## Week 9 at a glance

### We will be learning and practicing to:

- Clearly and unambiguously communicate computational ideas using appropriate formalism. Translate across levels of abstraction.
  - Defining important sets of numbers, e.g. set of integers, set of rational numbers
  - Classifying sets into: finite sets, countably infinite sets, uncountable sets
  - Defining functions, predicates, and binary relations using multiple representations
  - Determining whether a given binary relation is symmetric, antisymmetric, reflexive, and/or transitive
  - Determining whether a given binary relation is an equivalence relation and/or a partial order
- Know, select and apply appropriate computing knowledge and problem-solving techniques. Reason about computation and systems. Use mathematical techniques to solve problems. Determine appropriate conceptual tools to apply to new situations. Know when tools do not apply and try different approaches. Critically analyze and evaluate candidate solutions.
  - Using the definitions of the div and mod operators on integers
  - Using divisibility and primality predicates
  - Applying the definition of congruence modulo n and modular arithmetic
- Apply proof strategies, including direct proofs and proofs by contradiction, and determine whether a proposed argument is valid or not.
  - Using proofs as knowledge discovery tools to decide whether a statement is true or false

### TODO:

Review quiz based on Week 8 class material (due Monday 03/02/2026)

Test 2 Attempt 1 in the CBTF this week at your scheduled time.

Review quiz based on Week 9 class material (due Monday 03/09/2026)

# Week 9 Monday: Cardlinality and binary relations

## Cardinality of sets: recap

The set of positive integers $\mathbb{Z}^+$ is countably infinite.

Countably infinite means "same size as $\mathbb{N}$"

The set of integers $\mathbb{Z}$ is countably infinite and is a proper superset of $\mathbb{Z}^+$. In fact, the set difference

$$\mathbb{Z} \setminus \mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x \notin \mathbb{Z}^+\} = \{x \in \mathbb{Z} \mid x \leq 0\}$$

is countably infinite.

The set of rationals $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$ is countably infinite.

The set of real numbers $\mathbb{R}$ is uncountable. In fact, the closed interval $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$, any other nonempty closed interval of real numbers whose endpoints are unequal, as well as the related intervals that exclude one or both of the endpoints are each uncountable. The set of **irrational** numbers $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$ is uncountable.

$\mathbb{R} \setminus \mathbb{Q}$ is alt notation for set difference

Claim: The set difference between an uncountable set and a countable set is uncountable.

Proof: WTS $\forall X\ \forall Y\ ((\underbrace{Y \text{ is uncountable}}_{p} \land \underbrace{X \text{ is countable}}_{q}) \to \underbrace{Y-X \text{ is uncountable}}_{u})$.

Towards universal generalization, consider arbitrary sets $X$ and $Y$.

| $p$ | $q$ | $u$ | $(p \land q) \to u$ | $(\neg u \land q) \to \neg p$ |
|---|---|---|---|---|
| T | T | T | T | T |
| T | T | F | F | F |
| T | F | T | T | T |
| T | F | F | T | T |
| F | T | T | T | T |
| F | T | F | T | T |
| F | F | T | T | T |
| F | F | F | T | T |

Lemma: $(\overset{T}{p} \land \overset{T}{q}) \to u \equiv (\neg u \land q) \to \neg p$

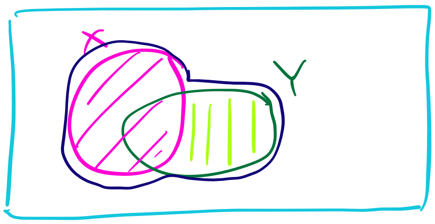
$\neg(p \land q) \lor u \equiv (\neg p \lor \neg q) \lor u \equiv \neg p \lor \neg q \lor u \equiv (u \lor \neg q) \lor \neg p \equiv \neg(\neg u \land q) \lor \neg p$

WTS $(Y$ is uncountable $\land$ $X$ is countable$) \to Y - X$ is uncountable

Equivalently, WTS $Y-X$ is countable $\land$ $X$ is countable $\to$ $\boxed{Y \text{ is countable}}$

Towards a direct proof, assume $Y-X$ is countable, $X$ is countable.

WTS $Y$ is countable.



$X \cup Y = Y-X \cup X$

$X \subseteq X \cup Y$

$Y \subseteq X \cup Y$

From last time

Lemma: The union of two countable sets is countable.

Lemma: The subset of a countable set is countable.

