Chapter 8 Discrete Mathematics Notes

Miagao

Contents

8 Properties of Relations

8.1 Relations on Sets

- This section will review relations from Chapter 1.
- Recall that an element of one set may be related to another by a relation R as long as they satisfy its definition.

Example: Less-than Relation

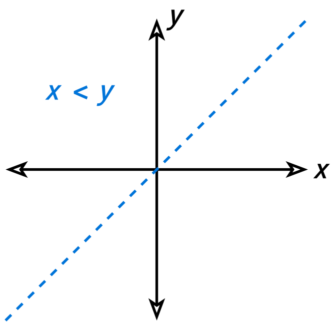
A relation L from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

For all real numbers x and y,

$$x\,L\,y \Leftrightarrow x < y$$

- $53\,L\,67$?
  - True, $53 < 67$.
- $141\,L\,141$?
  - False, $141 = 141$.
- $12\,L\,{-1}$?
  - False, $12 > -1$.

Additionally, L may be graphed as a subset of $\mathbb{R} \times \mathbb{R}$, the Cartesian plane using its rule, $x < y$.



Graph 8.1.1: *Anything ordered pair above the dotted line satisfy L.*

Example: Congruence Modulo 2 Relation

A relation E from $\mathbb{Z}$ to $\mathbb{Z}$ is defined as follows:

For every $(m,n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m\,E\,n \Leftrightarrow m - n \text{ is even}$$

- Prove that if n is any odd integer, then $n\,E\,1$.

Continued on next page

Example: *Congruence Modulo 2 Relation continued*

Proof:

Suppose n is any odd integer.
By definition of odd, $n = 2k + 1$ for some integer k.
By definition of E, $n\,E\,1$ if, and only 1if, $n - 1$ is even.
By substituion,

$$2k + 1\,E\,1 \Leftrightarrow 2k + 1 - 1 \text{ is even}$$

As said earlier, k is an integer, so by extension, $2k$ is even by definition of even.

- Therefore, $n\,E\,1$.
- Notably, integers m and n are only related by E if, and only if,

$$m \bmod 2 = n \bmod 2$$

- This means that m and n are **congruent modulo** 2.

This may also apply to modulo relations other than 2. For example, if T is defined from $\mathbb{Z}$ to $\mathbb{Z}$ as follows:

$$\textit{For all integers } m \textit{ and } n,$$

$$m\,T\,n \Leftrightarrow 3 \mid (m - n)$$

then m and n are **congruent modulo 3** by the relation T.

Inverse Relations

Definition:

Let R be relation from A to B. The inverse relation R^{-1} may be defined as follows:

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}$$

- Or, more formally,

$$\forall x \in A \text{ and } y \in B,$$
$$(y, x) \in B \times A \Leftrightarrow (x, y) \in R$$

- On finite sets, an easy way to determine the inverse relation is to reverese the direction of the arrows in the original relation's arrow diagram.

Example: Finite Relation Inverse

Given $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$, let R be the *divides* relation from A to B defined as follows:

$$\textit{For every ordered pair } (x, y) \in A \times B,$$

$$x\,R\,y \Leftrightarrow x \mid y$$

- What are the ordered pairs of R and R^{-1}?

Continued on next page

Example: *Finite Relation Inverse continued*

By listing out each ordered pair of R, R^{-1} may be easily found by reversing the order of each tuple.

$$R = \{(2,2),(2,6),(2,8),(3,6),(4,8)\}$$
$$R^{-1} = \{(2,2),(6,2),(8,2),(6,3),(8,4)\}$$

The same methodology applies to their arrow diagrams as well.

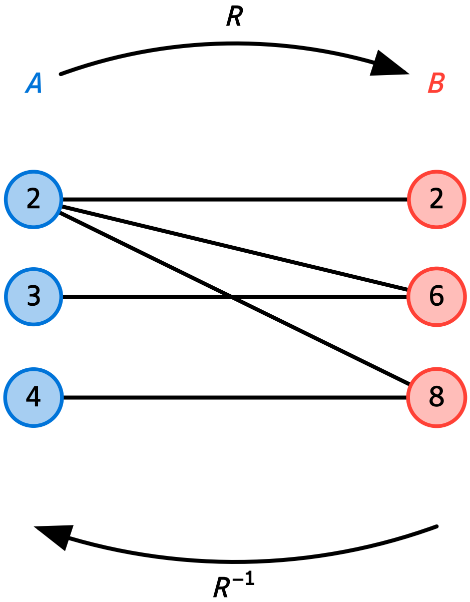


Diagram 8.1.4: *The arrow diagrams of R and R^{-1} are identical aside from the direction.*

- However, for relations on infinite sets, the inverse for the relation's rule must be found.

