

$$f_3(x) = \begin{cases} 
  x & \text{if } x \text{ is odd} \\
  x^2 & \text{if } x \geq 0 \\
  |x| & \text{if } x < 0 
\end{cases}$$

Is $f_3$ a function? No. Problem: $f_3(-1) = -1$ and $f_3(-1) = 1$
Symbolically, for a mapping \( f: X \rightarrow Y \):

\( f \) is a (well-defined) function if and only if

\[
\forall x \in X, \exists y \in Y, (f(x) = y \land (\forall z \in Y, (y \neq z \rightarrow f(x) \neq z)))
\]
Function Definition in Symbols

Symbolically, for a mapping \( f: X \rightarrow Y \):

\( f \) is a (well-defined) function if and only if

\[
\forall x \in X, \exists y \in Y, (f(x) = y \land (\forall z \in Y, (y \neq z \rightarrow f(x) \neq z)))
\]

For every \( x \) in the domain, there exists a \( y \) in the codomain such that \( f(x) = y \)
Symbolically, for a mapping $f: X \rightarrow Y$:

$f$ is a (well-defined) function if and only if

$$\forall x \in X, \exists y \in Y, (f(x) = y \land (\forall z \in Y, (y \neq z \rightarrow f(x) \neq z)))$$

For every $x$ in the domain, there exists a $y$ in the codomain such that $f(x) = y$

For every other element of the codomain, $z$, $f(x) \neq z$. 
If \( f \) is a function from \( A \) to \( B \), the set \( \text{range}(f) = \{ y \mid \exists x \in A, f(x) = y \} \) is called the \textbf{range} of \( f \). It is the set of all values in the codomain that have an element from the domain mapped to it.

- For any function \( f: A \rightarrow B \), \( \text{range}(f) \subseteq B \)
- It does not have to be the whole codomain
More Examples

\[ X_4 = \mathbb{Z}, \ Y_4 = \mathbb{Z} \]

Is \( f_4 \) a function?

\[ f_4(x): X_4 \rightarrow Y_4 \]

Domain?

\[ f_4(x) = 1 \]

Codomain?

Range?
More Examples

\[ X_4 = \mathbb{Z}, \ Y_4 = \mathbb{Z} \]

Is \( f_4 \) a function? \textbf{Yes}

\( f_4(x): X_4 \rightarrow Y_4 \)

Domain?

\( f_4(x) = 1 \)

Codomain?

Range?
More Examples

\[ X_4 = \mathbb{Z}, \ Y_4 = \mathbb{Z} \]

Is \( f_4 \) a function? Yes

\[ f_4(x): X_4 \rightarrow Y_4 \]

Domain? \( \mathbb{Z} \)

Codomain?

Range?
More Examples

\[ X_4 = \mathbb{Z}, \ Y_4 = \mathbb{Z} \quad \text{Is } f_4 \text{ a function? Yes} \]

\[ f_4(x): X_4 \rightarrow Y_4 \quad \text{Domain? } \mathbb{Z} \]

\[ f_4(x) = 1 \quad \text{Codomain? } \mathbb{Z} \]

\[ \text{Range?} \]
More Examples

$X_4 = \mathbb{Z}, \ Y_4 = \mathbb{Z}$

Is $f_4$ a function? **Yes**

$f_4(x) : X_4 \to Y_4$

Domain? $\mathbb{Z}$

$f_4(x) = 1$

Codomain? $\mathbb{Z}$

Range? $\{1\}$
More Examples

\( X_5 = \mathbb{Z}, \ Y_5 = \mathbb{Z} \)

Is \( f_5 \) a function?

\( f_5(x): X_5 \to Y_5 \)

Domain?

\( f_5(x) = \sqrt{x} \)

Codomain?

Range?
More Examples

\[ X_5 = \mathbb{Z}, \ Y_5 = \mathbb{Z} \]

Is \( f_5 \) a function? \textbf{No}

\( f_5(x) : X_5 \rightarrow Y_5 \)

Domain? \textbf{N/A}

\( f_5(x) = \sqrt{x} \)

Codomain? \textbf{N/A}

Range? \textbf{N/A}
More Examples

\[ X_6 = \{ x^2 \mid x \in \mathbb{Z} \} \]

Is \( f_6 \) a function?

\[ Y_6 = \mathbb{Z} \]

Domain?

\[ f_6(x) : X_6 \rightarrow Y_6 \]

Codomain?

\[ f_6(x) = \sqrt{x^2} \]

Range?
More Examples

\[ X_6 = \{ x^2 \mid x \in \mathbb{Z} \} \]

Is \( f_6 \) a function? **Yes**

\[ Y_6 = \mathbb{Z} \]

Domain?

\[ f_6(x): X_6 \rightarrow Y_6 \]

Codomain?

\[ f_6(x) = \sqrt{x} \]

Range?
More Examples

\(X_6 = \{ x^2 | x \in \mathbb{Z} \}\)

Is \(f_6\) a function? \textbf{Yes}

\(Y_6 = \mathbb{Z}\)

Domain? \(\{ x^2 | x \in \mathbb{Z} \}\)

\(f_6(x): X_6 \rightarrow Y_6\)

Codomain?