We can classify any set as

- **Finite size.** Fact: For each positive number $n$, for any sets $X$ and $Y$ each size $n$, there is a bijection between $X$ and $Y$.
- **Countably Infinite.** Fact: for any countably infinite sets $X$ and $Y$, there is a bijection between $X$ and $Y$.
- **Uncountable.** Examples: $\mathcal{P}(\mathbb{N})$, the power set of any infinite set, the set of real numbers, any nonempty interval of real numbers. Fact: there are (many) examples of uncountable sets that do not have a bijection between them.

~~True~~ or [✓ **False**]? For all sets $A$ and $B$ where $A \subseteq B$, if $A$ is infinite then $B$ is finite.

counterexample eg. $A = \mathbb{Z}^+$ $B = \mathbb{Z}$

need

- $A \subseteq B$
- $A$ infinite
- $B$ infinite

~~True or~~ [✓ **False**]? For all sets $A$ and $B$ where $A \subseteq B$, if $A$ is countable then $B$ is countable.

Counterexample eg. $A = \{1\}$ $B = \mathbb{R}$

need

- $A \subseteq B$
- $A$ countable
- $B$ uncountable

~~True or~~ [✓ **False**]? For all sets $A$ and $B$ where $A \subseteq B$, if $B$ is infinite then $A$ is finite.

counterexample

need

- $A \subseteq B$
- $B$ infinite
- $A$ infinite

eg. $A = \mathbb{Z}$ $B = \mathbb{Z}$

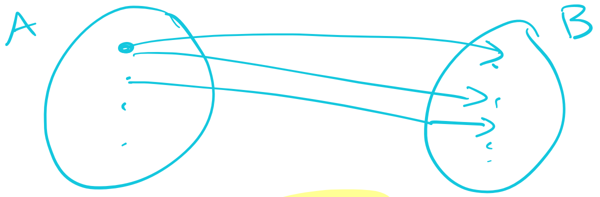
~~True~~ or [✓ **False**]? For all sets $A$ and $B$ where $A \subseteq B$, if $B$ is uncountable then $A$ is countable.

counterexample.

need

- $A \subseteq B$
- $B$ uncountable
- $A$ uncountable

$A = \overline{\mathbb{Q}}$ $\mathbb{R} = \mathbb{Q}$



## Binary relations

**Definition**: When $A$ and $B$ are sets, we say any subset of $A \times B$ is a **binary relation**. A relation $R$ can also be represented as

- A function $f_{TF} : A \times B \to \{T, F\}$ where, for $a \in A$ and $b \in B$, $f_{TF}(\ (a,b)\ ) = \begin{cases} T & \text{when } (a,b) \in R \\ F & \text{when } (a,b) \notin R \end{cases}$
- A function $f_{\mathcal{P}} : A \to \mathcal{P}(B)$ where, for $a \in A$, $f_{\mathcal{P}}(a) = \{b \in B \mid (a,b) \in R\}$

collection of elements of B to which a is related

When $A$ is a set, we say any subset of $A \times A$ is a (binary) **relation** on $A$.

ex. $A = \{1, 2, 3\}$ $R = \{ (1,1), (1,3) \}$

$f_{TF} : A \times A \to \{T, F\}$

| $(x,y)$ | $f_{TF}((x,y))$ |
|---|---|
| $(1,1)$ | T |
| $(1,2)$ | F |
| $(1,3)$ | T |
| $(2,1)$ | F |
| $(2,2)$ | F |
| $(2,3)$ | F |
| $(3,1)$ | F |
| $(3,2)$ | F |
| $(3,3)$ | F |

$f_{\mathcal{P}} : A \to \mathcal{P}(A)$

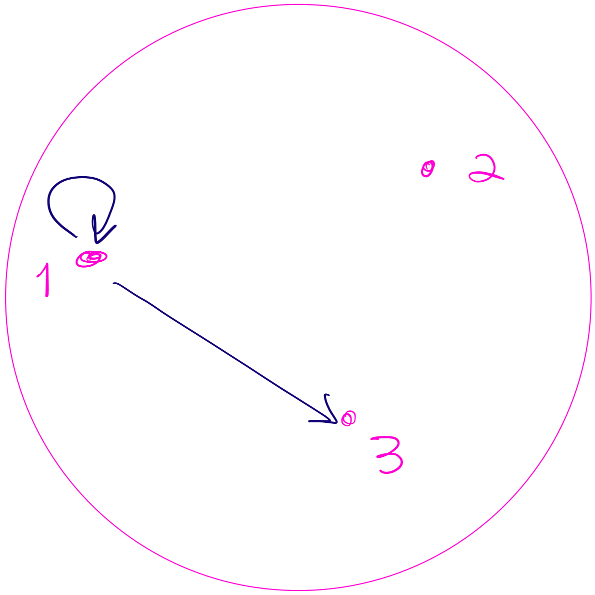
| $x$ | $f_{\mathcal{P}}(x)$ |
|---|---|
| 1 | $\{1, 3\}$ |
| 2 | $\emptyset$ |
| 3 | $\emptyset$ |