Example: Infinite Relation Inverse

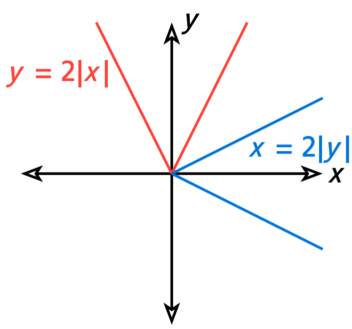
Let R be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined as follows:

For every ordered pair $(x,y) \in \mathbb{R} \times \mathbb{R}$,

$$x\,R\,y \Leftrightarrow y = 2|x|$$

- If the graph of R^{-1} are drawn on the Cartesian plane, will it be a function?
  - Using R's definition, R^{-1} may be expressed as a function of y.

$$R^{-1} = \{(y,x) \in \mathbb{R} \mid x = 2|y|\}$$



Continued on next page

Example: *Infinite Relation Inverse continued*

- Given this, the following tables may be procured:

x	y
0	0
1	2
−1	2
2	4
−2	4

y	x
0	0
2	1
2	−1
4	2
4	−2

- From the table above, it can be seen that R^{-1} has two x-values for each $y > 0$. For instance, both $(2, 1)$ and $(2, -1)$ are in R^{-1}, so it is not a function.

- While arrow diagrams can be a useful tool for finding inverse relations, their layouts do not clearly show arrow diagram properties, especially on one set.
- However, they *are* similar to directed graphs, and applying graph properties from previous chapters will make them more useful in those cases.

Directed Graph of a Relation

Definition:
A **relation on a set A** is a relation from A to A.

- In this case, if a relation R is defined on set A, then the relation's arrow diagram may also be expressed as a **directed graph**.
- Elements related to themselves are expressed as a loop.

Example: Directed Graph of a Relation
Let set $A = \{3, 4, 5, 6, 7, 8\}$
Let a relation R be defined on set A as follows:

$$\textit{For every } x, y \in A,$$

$$x\,R\,y \Leftrightarrow 2 \mid (x - y)$$

- A directed graph can be created as follows:

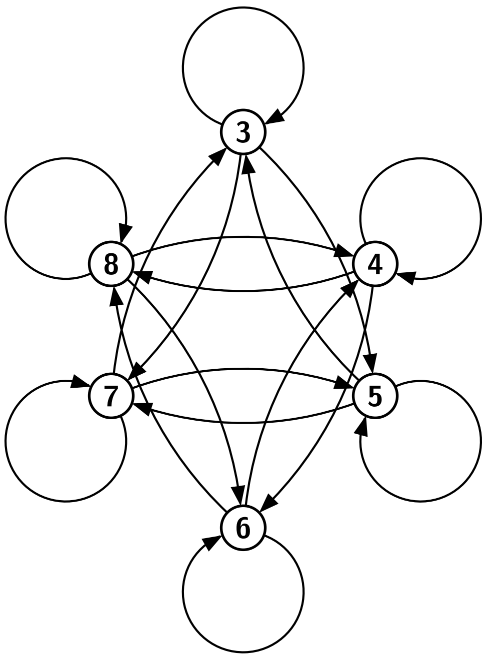


Diagram 8.1.7: The directed graph for R. It

Notice how every vertex in the directed graph connects to itself. This means that every element in A is related to itself by R. By extension, all vertices are only connected to vertices with the same parity.

- Many previously learned graph properties are present in the previous example's diagram, including loops, parallel edges, and connectedness.
- As mentioned earlier, some of those properties imply properties of the relation.

N-ary Relations and Relational Databases

- Particular relations formed from Cartesian products of n sets, known as N-ary relations, are the mathematical basis for relational database theory.

Definition:
Given the sets $A_1, A_2, \ldots, A_n$, the **n-ary relation** on
$A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The following special cases are defined as the following:

- **2**-ary is **binary**.
- **3**-ary is **tertiary**.
- **4**-ary is **quaternary**.

In a database, these n-ary relations can be thought of as tables with n columns with the headers $A_1, A_2, \ldots, A_n$.

8.2 Reflexivity, Symmetry, and Transitivity

Definition:
Let R be a relation on set A.