\(f_6(x) = \sqrt{x}\)

Range?
More Examples

\[ X_6 = \{ x^2 \mid x \in \mathbb{Z} \} \]

Is \( f_6 \) a function? Yes

\[ Y_6 = \mathbb{Z} \]

Domain? \( \{ x^2 \mid x \in \mathbb{Z} \} \)

\[ f_6(x): X_6 \rightarrow Y_6 \]

Codomain? \( \mathbb{Z} \)

\[ f_6(x) = \sqrt{x} \]

Range?
More Examples

\[ X_6 = \{ x^2 \mid x \in \mathbb{Z} \} \]

Is \( f_6 \) a function?  \textbf{Yes}

\[ Y_6 = \mathbb{Z} \]

Domain?  \( \{ x^2 \mid x \in \mathbb{Z} \} \)

\[ f_6(x) : X_6 \rightarrow Y_6 \]

Codomain?  \( \mathbb{Z} \)

\[ f_6(x) = \sqrt{x} \]

Range?  \( \mathbb{Z}^+ \cup \{0\} \)
Outline

- Binary Relations
- **Functions**
  - Introduction to Functions
  - **Function Equality**
  - Function Properties
  - Floor/Ceiling Functions
  - Division of Modular Arithmetic
  - Composition of Functions
Function Equality

Two functions, $f: A \rightarrow B$ and $g: X \rightarrow Y$ are equal iff the following hold:

1. $A = X$
2. $B = Y$
3. $\forall a \in A, f(a) = g(a)$

In English, two functions are equal if they have the same domain, same codomain, and map each element in the domain to the same element of the codomain.
Consider the functions: \( f: \mathbb{Z} \rightarrow \mathbb{Z} \), and \( g: \mathbb{Z} \rightarrow \mathbb{Z} \) defined as:

\[
f = \{(x, 1) \mid x \in \mathbb{Z}\}
\]

and

\[
g(y) = 1
\]

Are the two functions equal?
Consider the functions: $f: \mathbb{Z} \to \mathbb{Z}$, and $g: \mathbb{Z} \to \mathbb{Z}$ defined as:

$$f = \{(x, 1) | x \in \mathbb{Z}\} \quad \text{and} \quad g(y) = 1$$

Are the two functions equal?

1. Same domain ✓
Function Equality

Consider the functions: \( f: \mathbb{Z} \rightarrow \mathbb{Z} \), and \( g: \mathbb{Z} \rightarrow \mathbb{Z} \) defined as:

\[
\begin{align*}
f &= \{ (x, 1) \mid x \in \mathbb{Z} \} \\
g(y) &= 1
\end{align*}
\]

Are the two functions equal?

1. Same domain ✓
2. Same codomain ✓
3. \( \forall x \in \mathbb{Z}, f(x) = g(x) \)?
Consider the functions: \( f: \mathbb{Z} \rightarrow \mathbb{Z} \), and \( g: \mathbb{Z} \rightarrow \mathbb{Z} \) defined as:

\[
f = \{(x, 1) \mid x \in \mathbb{Z}\}
\]
and

\[
g(y) = 1
\]

Are the two functions equal?

1. Same domain ✓
2. Same codomain ✓
3. \( \forall x \in \mathbb{Z}, f(x) = g(x) \)?

- Pick an arbitrary \( x \in \mathbb{Z} \)
- Then \( (x, 1) \in f \), or \( f(x) = 1 \)
- Similarly \( g(x) = 1 \)
Function Equality

Consider the functions: \( f: \mathbb{Z} \rightarrow \mathbb{Z} \), and \( g: \mathbb{Z} \rightarrow \mathbb{Z} \) defined as:

\[
f = \{(x, 1) \mid x \in \mathbb{Z}\} \quad \text{and} \quad g(y) = 1
\]

Are the two functions equal? Yes

1. Same domain ✓
2. Same codomain ✓
3. \( \forall x \in \mathbb{Z}, f(x) = g(x) \) ✓

- Pick an arbitrary \( x \in \mathbb{Z} \)
- Then \( (x, 1) \in f \), or \( f(x) = 1 \)
- Similarly \( g(x) = 1 \)
Outline