no ordered pairs in R whose first component is 2

For relation $R$ on a set $A$, we can represent this relation as a **graph**: a collection of nodes (vertices) and edges (arrows). The nodes of the graph are the elements of $A$ and there is an edge from $a$ to $b$ exactly when $(a,b) \in R$.

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

$R = \{ (1,1), (1,3) \}$



$\mathcal{P}(\mathbb{R})$ = the power set of $\mathbb{R}$ $= \{X \mid X \subseteq \mathbb{R}\}$

*Example*: For $A = \mathcal{P}(\mathbb{R})$, we can define the relation $EQ_{\mathbb{R}}$ on $A$ as

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

Example elements of $EQ_{\mathbb{R}}$ are:

$(\emptyset, \emptyset)$ , $(\mathbb{N}, \mathbb{Q})$ , $(\mathbb{Q}, \{x \in \mathbb{Q} \mid 0 \leq x \leq 1\})$,

$(\mathbb{R}, \mathbb{R})$ , $\underbrace{(\mathbb{R}, \overline{\mathbb{Q}})}_{\text{challenge}}$

Example elements of $\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})$ that are not in $EQ_{\mathbb{R}}$ are:

$(\mathbb{R}, \mathbb{N})$ , $(\{1\}, \{1, 5\})$

*Example*: Let $R_{(\mathbf{mod}\ n)}$ be the set of all pairs of integers $(a, b)$ such that $(a \ \mathbf{mod}\ n = b \ \mathbf{mod}\ n)$. Then $a$ is **congruent to** $b$ **mod** $n$ means $(a, b) \in R_{(\mathbf{mod}\ n)}$. A common notation is to write this as $a \equiv b(\mathbf{mod}\ n)$.

$R_{(\mathbf{mod}\ n)}$ is a relation on the set of integers, $\mathbb{Z}$ .

Some example elements of $R_{(\mathbf{mod}\ 4)}$ are:

$(1, 5)$ $\quad 1 = 0 \cdot 4 + 1$

$\quad 5 = 1 \cdot 4 + 1$

$(-1, 3)$ $\quad -1 = (-1) \cdot 4 + 3$

remainder is integer between 0 and n-1 (inclusive)

Functions $f$ defined by ① Domain ② Codomain ③ Rule where rule needed to satisfy $\forall x \in \text{Domain}\ \exists y \in \text{Codomain}\ (f(x) = y)$ and $\forall x \in \text{Domain}\ (\exists y_1 \in \text{Codomain}\ \exists y_2 \in \text{Codomain}\ (f(x) = y_1 \wedge f(x) = y_2 \rightarrow y_1 = y_2))$.

Such a function defines a binary relation $R_f$

$$R_f = \{(x, y) \in \text{Domain} \times \text{Codomain} \mid y = f(x)\}$$

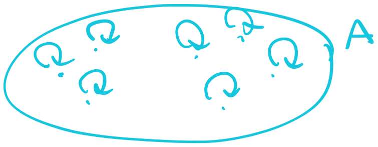
# Week 9 Wednesday: Binary relations definitions and representations

## Properties of binary relations

A relation $R$ on a set $A$ is called **reflexive** means $(a, a) \in R$ for every element $a \in A$.

*Informally*, every element is related to itself. $\forall a \in A \; ( \; (a,a) \in R )$

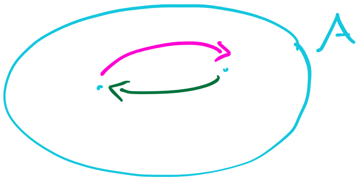
*Graphically*, there are self-loops (edge from a node back to itself) at every node.