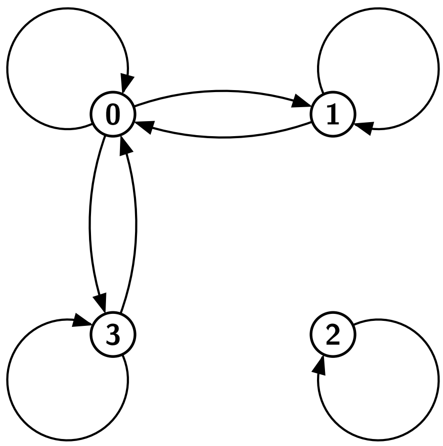
1. R is **reflexive** $\Leftrightarrow$ for all $x \in A$, $x\,R\,x$.
2. R is **symmetric** $\Leftrightarrow$ for every $x, y \in A$, if $x\,R\,y$, then $y\,R\,x$.
3. R is **transitive** $\Leftrightarrow$ for all $x, y, z \in A$, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$.

- Relating this back to directed graphs for relations, these properties may be identified graphically:
  1. The reflexive property may be shown by loops on every vertex.
  2. The symmetric property may be shown by connections between two vertices always being through opposite parallel edges.
  3. The transitive property may be shown by there being no *incomplete directed triangles*.
- Logically, the following negations may be used to disprove them:
  1. R is **not reflexive** $\Leftrightarrow \exists x \in A$ such that $(x, x) \notin R$.
  2. R is **not symmetric** $\Leftrightarrow \exists x, y \in A$ such that if $(x, y) \in R$, then $(y, x) \notin R$.
  3. R is **not transitive** $\Leftrightarrow \exists x, y, z \in A$ such that if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \notin R$.

Example: Properties of Relations on Finite Sets
Let $A = \{0, 1, 2, 3\}$ and R, S, and T be defined as follows:

$$R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\}$$
$$S = \{(0,0), (0,2), (0,3), (2,3)\}$$
$$T = \{(0,1), (2,3)\}$$

- Is R reflexive, symmetric, and/or transitive?



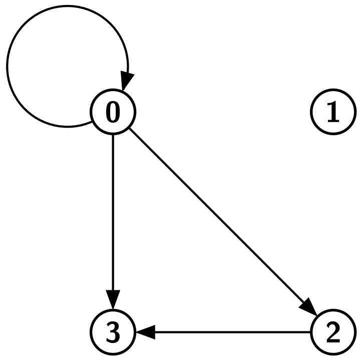
Graph 8.2.8: *The directed graph for R.*

  - R is reflexive because there is a loop an each vertex in the directed graph.
  - R is also symmetric because for each connection from one vertex to another, there is a second connection from the second vertex to the first.
  - However, R is not transitive because there is no complete directed triangle on the directed graph (no directed edge from 1 to 3)

Continued on next page

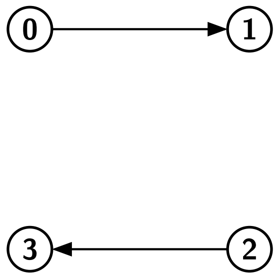
Example: *Properties of Relations on Finite Sets continued*

- Is S reflexive, symmetric, and/or transitive?
  - Similar to the first example, creating a directed graph makes this easier.



Graph 8.2.10: *The directed graph for S.*

  - S is not reflexive because the only vertex with a loop is 0.
  - S is not symmetric because when there are connections between vertices, it is only from one vertex to another.
  - S is transitive because there is one case where a vertex is both directly and transitively connected to a vertex ($\mathbf{0} \to \mathbf{2} \to \mathbf{3}$ and $\mathbf{0} \to \mathbf{3}$)
- Is T reflexive, symmetric, and/or transitive?
  - Again, we will create a directed graph to represent T.



Graph 8.2.11: *The directed graph for T.*

  - T is not reflexive because no vertices are connected to themselves via a loop.
  - T is not symmetric because when there are connections between vertices, it is only from one vertex to another.
  - T is not transitive because there only exists two edges in the graph.

Properties of Relations on Infinite Sets

- For proving relation properties on infinite sets, we have to refer back to their definitions
  - Recall that to prove that a relation is symmetric, we must prove

$$\forall x, y \in A, x\,R\,y \Rightarrow y\,R\,x$$

- For instance, to prove an *equality* relation on the set of all real numbers, we have to prove

$$\forall x, y \in \mathbb{R}, x = y \Rightarrow y = x$$

- While these examples are intuitive, generalizing from the generic particular is often neccessary to prove properties.

Example: Equality Relation

Let R be a relation defined on $\mathbb{R}$ as follows:

$$\textit{For all real numbers } x \textit{ and } y,$$

$$x\,R\,y \Leftrightarrow x = y$$

- Is R reflexive?
  - Yes. x is equal to itself, meaning that $x\,R\,x$.
- Is R symmetric?
  - Yes. Equality is symmetric; $x = y \Rightarrow y = x$. Thus, $x\,R\,y \Rightarrow y\,R\,x$.
- Is R transitive?
  - Yes. Equality is transitive; $x = y$ and $y = z \Rightarrow x = z$. Thus, $x\,R\,y \wedge y\,R\,z \Rightarrow x\,R\,z$

- Recall that two integers may be congruent modulo for integers other than 2 as long as that integer divides their difference.