- Binary Relations
- **Functions**
  - Introduction to Functions
  - Function Equality
  - **Function Properties**
  - Floor/Ceiling Functions
  - Division of Modular Arithmetic
  - Composition of Functions
Injective Functions

A function $f: A \rightarrow B$ is **injective** if $\forall x_1, x_2 \in A, (f(x_1) = f(x_2) \rightarrow x_1 = x_2)$

Also known as **one-to-one** or **1-1**

- Each element in the domain is mapped to a unique element from the codomain (no element in the codomain is hit twice)
- To prove a function is 1-1
  - Take an arbitrary $x$ and $y$ such that $f(x) = f(y)$
  - Conclude that $x = y$
- To prove a function is not 1-1
  - Find a counterexample where $x \neq y$ but $f(x) = f(y)$
Surjective Functions

A function $f: A \rightarrow B$ is **surjective** if $\forall y \in B, \exists x \in A, f(x) = y$

Also known as **onto**

- Every element in the codomain has an element that maps to it
- To prove a function is onto:
  - Take arbitrary $y$ in the codomain
  - Find the value of $x$ in the domain such that $f(x) = y$
- To prove a function is not onto:
  - Find a counterexample, element $y$ in codomain s.t. no element maps to it
**Bijective Functions**

**Idea:** What if a function is both 1-1 and onto?
A function $f: A \to B$ is **bijective** if it is injective and surjective.

A bijective function is called a **bijection**, or a **one-to-one correspondence**.
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Injective (1-1)?
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

**Injective (1-1)?**

1. Let $x = 1$ and $y = 5$ (clearly $x$ and $y$ are both in $\mathbb{Z}$)
2. $f_1(x) = 1, f_1(y) = 1$
3. Therefore $f_1(x) = f_1(y)$, but $x \neq y$
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Injective (1-1)?

1. Let $x = 1$ and $y = 5$ (clearly $x$ and $y$ are both in $\mathbb{Z}$)
2. $f_1(x) = 1, f_1(y) = 1$
3. Therefore $f_1(x) = f_1(y)$, but $x \neq y$

We've found a counterexample, so $f_1$ is not 1-1
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Surjective (onto)?
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

**Surjective (onto)?**

1. Consider $y = 2$ (clearly 2 is in the codomain $\mathbb{Z}$)
2. There is no $x \in \mathbb{Z}$ s.t. $f_1(x) = y$
Examples

Let $f_1: \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Surjective (onto)?

1. Consider $y = 2$ (clearly 2 is in the codomain $\mathbb{Z}$)
2. There is no $x \in \mathbb{Z}$ s.t. $f_1(x) = y$

We've found a counterexample, so $f_1$ is not onto
Examples

Let $f_1 : \mathbb{Z} \to \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Bijective (one-to-one correspondence)?
Examples

Let $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_1(a) = 1$

Is $f_1$ injective, surjective, bijective?

Bijective (one-to-one correspondence)?

No. To be bijective $f_1$ must be injective AND surjective
Examples

Let \( f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+ \), defined by \( f_2(a) = |a| \) (absolute value of \( a \))

Is \( f_2 \) injective, surjective, bijective?

Injective (1-1)?
Examples

Let $f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+$, defined by $f_2(a) = |a|$ (absolute value of $a$) Is $f_2$ injective, surjective, bijective?

**Injective (1-1)?**

1. Let $x = 2$ and $y = -2$ (clearly $x$ and $y$ are both in $\mathbb{Z}$)
2. $f_1(x) = 2, f_1(y) = 2$
3. Therefore $f_1(x) = f_1(y)$, but $x \neq y$
Examples

Let $f_2: \mathbb{Z} \rightarrow \mathbb{Z}^+$, defined by $f_2(a) = |a|$ (absolute value of a)

Is $f_2$ injective, surjective, bijective?

Injective (1-1)?

1. Let $x = 2$ and $y = -2$ (clearly $x$ and $y$ are both in $\mathbb{Z}$)
2. $f_1(x) = 2, f_1(y) = 2$
3. Therefore $f_1(x) = f_1(y), \text{ but } x \neq y$

We've found a counterexample, so $f_2$ is not 1-1
Examples

Let \( f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+ \), defined by \( f_2(a) = |a| \) (absolute value of \( a \))

Is \( f_2 \) injective, surjective, bijective?

Surjective (onto)?
Examples

Let \( f_2 : \mathbb{Z} \to \mathbb{Z}^+ \), defined by \( f_2(a) = |a| \) (absolute value of a)

Is \( f_2 \) injective, surjective, bijective?