A relation $R$ on a set $A$ is called **symmetric** means $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

*Informally*, order doesn't matter for this relation. $\forall a \in A \, \forall b \in A \; ( \; (a,b) \in R \to (b,a) \in R )$

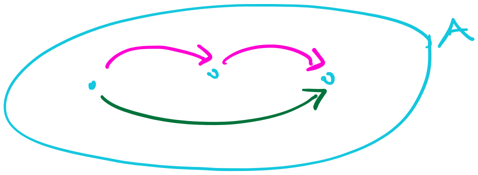
*Graphically*, every edge has a paired "backwards" edge so we might as well drop the arrows and think of edges as undirected.

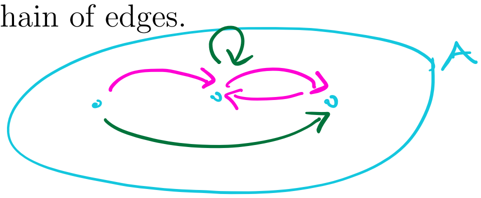


A relation $R$ on a set $A$ is called **transitive** means whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

*Informally*, chains of relations collapse. $\forall a \in A \, \forall b \in A \, \forall c \in A ( ( (a,b) \in R \wedge (b,c) \in R ) \to (a,c) \in R )$

*Graphically*, there's a shortcut between any endpoints of a chain of edges.

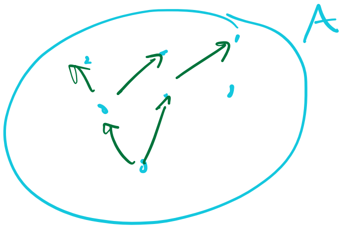




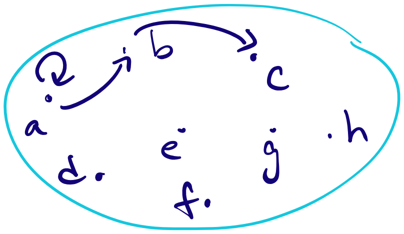
A relation $R$ on a set $A$ is called **antisymmetric** means $\forall a \in A \, \forall b \in A \; ( \; ( \; (a, b) \in R \wedge (b, a) \in R \; ) \to a = b \; )$

*Informally*, the relation has directionality. "like an ordering"

*Graphically*, can organize the nodes of the graph so that all non-self loop edges go up.

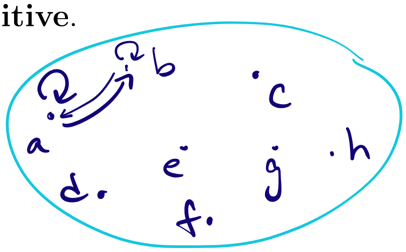


When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **not reflexive** and is **not symmetric** and is **not transitive**.



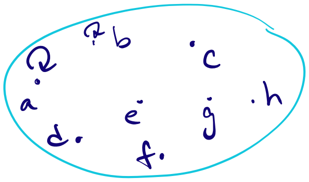
$\{(a,a), (a,b), (b,c)\}$

When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **not reflexive** but is **symmetric** and is **transitive**.



$\{(a,a), (a,b), (b,a), (b,b)\}$

When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **symmetric** and is **antisymmetric**.



$\{(a,a), (b,b)\}$

Is the relation $EQ_{\mathbb{R}}$ reflexive? symmetric? transitive? antisymmetric?

✓ ✓ ✓ ✗

Counterexample to antisymmetry: need $X_1 \subseteq \mathbb{R}$, $X_2 \subseteq \mathbb{R}$ where $(X_1, X_2) \in EQ_{\mathbb{R}}$ and $(X_2, X_1) \in EQ_{\mathbb{R}}$ but $X_1 \neq X_2$.

Choose $X_1 = \{1, 3\}$ $X_2 = \{\pi, \sqrt{2}\}$

Is the relation $R_{(\textbf{mod } 4)}$ reflexive? symmetric? transitive? antisymmetric?

✓ ✓ ✓ ✗

Counterexample to antisymmetry: need $n_1 \in \mathbb{Z}$, $n_2 \in \mathbb{Z}$ where $(n_1, n_2) \in R_{(\text{mod } 4)}$ and $(n_2, n_1) \in R_{(\text{mod } 4)}$ but $n_1 \neq n_2$

Choose $n_1 = 1$, $n_2 = 5$.

For each $n \in \mathbb{Z}^+$, $R_{(\text{mod } n)}$ is an equivalence relation.