Example: Properties of Congruence Modulo 3

Let a relation T be defined on $\mathbb{Z}$ as follows:

$$\textit{For all integers } m \textit{ and } n,$$

$$m\,T\,n \Leftrightarrow 3 \mid (m - n)$$

- Is T reflexive?
  - **Proof:**
    Suppose m is a *particular but arbitrarily chosen* integer such that $m\,T\,m$. By definition of T,

    $$3 \mid (m - m) = 3 \mid 0$$

    By definition of divisiblity, 3 divides 0 because $0 = 0 \cdot 3$.
  - Thus, T is reflexive.

- Is T symmetric?
  - **Proof:**
    Suppose m and n are *particular but arbitrarily chosen* integers such that $m\,T\,n$.
    By definition of T,

    $$3 \mid (m - n)$$

    By definition of divisibility, $m - n = 3k$ for some integer k.

    $$\begin{aligned} m - n &= 3k \text{ for some integer } k \\ n - m &= 3(-k) \text{ for some integer } k \text{ by algebra} \end{aligned}$$

    $\mathbb{Z}$ is closed under multiplication, so $-k$ is an integer.
    Therefore, by definition of divisibility, $3 \mid (n - m)$.
  - Thus, T is symmetric.

Continued on next page

Example: *Properties of Congruence Modulo 3 continued*

- Is T transitive?
  - **Proof:**
    Suppose m, n, and p are *particular but arbitrarily chosen* integers such that $m\,T\,n$ and $n\,T\,p$.
    By definition of T,
    $$3 \mid (m-n) \text{ and } 3 \mid (n-p)$$
    By definition of divisibility, $m-n=3r$ and $n-p=3s$ for some integers r and s.
    $$(m-n)+(n-p)=3r+3s \text{ by adding both together}$$
    $$m-p=3(r+s) \text{ by algebra}$$
    $(r+s)$ is an integer because $\mathbb{Z}$ is closed under addition.
    Therefore, by definition of divisibility, $3 \mid (m-p)$.
  - Thus, T is transitive.

The Transitive Closure of a Relation

Definition:
The **transitive closure** of R, denoted R^t, is a relation on set A that satisfies the following three properties:

1. R^t is **transitive**.
2. $R \subseteq R^t$.
3. Given S, another transitive relation containing R, $R^t \subseteq S$.

- Generally, relations are not transitive because the property requires a particular pair to exist in the relation given a transitive connection between two elements on the set.
- Thus, to find the next closest transitive relation, the transitive closure, tuples need to be added to ensure the transitivity of the relation.

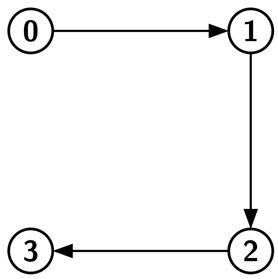
Example: Transitive Closure of a Relation
Let $A=\{0,1,2,3\}$.
Let relation R be defined on A as follows:
$$R=\{(0,1),(1,2),(2,3)\}$$

- What is the transitive closure of R?
  - Given the **second property** of transitive closures defined earlier:
    $$\{(0,1),(1,2),(2,3)\} \subseteq R^t$$

Continued on next page

Example: *Transitive Closure of a Relation continued*

- First, a directed graph for R may be constructed.

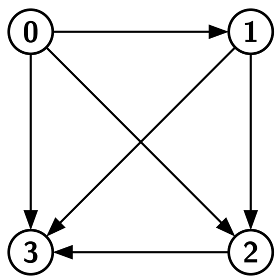


Graph 8.2.14: *The directed graph for* R*. From here, we can see transitive connections from vertices* **0** *and* **1***, respectively, to other vertices in the graph.*

- Now we can look for potential edges that can be added to create R^t.
- From vertex **0**, we know that we can add edges to vertex **2** and **3** because vertex **0** has indirect connections to them.
- Additionally, we can add an edge from vertex **1** to **3** because it is transitively connected to it through vertex **2**.
- Thus, we can say that R^t equals

$$R^t = \{(0,1),(0,2),(0,3),(1,2),(1,3),(2,3)\}$$

- This works because we know that the previous ordered pairs are at least in R^t. However, this relation is transitive, thus it equals R^t.



Graph 8.2.15: *The directed graph for* R^t.

8.3 Equivalence Relations

The Relation Induced by a Partition

- Recall that a **partition** of a set is a collection of mutually disjoint sets whose union is the original set.