**Surjective (onto)?**

1. Let \( y \) be an arbitrary element of \( \mathbb{Z}^+ \)
2. \( f_2(y) = y \)
Examples

Let $f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+$, defined by $f_2(a) = |a|$ (absolute value of a)

Is $f_2$ injective, surjective, bijective?

**Surjective (onto)?**

1. Let $y$ be an arbitrary element of $\mathbb{Z}^+$
2. $f_2(y) = y$

Therefore, since we chose $y$ arbitrarily, every element of $\mathbb{Z}^+$ gets mapped to by something, therefore $f_2$ is onto
Examples

Let $f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+$, defined by $f_2(a) = |a|$ (absolute value of $a$)

Is $f_2$ injective, surjective, bijective?

Bijective (one-to-one correspondence)?
Examples

Let $f_2 : \mathbb{Z} \rightarrow \mathbb{Z}^+$, defined by $f_2(a) = |a|$ (absolute value of a)

Is $f_2$ injective, surjective, bijective?

Bijective (one-to-one correspondence)?

No. To be bijective $f_2$ must be injective AND surjective
Examples

Let $f_3 : \mathbb{Z} \to \mathbb{Z}$, defined by $f_3(a) = a + 16$

Is $f_3$ injective, surjective, bijective?

Injective (1-1)?
Examples

Let $f_3 : \mathbb{Z} \to \mathbb{Z}$, defined by $f_3(a) = a + 16$

Is $f_3$ injective, surjective, bijective?

**Injective (1-1)?**

1. Let $x$ and $y$ be arbitrary elements of $\mathbb{Z}$
2. Assume $f_3(x) = f_3(y)$
3. $x + 16 = y + 16 \to x = y$
Let \( f_3 : \mathbb{Z} \to \mathbb{Z} \), defined by \( f_3(a) = a + 16 \)

Is \( f_3 \) injective, surjective, bijective?

**Injective (1-1)?**

1. Let \( x \) and \( y \) be arbitrary elements of \( \mathbb{Z} \)
2. Assume \( f_3(x) = f_3(y) \)
3. \( x + 16 = y + 16 \to x = y \)

Therefore, since we chose \( x \) and \( y \) arbitrarily, and \( f_3(x) = f_3(y) \to x = y \), then \( f_3 \) is 1-1
Examples

Let $f_3: \mathbb{Z} \to \mathbb{Z}$, defined by $f_3(a) = a + 16$

Is $f_3$ injective, surjective, bijective?

Surjective (onto)?
Examples

Let $f_3 : \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $f_3(a) = a + 16$

Is $f_3$ injective, surjective, bijective?

**Surjective (onto)?**

1. Let $y$ be an arbitrary element of $\mathbb{Z}$
2. $x = y - 16$ is also therefore in $\mathbb{Z}$
3. $f_3(x) = x + 16 = (y - 16) + 16 = y$
Examples

Let \( f_3 : \mathbb{Z} \to \mathbb{Z} \), defined by \( f_3(a) = a + 16 \)

Is \( f_3 \) injective, surjective, bijective?

Surjective (onto)?

1. Let \( y \) be an arbitrary element of \( \mathbb{Z} \)
2. \( x = y - 16 \) is also therefore in \( \mathbb{Z} \)
3. \( f_3(x) = x + 16 = (y - 16) + 16 = y \)

Therefore, since we chose \( y \) arbitrarily, every element of \( \mathbb{Z} \) gets mapped to by something, therefore \( f_3 \) is onto
Examples

Let \( f_3 : \mathbb{Z} \to \mathbb{Z} \), defined by \( f_3(a) = a + 16 \)

Is \( f_3 \) injective, surjective, bijective?

**Bijective (one-to-one correspondence)?**
Examples

Let $f_3 : \mathbb{Z} \to \mathbb{Z}$, defined by $f_3(a) = a + 16$

Is $f_3$ injective, surjective, bijective?

Bijective (one-to-one correspondence)?

Yes. To be bijective $f_3$ must be injective AND surjective, and it is!
Inverse of Functions

For any function \( f: A \rightarrow B \), the \textbf{inverse mapping} of \( f \), denoted by \( f^{-1} \), is defined by the mapping \( f^{-1}: B \rightarrow A \) where:
\[
(f^{-1})(y) = x \quad \text{where} \quad (x, y) \in f
\]

If \( f \) is a \textbf{bijection} then \( f^{-1} \) is a function (otherwise it is just a mapping)
- \( f^{-1} \) maps codomain elements of \( f \) to domain elements of \( f \)
- If \( f(x) = y \) then \( f^{-1}(y) = x \)
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: exactly one arrow out of each codomain element
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:
- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: *exactly* one arrow out of each codomain element

```
  a  w
  b  x
 f   y
  c  z
```
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: exactly one arrow out of each codomain element
For $f^{-1}$ to be a function, $f$ must be a bijection:
- 1-1: guarantees at most one arrow out of each codomain element
- Onto: guarantees at least one arrow out of each codomain element
- Bijection: exactly one arrow out of each codomain element