*Summary*: binary relations can be useful for organizing elements in a domain. Some binary relations have special properties that make them act like some familiar relations. Equivalence relations (reflexive, symmetric, transitive binary relations) "act like" equals. Partial orders (reflexive, antisymmetric, transitive binary relations) "act like" less than or equals to.

$\leq$

## Definitions and representations

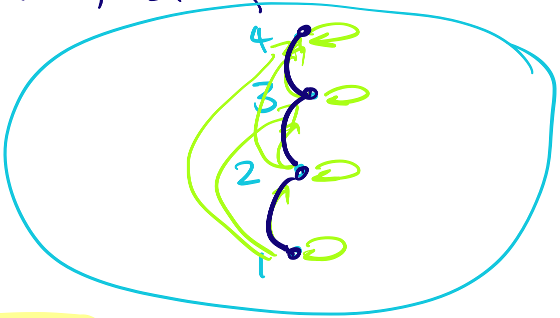
A relation is an **equivalence relation** means it is reflexive, symmetric, and transitive. Friday

A relation is a **partial ordering** (or partial order) means it is reflexive, antisymmetric, and transitive.

For a partial ordering, its **Hasse diagram** is a graph representing the relationship between elements in the ordering. The nodes (vertices) of the graph are the elements of the domain of the binary relation. The edges do not have arrow heads. The directionality of the partial order is indicated by the arrangements of the nodes. The nodes are arranged so that nodes connected to nodes above them by edges indicate that the relation holds between the lower node and the higher node. Moreover, the diagram omits self-loops and omits edges that are guaranteed by transitivity.

Domain $\{1,2,3,4\}$ Relation $\leq$

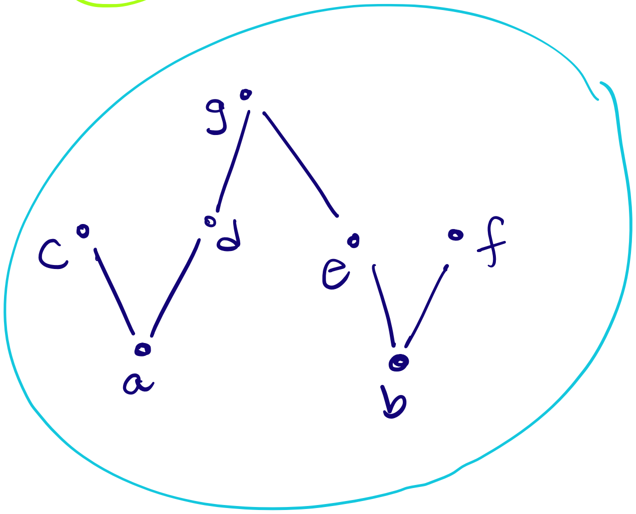
$\{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$



Draw the Hasse diagram of the partial order on the set $\{a, b, c, d, e, f, g\}$ defined as

$$\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(g,g),$$
$$(a,c),(a,d),(d,g),(a,g),(b,f),(b,e),(e,g),(b,g)\}$$

- reflexity
- antisymmetry
- transitivity



# Week 9 Friday: Equivalence relations applications

## Exploring equivalence relations

How to divide a set into a collection of "similar elements"

A **partition** of a set $A$ is a set of non-empty disjoint subsets $A_1, A_2, \cdots, A_n$ such that

$$A = \bigcup_{i=1}^{n} A_i = \{x \mid \exists i (x \in A_i)\}$$

cover the whole set

union

$A_i \neq \emptyset$

$A_i \cap A_j = \emptyset \quad (i \neq j)$

An **equivalence class** of an element $a \in A$ with respect to an equivalence relation $R$ on the set $A$ is the set

$$[a]_R \quad \{s \in A \mid (a, s) \in R\}$$

representative

all elements related to a

We write $\boxed{[a]_R}$ for this set, which is the equivalence class of $a$ with respect to $R$.

**Fact**: When $R$ is an equivalence relation on a nonempty set $A$, the collection of equivalence classes of $R$ is a partition of $A$.

Also, given a partition $P$ of $A$, the relation $R_P$ on $A$ given by

$$R_P = \{(x, y) \in A \times A \mid x \text{ and } y \text{ are in the same part of the partition } P\}$$

is an equivalence relation on $A$.

Pf strategy: Start with A and equivalence relation. WTS $\{[a]_R \mid a \in A\}$ is a partition of A

Assume reflexive, symmetric, transitive.