Definition:
Given a partition of set A, the **relation induced by the partition**, R, is defined on A as follows:

$$\text{For every } x, y \in A,$$

$$x\,R\,y \Leftrightarrow \text{There is a subset } A_i \text{ of the partition such that both } x \text{ and } y \text{ are in } A_i.$$

Example: Relation Induced by the Partition
Let $A = \{0, 1, 2, 3, 4\}$. A partition of A is as follows:

$$\{0, 3, 4\}, \{1\}, \{2\}$$

- What is the relation R induced by this partition?
  - *We can evaluate the ordered pairs in R by analyzing the contents of each set in the partition.*
  - According to the contents of the first set:

$$\begin{gathered} 0\,R\,0 \\ 0\,R\,3 \\ 0\,R\,4 \\ 3\,R\,0 \\ 3\,R\,3 \\ 3\,R\,4 \\ 4\,R\,0 \\ 4\,R\,3 \\ 4\,R\,4 \end{gathered}$$

  - Additionally, acording to the contents of the other sets:

$$\begin{gathered} 1\,R\,1 \\ 2\,R\,2 \end{gathered}$$

  - Therefore,

$$R = \{(0,0), (0,3), (0,4), (3,0), (3,3), (3,4), (4,0), (4,3), (4,4), (1,1), (1,2)\}$$

Theorem 8.3.1:
Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Definition of an Equivalence Relation

Definition:
Let A bet a set and R be a relation on A. R is an **equivalence relation**, if, and only if, R is reflexive, symmetric, and transitive.

Example: An Equivlanece Relation on a Set of Subsets
Let X be the set of all nonempty subsets of $\{1, 2, 3\}$. Then,

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

- Define a relation R on X as follows:

For every A and B in X,

$$A\,R\,B \Leftrightarrow \textbf{The least element in } A \textbf{ equals the least element in } B.$$

- *Prove that R has all three properties.*
- **Prove that R is reflexive:**
  - Suppose that A is a nonempty subset of $\{1, 2, 3\}$.
  - Logically, the least element of A should always equal the least element of A.
  - Therefore, $A\,R\,A$.
  - R is reflexive.
- **Prove that R is symmetric:**
  - Suppose that A and B are nonempty subsets of $\{1, 2, 3\}$ such that $A\,R\,B$.
  - If $A\,R\,B$, then the least element of A equals the least element in B.
  - This implies that the least element in B equals the last element of A.
  - So, in this case, $B\,R\,A$.
  - R is symmetric.
- **Prove that R**
  - Suppose that A, B, and C are nonempty subsets of $\{1, 2, 3\}$ such that $A\,R\,B$ and $B\,R\,C$.
  - By definition of R, the least element of A equals the least element in B, and the least element in B equals the least element in C.
  - As a result, the least element of A must equal the least element in C.
  - Hence, $A\,R\,C$.
  - R is transitive.

Because R is reflexive, symmetric, and transitive, it is an equivalence relation.

Equivalence Classes of an Equivalence Relation

Definition:
Suppose that R is an equivalence relation on a set A. For each element a in A, the **equivalence class of a**, denoted $[a]$ and called the **class of a** for short, is the set of all elements $x \in A$ such that $x\,R\,a$.

$$[a] = \{x \in A \mid x\,R\,a\}$$

- Procedurely,

$$\text{for every } x \in A, x \in [a] \Leftrightarrow x \, R \, a$$

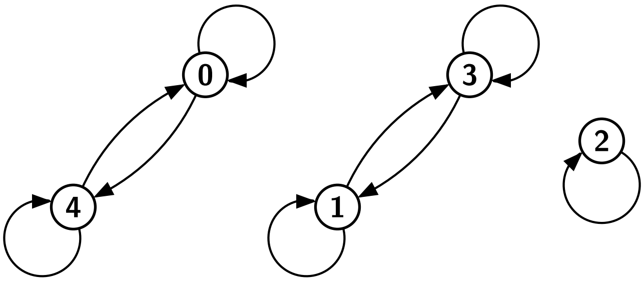
- The notation $[a]_R$ may be used to specify an equivalence class of a for a particular relation R.
- An important property of equivalence classes is that they can take on **different names**.