Not a function because $z$ does not map to anything
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- 1-1: guarantees at most one arrow out of each codomain element
- Onto: guarantees at least one arrow out of each codomain element
- Bijection: **exactly** one arrow out of each codomain element
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: **exactly** one arrow out of each codomain element
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: exactly one arrow out of each codomain element

Not a function because $x$ maps to more than one thing
For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection** (exactly): exactly one arrow out of each codomain element
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- **1-1**: guarantees at most one arrow out of each codomain element
- **Onto**: guarantees at least one arrow out of each codomain element
- **Bijection**: exactly one arrow out of each codomain element

\[ f^{-1} \]

```
\begin{array}{cccc}
a & \rightarrow & w \\
\downarrow & & \downarrow \\
b & \rightarrow & x \\
\downarrow & & \downarrow \\
c & \rightarrow & y \\
\downarrow & & \downarrow \\
d & \rightarrow & z \\
\end{array}
```
Inverse of Functions

For $f^{-1}$ to be a function, $f$ must be a bijection:

- 1-1: guarantees at most one arrow out of each codomain element
- Onto: guarantees at least one arrow out of each codomain element
- Bijection: **exactly** one arrow out of each codomain element

Exactly one arrow out of every element of codomain, therefore $f^{-1}$ is a function
If $f: A \rightarrow B$ is onto:
- Then for every codomain element, there is at least one domain element
- $|A| \geq |B|$

If $f: A \rightarrow B$ is 1-1:
- For every domain element, there is a unique codomain element
- $|A| \leq |B|$

If $f: A \rightarrow B$ is a bijection, then $f$ is 1-1 and onto
- $|A| \leq |B|$ and $|A| \geq |B|$, therefore $|A| = |B|$
Cardinality of Domain vs Codomain

If \( f: A \rightarrow B \) is onto:
- Then for every codomain element, there is at least one domain element
- \( |A| \geq |B| \)

If \( f: A \rightarrow B \) is 1-1:
- For every domain element, there is a unique codomain element
- \( |A| \leq |B| \)

If \( f: A \rightarrow B \) is a bijection, then \( f \) is 1-1 and onto
- \( |A| \leq |B| \) and \( |A| \geq |B| \), therefore \( |A| = |B| \)

This will be useful for comparing the cardinality of sets!
Cardinality of \( \mathbb{N} \) and \( \mathbb{Z} \)

**Theorem:** The cardinalities of \( \mathbb{N} \) and \( \mathbb{Z} \) are the same

**Proof:** Show a bijection from \( \mathbb{N} \) to \( \mathbb{Z} \)
Cardinality of $\mathbb{N}$ and $\mathbb{Z}$

**Theorem:** The cardinalities of $\mathbb{N}$ and $\mathbb{Z}$ are the same

**Proof:** Show a bijection from $\mathbb{N}$ to $\mathbb{Z}$

Let $f: \mathbb{N} \rightarrow \mathbb{Z}$ be defined by

$$f(x) = \begin{cases} 
-i & \text{if } x = 2i \text{ (x is even)} \\
 i & \text{if } x = 2i + 1 \text{ (x is odd)} 
\end{cases}$$

Is $f$ a bijection?
Cardinality of $\mathbb{N}$ and $\mathbb{Z}$

Let $x$ and $y$ be arbitrary elements of $\mathbb{N}$

Assume $f(x) = f(y)$. Then $x$ and $y$ must both be even, or both be odd.

If even: $x = 2i$ and $y = 2i$.

If odd: $x = 2i + 1$ and $y = 2i + 1$.

Therefore, if $f(x) = f(y)$, $x = y$, which means $f$ is 1-1
Cardinality of $\mathbb{N}$ and $\mathbb{Z}$

Let $z$ be an arbitrary element of $\mathbb{Z}$

Case 1: $z < 0$

$$x = 2 \times -z$$ is an integer $> 0$, therefore $x$ is in $\mathbb{N}$ and $f(x) = z$

Case 2: $z \geq 0$

$$x = 2 \times z + 1$$ is an integer $> 0$, therefore $x$ is in $\mathbb{N}$ and $f(x) = z$

Therefore for any arbitrary $z$ in $\mathbb{Z}$, exists an $x$ in $\mathbb{N}$ s.t. $f(x) = z$. So $f$ is onto.
Cardinality of $\mathbb{N}$ and $\mathbb{Z}$