① pieces are nonempty
② pieces are disjoint
③ pieces cover set

Converse: start with A and partition P. WTS $R_P$ is an equivalence relation i.e. ① refl, ② sym, ③ transitive

*Recall*: We say $a$ is **congruent to** $b$ **mod** $n$ means $(a, b) \in R_{(\mathbf{mod}\ n)}$. A common notation is to write this as $a \equiv b(\mathbf{mod}\ n)$.

eg. $1 \equiv 5 \pmod 4$

We can partition the set of integers using equivalence classes of $R_{(\mathbf{mod}\ 4)}$

$[-7]_{R(\text{mod }4)} = \{s \in \mathbb{Z} \mid (-7, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = (-7) \text{ mod} = 1\} = [1]_{R(\text{mod }4)}$

$[0]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (0, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid 0 \text{ mod } 4 = s \text{ mod } 4\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 0\} = \{s \in \mathbb{Z} \mid \exists q \in \mathbb{Z} (s = 4q)\} = \{4q \mid q \in \mathbb{Z}\}$

$[1]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (1, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 1\}$

$[2]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (2, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 2\} = [6]_{R(\text{mod }4)} = [-2]_{R(\text{mod }4)}$

$[3]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (3, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 3\}$

$[4]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (4, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 0\}$

$[5]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (5, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = 5 \text{ mod } 4 = 1\}$

$[-1]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (-1, s) \in R_{(\text{mod }4)}\} = \{s \in \mathbb{Z} \mid s \text{ mod } 4 = (-1) \text{ mod } 4 = 3\}$

$-1 = -1 \cdot 4 + 3$

$$\mathbb{Z} = [0]_{R_{(\mathbf{mod}\ 4)}} \cup [1]_{R_{(\mathbf{mod}\ 4)}} \cup [2]_{R_{(\mathbf{mod}\ 4)}} \cup [3]_{R_{(\mathbf{mod}\ 4)}}$$

$0 \leq r < n$

$-7 = (-2)4 + 1$

$\{[a]_{R(\text{mod }4)} \mid a \in \mathbb{Z}\}$

$= \{[0]_{R(\text{mod }4)}, [1]_{R(\text{mod }4)}, [2]_{R(\text{mod }4)}, [3]_{R(\text{mod }4)}\}$ set with 4 elements

$[0]_{R(\text{mod }4)} \cup [1]_{R(\text{mod }4)} \cup [2]_{R(\text{mod }4)} \cup [3]_{R(\text{mod }4)} = \mathbb{Z}$

Integers are useful because they can be used to encode other objects and have multiple representations. However, infinite sets are sometimes expensive to work with computationally. Reducing our attention to a *partition of the integers* based on congrunce mod $n$, where each part is represented by a (not too large) integer gives a useful compromise where many algebraic properties of the integers are preserved, and we also get the benefits of a finite domain. Moreover, modular arithmetic is well-suited to model any cyclic behavior.

**Lemma**: For $a, b \in \mathbb{Z}$ and positive integer $n$, $(a, b) \in R_{(\textbf{mod } n)}$ if and only if $n|a - b$. Exercise

**Proof**:

Let $a, b$ be arbitrary integers and let $n$ be an arbitrary positive integer. We need to prove two directions of implication.

Goal ① WTS if $n|a-b$ then $(a,b) \in R_{(\text{mod } n)}$.

Pf ① Towards direct proof, assume $n|a-b$.

By definition of "divides" this means there's an integer, call it $q$ such that $a-b=qn$. ☆

WTS $(a,b) \in R_{(\text{mod } n)}$, namely that $a$ and $b$ have the same remainder upon division by $n$.

By division theorem, there are integers $q_a$ and $r$ where $0 \le r < n$ and $a = q_a n + r$. ⇧

Solving ☆ for $b$, and substituting ⇧ for $a$, we get

$b = a - qn = q_a n + r - qn = (q_a - q) n + r$.

Since $q_a - q$ is an integer and $r$ is an integer with $0 \le r < n$, the division theorem gives that $b \text{ mod } n = r$, so $b \text{ mod } n = a \text{ mod } n$ ▨

Goal ② WTS if $(a,b) \in R_{(\text{mod } n)}$ then $n|a-b$

By definition of $R_{(\text{mod } n)}$, $a \text{ mod } n = b \text{ mod } n$.