Example: Equivalence Classes of a Relation Given as a Set of Ordered Pairs

Let $A = \{0, 1, 2, 3, 4\}$ and define relation R on A as follows:

$$R = \{(0,0), (0,4), (1,1), (1,3), (2,2), (3,1), (3,3), (4,0), (4,4)\}$$

Additionally, the directed graph is as follows:



- What are the distinct equivalence classes of R?

$$[0] = \{x \in A \mid x \, R \, 0\} = \{0, 4\}$$
$$[1] = \{x \in A \mid x \, R \, 1\} = \{1, 3\}$$
$$[2] = \{x \in A \mid x \, R \, 2\} = \{2\}$$
$$[3] = \{x \in A \mid x \, R \, 3\} = \{1, 3\}$$
$$[4] = \{x \in A \mid x \, R \, 4\} = \{0, 4\}$$

Removing duplicate sets, the distinct equivalence classes are as follows:

$$\{0, 4\}, \{1, 3\}, \{2\}$$

Example: Equivalent Classes of the Identity Relation

Let A be any set and define a relation R on A as follows:

$$\textit{For every } x, y \in A,$$

$$x \, R \, y \Leftrightarrow x = y$$

R is also an equivalence relation.

- What are the distinct equivalence classes of R?

$$[a] = \{x \in A \mid x \, R \, a\}$$
$$[a] = \{x \in A \mid x = a\} \text{ by definition of } R$$
$$[a] = \{a\}$$

Given this definition, the classes for all elements in A are all distinct equivalence classes of R.

Lemma 8.3.2:
Suppose R is an equivalence relation on set A, and a and b are elements of A.

$$a\,R\,b \Rightarrow [a] = [b]$$

Lemma 8.3.3:
If R is an equivalence relation on set A, and a and b are elements of A, then

$$[a] \cap [b] = \emptyset \text{ or } [a] = [b]$$

Theorem 8.3.4:
Given equivalence relation R on set A, the distinct equivalence classes of R altogether are equivalent to A's partition.

Congruence Modulo n

Example: Equivalence Classes of Congruence Modulo 3
Let R be the congruence modulo 3 relation on $\mathbb{Z}$, or

$$m\,R\,n \Leftrightarrow 3 \mid (m - n)$$

- What are the equivalence classes of R?
  - For each integer a,

$$[a] = \{x \in \mathbb{Z} \mid x\,R\,a\}$$
$$[a] = \{x \in \mathbb{Z} \mid 3 \mid (x - a)\} \text{ by definition of } R$$
$$[a] = \{x \in \mathbb{Z} \mid (x - a) = 3k \text{ for some integer } k\} \text{ by definition of divisibility}$$
$$[a] = \{x \in \mathbb{Z} \mid x = 3k + a\}$$

  - It should follow that there are three equivalence classes of R.

$$[0] = \{x \in \mathbb{Z} \mid x = 3k \text{ for some integer } k\}$$
$$[1] = \{x \in \mathbb{Z} \mid x = 3k + 1 \text{ for some integer } k\}$$
$$[2] = \{x \in \mathbb{Z} \mid x = 3k + 2 \text{ for some integer } k\}$$

This is an instance of a relation where equivalence classes can take on different names. Since the relation in based on remainders, $[0]$ is the same equivalence class as $[3]$ or $[6]$.

Definition:
Suppose R is an equivalence relation on set A and S is an equivalence class for R. A **representative** of the class S is an element is any element a such that $[a] = S$.

Definition:
Let m and n be integers and let d be a positive integer. m is said to be **congruent to** n **modulo** d, shown as

$$m \equiv n (\text{mod}\, d) \Leftrightarrow d \mid (m - n)$$

Example: Evaluating Congruencies

Determine the truth values of the following congruencies:

$$12 \equiv 7 \pmod 5$$
$$6 \equiv -8 \pmod 4$$
$$3 \equiv 3 \pmod 7$$

- The first congruency is true.

$$\begin{aligned} 12 - 7 &= 5 \\ &= 5 \cdot 1 \\ \therefore 5 &\mid (12 - 7) \end{aligned}$$

- The second congruency is false.

$$\begin{aligned} 6 - (-8) &= 14 \\ \therefore 5 &\nmid (6 - (-8)) \end{aligned}$$

- The third congruency is true.

$$\begin{aligned} 3 - 3 &= 0 \\ &= 7 \cdot 0 \\ \therefore 7 &\mid (3 - 3) \end{aligned}$$

A Definition for Rational Numbers

- When expressed as fractions, the same rational number can be expressed using different numerators and denominators

$$\frac{6}{7} = \frac{12}{14}$$

  - Yet, they could represent the different tuples $(6, 7)$ and $(12, 14)$.
- Algebraically, it follows that

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

Example: Rational Numbers As Equivalence Classes

Let A be the set of all ordered pairs of integers excluding pairs whose second element is zero.

$$A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$$

Additionally, let R be a relation on A as follows:

For all pairs (a, b) *and* $(c, d) \in A$,

$$(a, b) R (c, d) \Leftrightarrow ad = bc$$

Continued on next page

Example: *Rational Numbers as Equivalence Classes continued*

- Prove that R is transitive.