**Theorem:** The cardinalities of $\mathbb{N}$ and $\mathbb{Z}$ are the same

**Proof:** Show a bijection from $\mathbb{N}$ to $\mathbb{Z}$

Let $f: \mathbb{N} \rightarrow \mathbb{Z}$ be defined by

$$f(x) = \begin{cases} 
-i & \text{if } x = 2i \text{ (x is even)} \\
i & \text{if } x = 2i + 1 \text{ (x is odd)}
\end{cases}$$

Therefore $f$ is both 1-1 and onto. So $f$ is a bijection. Therefore $\mathbb{N}$ and $\mathbb{Z}$ have the same size.
Outline

- Binary Relations
- **Functions**
  - Introduction to Functions
  - Function Equality
  - Function Properties
- **Floor/Ceiling Functions**
  - Division of Modular Arithmetic
  - Composition of Functions
Floor Functions

The floor function is the function $\text{floor} : \mathbb{R} \rightarrow \mathbb{Z}$ defined by

$$\text{floor}(x) = \max\{ y \mid y \in \mathbb{Z}, y \leq x \}$$

Evaluates to the maximum integer below the given number.

Denoted by: $\text{floor}(x) = \lfloor x \rfloor$

Examples

$$\lfloor 4.5 \rfloor = 4 \quad \lfloor 17 \rfloor = 17$$

$$\lfloor -8.7 \rfloor = -9 \quad \lfloor \pi \rfloor = \lfloor 3.14159 \rfloor = 3$$
The ceiling function is the function floor : $\mathbb{R} \rightarrow \mathbb{Z}$ defined by

$$\text{ceiling}(x) = \min\{ y \mid y \in \mathbb{Z}, y \geq x \}$$

Evaluates to the minimum integer above the given number.

Denoted by: $\text{ceiling}(x) = \lceil x \rceil$

**Examples**

$$\lceil 4.5 \rceil = 5 \quad \text{and} \quad \lceil 17 \rceil = 17$$
$$\lceil -8.7 \rceil = -8 \quad \text{and} \quad \lceil \pi \rceil = \lceil 3.14159 \rceil = 4$$
Outline

- Binary Relations
- **Functions**
  - Introduction to Functions
  - Function Equality
  - Function Properties
  - Floor/Ceiling Functions
  - **Division and Modular Arithmetic**
  - Composition of Functions
Let $x$ and $y$ be integers. Then $x$ divides $y$ if there is an integer $k$ s.t. $y = kx$.

Denoted by $x \mid y$

- $x$ does not divide $y$ is denoted by $x \nmid y$

If $x \mid y$, then we say:

- $y$ is a multiple of $x$
- $x$ is a factor or divisor of $y$
Divides Examples

The question “\(x \mid y?\)” asks “Does \(x\) divide \(y\)?”

**Examples**

- 4 \(\mid\) 8?  **Yes!** 8 = 2 \(\cdot\) 4
- 5 \(\mid\) 15?  **Yes!** 15 = 3 \(\cdot\) 5
- 6 \(\mid\) 15?  **No!** 15 = 2 \(\cdot\) 6 + 3
**Division Algorithm**

**Theorem**

Let \( n \in \mathbb{Z} \) and let \( d \in \mathbb{Z}^+ \) Then there are unique integers \( q \) and \( r \), with \( 0 \leq r \leq d - 1 \), s.t. \( n = q \cdot d + r \).

- If \( x \mid y \) then \( r = 0 \), i.e., \( y = qx + 0 \) for some \( q \in \mathbb{Z} \)
- If \( x \nmid y \) then \( r \neq 0 \), i.e., \( y = qx + r \) for some \( q \in \mathbb{Z} \) and \( 1 \leq r \leq x - 1 \).

Even vs odd: \( 2 \mid x ? \)

\[
x = \begin{cases} 
2q + 0 & \text{if } x \text{ is even} \\
2q + 1 & \text{if } x \text{ is odd}
\end{cases}
\]
The Division Algorithm for \( n \in \mathbb{Z} \) and \( d \in \mathbb{Z}^+ \) gives unique values \( q \in \mathbb{Z} \) and \( r \in \{0, \ldots, d - 1\} \).

- The number \( q \) is called the quotient.
- The number \( r \) is called the remainder.
Integer Division Definition

The Division Algorithm for \( n \in \mathbb{Z} \) and \( d \in \mathbb{Z}^+ \) gives unique values

\[ q \in \mathbb{Z} \text{ and } r \in \{0, \ldots, d - 1\}. \]

- The number \( q \) is called the quotient.
- The number \( r \) is called the remainder.