Let $q_a = a \text{ div } n$, $q_b = b \text{ div } n$, $r = a \text{ mod } n = b \text{ mod } n$

By division theorem,

$a = q_a n + r$ and $b = q_b n + r$.

WTS $n | a-b$.

$a - b = (q_a n + r) - (q_b n + r) = q_a n - q_b n + \cancel{r} - \cancel{r}$

$= (q_a - q_b) n$.

Since $q_a - q_b$ is an integer, we've proved $n | a-b$ ▨

Lemma is enough to give us...

$a = q_1 n + r$

$b = q_2 n + r$

**Modular arithmetic**:

**Lemma**: For $a, b, c, d \in \mathbb{Z}$ and positive integer $n$, if $a \equiv b$ ( **mod** $n$) and $c \equiv d$ ( **mod** $n$) then $a + c \equiv b + d$ ( **mod** $n$) and $ac \equiv bd$ ( **mod** $n$). **Informally**: can bring mod "inside" and do it first, for addition and for multiplication.

$(102 + 48)$ **mod** $10 =$ $(102 \bmod 10 + 48 \bmod 10) \bmod 10 = (2 + 8) \bmod 10 = 10 \bmod 10 = 0$

$(7 \cdot 10)$ **mod** $5 =$ $(7 \bmod 5)(10 \bmod 5) \bmod 5 = 2 \cdot 0 \bmod 5 = 0 \bmod 5 = 0.$

$(2^5)$ **mod** $3 =$ $32 \bmod 3 = 2$ $\quad (2^5) \bmod 3 = (2 \cdot 2 \cdot 2 \cdot 2 \cdot 2) \bmod 3.$

$$(2 \bmod 3)^{5 \bmod 3} \bmod 3 = 2^2 \bmod 3 = 4 \bmod 3 = 1$$

Let's try really big numbers

$$\overset{a}{123456} \times \overset{c}{789012} \bmod \overset{n}{1000}$$

$$= (123456 \bmod 1000 \times 789012 \bmod 1000) \bmod 1000$$

$$= (\overset{b}{456} \times \overset{d}{12}) \bmod 1000$$

$$= (4560 + 912) \bmod 1000$$

$$= 5472 \bmod 1000 = 472$$

Compute the last digit of mod 10

$(42)^{2026}$ mod 10

$$42^{2026} \bmod 10 = (\underbrace{42 \cdot \,\text{-}\, \cdot \,\text{-}\, \text{-}\, \text{-} \quad 42}_{2026 \text{ times}}) \bmod 10 \quad \cdots$$

$$= (\underbrace{(42 \bmod 10) \cdot \cdot \cdot \text{-}\, \text{-} \quad (42 \bmod 10)}_{2026 \text{ times}}) \bmod 10$$

$$= (\underbrace{2 \cdot \cdot \cdot \text{-}\, \text{-} \quad 2}_{2026 \text{ times}}) \bmod 10$$

$2^5 \bmod 10 = (2^4 \bmod 10 \cdot 2 \bmod 10) \bmod 10$
$= 6 \cdot 2 \bmod 10 = 2$

$2^0 \bmod 10 = 1$ $\quad 2^1 \bmod 10 = 2$ $\quad 2^2 \bmod 10 = 4$ $\quad 2^3 \bmod 10 = 8$ $\quad 2^4 \bmod 10 = 6$ $\quad 2^5 \bmod 10 = 2$ $\quad 2^6 \bmod 10 = 4$ $\quad 2^7 \bmod 10 = 8$ $\quad 2^8 \bmod 10 = 6$

Claim: $n \bmod 4$ determines value of $2^n \bmod 10$. $\quad$ Calculate: $2026 = 506 \cdot 4 + 2$

*Extra* Describe the pattern that helps you perform this computation and prove it using mathematical induction.

So $(42)^{2026} \bmod 10 = 2^{2026} \bmod 10 = 4$

More precisely, the claim is that for $n \geq 1$

$$2^n \bmod 10 = \begin{cases} 6 & \text{if } n \bmod 4 = 0 \\ 2 & \text{if } n \bmod 4 = 1 \\ 4 & \text{if } n \bmod 4 = 2 \\ 8 & \text{if } n \bmod 4 = 3 \end{cases}$$

Since $2026 = 506 \cdot 4 + 2$, $2026 \bmod 4 = 2$ and thus claim gives $2^{2026} \bmod 10 = 4$.