Suppose (a,b), (c,d), and (e,f) are *particular but arbitrarily chosen* elements of A such that $(a,b)R(c,d)$ and $(c,d)R(e,f)$.
By definition of R,

$$(1)\ ad = bc$$
$$(2)\ cf = de$$

Because the second elements for all tuples in A are nonzero, both sides of (1) and (2) may be multiplied by f and b, respectively.

$$(1')\ adf = bcf$$
$$(2')\ bcf = bde$$

Now, $(1')$ and $(2')$ are equal to the same thing. Thus,

$$\begin{aligned} adf &= bde \\ af &= be \text{ because } d \neq 0 \end{aligned}$$

Therefore, by definition of R, $(a,b)R(e,f)$.
R is transitive.

- What are the equivalence classes of R?

Every unique rational number may represent an equivalence class for R. Meanwhile, equivalent rational numbers are stored in each equivalence class because the rule for R follows the same logic as the equality of rational numbers.

$$[(1,2)] = \{(1,2),(-1,-2),(2,4),(-2,-4),...(n,2n)\} \text{ for each } n \in \mathbb{Z} - \{0\}$$

8.4 Modular Arithmetic with Applications to Cryptography

Cryptography refers to study of learning techniqiues to mask messages. **Encryption** transforms **plaintext** into **ciphertext**, which is largely unreadable without using **decryption**. Methods of encryption are known as **ciphers**.

- For example, the **Caesar cipher** encrypts messages by doing an alphanumeric shift that wraps back to the beginning.
  - Thus, given numerical represents of ciphertext C and plaintext M:

$$C = (M + 3) \bmod 26$$

  - *Each letter in the Latin alphabet may be associated with a number according to their position.*
- Simple ciphers like the Caesar cipher can be very unsecure, espeically with larger plaintext where patterns are accentuated.
- Meanwhile, public-key cryptography systems, including the **RSA cipher**, use properties of congruence modulo n, making them very difficult to decrypt.

Properties of Congruence Modulo n

Theorem 8.4.1:

Let a, b, and n be any integers for $n > 1$. These statements are all equivalent to each other:

- $n \mid (a - b)$.
- $a \equiv b (\operatorname{mod} n)$.
- $a = b + kn$ for some integer k.
- a and b have the same nonnegative remainder when divided by n.
- $a \operatorname{mod} n = b \operatorname{mod} n$.

- Recall the quotient-remainder theorem

$$a = nq + r \text{ for } 0 \leq r < n$$

- Consequently, there are exactly n integers that satisfy the constraint, and, by extension, n possible remainders.

Definition:

Given integers a and n for $n > 1$, **the residue of** $a \operatorname{mod} n$—or **the residue of** a for short—is $a \operatorname{mod} n$. Furthermore, the sequence $0, 1, 2, \ldots, n - 1$ is the **complete set of residues modulo** n. By equating $a \operatorname{mod} n$ to its residue, we are **reducing a number modulo** n.

Theorem 8.4.2:

Given an integer n for $n > 1$, congruence mondulo n is an equivalence relation on $\mathbb{Z}$. The distinct equivlaence classes of the set are

$$[a] = \{m \in Z \mid m \equiv a (\operatorname{mod} n)\}$$

for each $a = 0, 1, 2, \ldots, n - 1$.

Modular Arithmetic

A core principle of congruence modilo n is that performing operations closed under $\mathbb{Z}$ before reducing via modulo n is the exact same as performing modulo n on the operands.

Theorem 8.4.3:

Given integers a, b, c, d, and n for $n > 1$, suppose that

$$a \equiv c \operatorname{mod} n \text{ and } b \equiv d (\operatorname{mod} n)$$

The following equivalencies must hold:

- $(a + b) \equiv (c + d)(\operatorname{mod} n)$.
- $(a - b) \equiv (c - d)(\operatorname{mod} n)$.
- $ab \equiv cd (\operatorname{mod} n)$.
- $a^m \equiv c^m (\operatorname{mod} n) \forall \text{ integer } m$.

Example: Modular Arithmetic Basics

Modular arithmetic's main application is reducing large computations.