The operations \textit{div} and \textit{mod} produce the quotient and the remainder, respectively, as a function of \( n \) and \( d \).

- \( n \div d = q \)
- \( n \mod d = r \)

In programming, \( n \% d = r \) denotes \( n \mod d = r \).
For any integer $n > 0$, $x \mod n$ can be seen as a function $\text{mod}_n(x)$:

- $\text{mod}_n : \mathbb{Z} \rightarrow \{0, 1, 2, \ldots, n - 1\}$, where $\text{mod}_n(x) = x \mod n$.

Addition $\text{mod} n$ is defined by adding two numbers and then applying $\text{mod}_n$:

- All results in the range $\{0, 1, \ldots, n - 1\}$
Addition mod $n$

For any integer $n > 0$, $x \mod n$ can be seen as a function $\mod_n(x)$:

- $\mod_n : \mathbb{Z} \rightarrow \{0, 1, 2, \ldots, n - 1\}$, where $\mod_n(x) = x \mod n$.

**Addition mod $n$** is defined by adding two numbers and then applying $\mod_n$:

- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 7$

- $\mod_7(4, 6) = \mod_7(15, 17) = \mod_7(8, 20) =$
Addition mod $n$

For any integer $n > 0$, $x \mod n$ can be seen as a function $\mod_n(x)$:
- $\mod_n : \mathbb{Z} \rightarrow \{0, 1, 2, \ldots, n - 1\}$, where $\mod_n(x) = x \mod n$.

Addition mod $n$ is defined by adding two numbers and then applying $\mod_n$.
- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 7$

$+ \mod_7(4, 6) = (4 + 6) \mod 7 = 10 \mod 7 = 3$

$+ \mod_7(15, 17) =$

$+ \mod_7(8, 20) =$
Addition mod $n$

For any integer $n > 0$, $x \mod n$ can be seen as a function $\text{mod}_n(x)$:

- $\text{mod}_n : \mathbb{Z} \rightarrow \{0, 1, 2, \ldots, n - 1\}$, where $\text{mod}_n(x) = x \mod n$.

Addition mod $n$ is defined by adding two numbers and then applying mod $n$:

- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 7$

- $\text{mod}_7(4, 6) = (4 + 6) \mod 7 = 10 \mod 7 = 3$
- $\text{mod}_7(15, 17) = (15 + 17) \mod 7 = 32 \mod 7 = 4$
- $\text{mod}_7(8, 20) =$
**Addition mod** $n$

For any integer $n > 0$, $x \mod n$ can be seen as a function $\mod_n(x)$:

- $\mod_n : \mathbb{Z} \rightarrow \{0, 1, 2, \ldots, n - 1\}$, where $\mod_n(x) = x \mod n$.

**Addition mod** $n$ is defined by adding two numbers and then applying $\mod_n$:

- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 7$

- $\mod_7(4, 6) = (4 + 6) \mod 7 = 10 \mod 7 = 3$

- $\mod_7(15, 17) = (15 + 17) \mod 7 = 32 \mod 7 = 4$

- $\mod_7(8, 20) = (8 + 20) \mod 7 = 28 \mod 7 = 0$
Multiplication $\text{mod } n$ is defined by multiplying two numbers and then applying $\text{mod } n$.

- All results in the range \{0, 1, \ldots, n - 1\}

Suppose $n = 11$.

* $\text{mod}_{11}(4, 6) =$

* $\text{mod}_{11}(5, 7) =$

* $\text{mod}_{11}(8, 23) =$
Multiplication mod $n$

Multiplication $\mod n$ is defined by multiplying two numbers and then applying $\mod n$.

- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 11$.

* $\mod_{11}(4, 6) = (4 \times 6) \mod 11 = 24 \mod 11 = 2$

* $\mod_{11}(5, 7) = \phantom{24}$

* $\mod_{11}(8, 23) = \phantom{24}$
Multiplication mod $n$

Multiplication mod $n$ is defined by multiplying two numbers and then applying mod $n$.

- All results in the range $\{0, 1, \ldots, n - 1\}$

Suppose $n = 11$.

- $\text{mod}_{11}(4, 6) = (4 \cdot 6) \mod 11 = 24 \mod 11 = 2$

- $\text{mod}_{11}(5, 7) = (5 \cdot 7) \mod 11 = 35 \mod 11 = 2$

- $\text{mod}_{11}(8, 23) =$
Multiplication mod $n$

Multiplication $\text{mod } n$ is defined by multiplying two numbers and then applying $\text{mod } n$.

- All results in the range \{0, 1, ..., $n - 1$\}

Suppose $n = 11$.

* $\text{mod}_{11}(4, 6) = (4 \times 6) \text{ mod } 11 = 24 \text{ mod } 11 = 2$

* $\text{mod}_{11}(5, 7) = (5 \times 7) \text{ mod } 11 = 35 \text{ mod } 11 = 2$

* $\text{mod}_{11}(8, 23) = (8 \times 23) \text{ mod } 11 = 184 \text{ mod } 11 = 8$
If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$ if $m$ divides $a - b$.

The notation $a \equiv b \pmod{m}$ indicates that $a$ is congruent to $b$ modulo $m$.

- $a \equiv b \pmod{m}$ is a congruence.
- Indicates that $a$ and $b$ are in the same equivalence class.

Is 17 congruent to 5 modulo 6?
Congruence Modulo

If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$ if $m$ divides $a - b$.

The notation $a \equiv b \pmod{m}$ indicates that $a$ is congruent to $b$ modulo $m$.

- $a \equiv b \pmod{m}$ is a congruence.
- Indicates that $a$ and $b$ are in the same equivalence class.

Is 17 congruent to 5 modulo 6? Yes, because 6 divides $17 - 5$. 
If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$ if $m$ divides $a - b$.

The notation $a \equiv b \ (\text{mod } m)$ indicates that $a$ is congruent to $b$ modulo $m$.

- $a \equiv b \ (\text{mod } m)$ is a congruence.
- Indicates that $a$ and $b$ are in the same equivalence class.

Is 17 congruent to 5 modulo 6? **Yes**, because 6 divides 17 - 5.

- $17 \, \text{mod} \, 6 = 5$; it is in the equivalence class for 5 in $\text{mod} \, 6$.
- $5 \, \text{mod} \, 6 = 5$; it is in the equivalence class for 5 in $\text{mod} \, 6$.
- Binary Relations
- **Functions**
  - Introduction to Functions
  - Function Equality
  - Function Properties
  - Floor/Ceiling Functions
  - Division of Modular Arithmetic
  - **Composition of Functions**
Composition of Functions

If $f$ and $g$ are two functions, where $f: X \rightarrow Y$ and $g: Y \rightarrow Z$, the composition of $g$ with $f$, denoted by $g \circ f$, is the function:

$$(g \circ f): X \rightarrow Z, \text{ s.t. for all } x \in X, (g \circ f)(x) = g(f(x))$$
Consider the functions $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^-$ and $g: \mathbb{Z} \rightarrow \{0, 1\}$ where:

$$f(x) = -x$$

$$g(x) = \begin{cases} 0 & \text{if } \left\lfloor \frac{x}{2} \right\rfloor = \frac{x}{2} \\ 1 & \text{otherwise} \end{cases}$$
Example

Consider the functions $f: \mathbb{Z}^+ \to \mathbb{Z}^-$ and $g: \mathbb{Z} \to \{0, 1\}$ where:

$$f(x) = -x$$

$$g(x) = \begin{cases} 
0 & \text{if } \frac{x}{2} = \frac{x}{2} \\
1 & \text{otherwise}
\end{cases}$$

Then we can work out that:

$$(g \circ f)(x) = g(f(x)) = g(-x) = \begin{cases} 
0 & \text{if } \frac{-x}{2} = \frac{-x}{2} \\
1 & \text{otherwise}
\end{cases}$$
Interesting Function Composition

Idea: Compose the inverse function (if it exists) with the original function
Interesting Function Composition

Idea: Compose the inverse function (if it exists) with the original function.

A function mapping an element to itself is called an identity function.

- Identity function over $A$, denoted by $I_A: A \rightarrow A$ is $I_A(a) = a$.
Interesting Function Composition

**Idea:** Compose the inverse function (if it exists) with the original function.

A function mapping an element to itself is called an **identity function**

- Identity function over $A$, denoted by $I_A : A \rightarrow A$ is $I_A(a) = a$

If $f : X \rightarrow Y$, we have $(f^{-1} \circ f) = I_X$
Interesting Function Composition

**Idea:** Compose the inverse function (if it exists) with the original function.

A function mapping an element to itself is called an **identity function**.
- Identity function over $A$, denoted by $I_A : A \to A$ is $I_A(a) = a$.

If $f: X \to Y$, we have $(f^{-1} \circ f) = I_X$.

Is $(f \circ f^{-1})$ also an identity function?
Interesting Function Composition

**Idea:** Compose the inverse function (if it exists) with the original function

A function mapping an element to itself is called an **identity function**

- Identity function over $A$, denoted by $I_A : A \rightarrow A$ is $I_A(a) = a$

If $f : X \rightarrow Y$, we have $(f^{-1} \circ f) = I_X$

Is $(f \circ f^{-1})$ also an identity function? **Yes.** $I_Y$