- $55 + 26 \equiv (3 + 2)(\bmod 4)$

$$\begin{aligned} 81 &\equiv 5(\bmod 4) \\ 81 - 5 &= 76 \\ &= 4 \cdot 19 \\ \therefore 5 &\mid (81 - 5) \end{aligned}$$

- $55 - 26 \equiv (3 - 2)(\bmod 4)$

$$\begin{aligned} 29 &\equiv 1(\bmod 4) \\ 29 - 1 &= 28 \\ &= 4 \cdot 9 \\ \therefore 5 &\mid (29 - 1) \end{aligned}$$

- $55 \cdot 26 \equiv (3 \cdot 2)(\bmod 4)$

$$\begin{aligned} 1430 &\equiv 6(\bmod 4) \\ 1430 - 6 &= 1424 \\ &= 4 \cdot 356 \\ \therefore 5 &\mid (1430 - 6) \end{aligned}$$

- $55^2 \equiv \left(3^2\right)(\bmod 4)$

$$\begin{aligned} 3025 &\equiv 9(\bmod 4) \\ 3025 - 9 &= 3016 \\ &= 4 \cdot 754 \\ \therefore 5 &\mid (3025 - 9) \end{aligned}$$

Corollary 8.4.4:

Given integers a, b, and n for $n > 1$,

$$\begin{aligned} ab &\equiv [(a \bmod n)(b \bmod n)](\bmod n) \\ ab \bmod n &= [(a \bmod n)(b \bmod n)] \bmod n \end{aligned}$$

Additionally, for any positive integer m:

$$a^m \equiv \left[(a \bmod n)^m\right](\bmod n)$$

- When modular arithmetic is applied to large numbers, *such as in RSA cryptography*, computations use two particular properties of exponents:

$$\begin{aligned} x^{2a} &= \left(x^2\right)^a \text{ for all real numbers } x \text{ and } a \text{ for } x \geq 0. \\ x^{a+b} &= x^a x^b \text{ for all real numbers } x, a \text{ and } b \text{ for } x \geq 0. \end{aligned}$$

Example: Modulo n with powers of 2

Solve $144^4 \bmod 713$.

$$\begin{aligned}
144^4 \bmod 713 &= \left(144^2\right)^2 \bmod 713 \\
&= \left(144^2 \bmod 713\right)^2 \bmod 713 \\
&= (20736 \bmod 713)^2 \bmod 713 \\
&= 59^2 \bmod 713 \\
&= 3481 \bmod 713 \\
&= 629
\end{aligned}$$

Example: Modulo n without powers of 2

Solve $12^{43} \bmod 713$.

- *Recalling the second property, 43 can be split into multiple exponents to simplify the problem.*

$$\begin{aligned}
43 &= 2^5 + 2^3 + 2^1 + 2^0 \\
&= 32 + 8 + 2 + 1 \\
12^{43} &= 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12
\end{aligned}$$

- The exponents may be computed before plugging them back into the exponent.

$$\begin{aligned}
12 \bmod 713 &= 12 \\
12^2 \bmod 713 &= 144 \\
12^4 \bmod 713 &= 144^2 \bmod 713 \\
&= 59 \\
12^8 \bmod 713 &= 59^2 \bmod 713 \\
&= 629 \\
12^{32} \bmod 713 &= 629^2 \bmod 713 \\
&= 485
\end{aligned}$$

- It follows that by **Corollary 8.4.4.**,

$$\begin{aligned}
12^{43} \bmod 713 &= \left[\left(12^{32} \bmod 713\right) \cdot \left(12^8 \bmod 713\right) \cdot \left(12^2 \bmod 713\right) \cdot \left(12^1 \bmod 713\right)\right] \bmod 713 \\
&= (485 \cdot 629 \cdot 59 \cdot 144 \cdot 12) \bmod 713 \text{ by substitution} \\
&= 527152320 \bmod 713 \\
&= 48
\end{aligned}$$

Extending the Euclidean Algortihm

- Recall the process for the euclidean algorithm:

```
'''
For a >= b >= 0, calculate the greatest common divisor between a and b.
Continuously apply the quotient remainder theorem until a remainder of 0 is reached.
'''
def euclidean(a: int, b: int) -> int:
  if b == 0:
    return a
  return euclidean(b, a % b)
```

Definition:
An integer d is a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.

Theorem 8.4.5:
For all nonzero integers a and b, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Example: Expressing a GCD as a Linear Combination
Express $\gcd(330, 156)$ as the linear combination of 330 and 156 using the Euclidean algorithm.

- Using Euclidean's algorithm:

$$\begin{aligned} 330 &= 156 \cdot 2 + 18 \\ 156 &= 18 \cdot 8 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

- This implies that $\gcd(330, 156) = 6$.
- *Defining each remainder in terms of everything else:*

$$\begin{aligned} 18 &= 330 - 156 \cdot 2 \\ 12 &= 156 - 18 \cdot 8 \\ 6 &= 18 - 12 \cdot 1 \end{aligned}$$

- Now, we can backtrack through each step through continuous substitutions, eventually reaching the linear combination form of the greatest common denominator.

$$\begin{aligned} \gcd(330, 156) &= 6 \\ &= 18 - 12 \cdot 1 \\ &= 18 - (156 - 18 \cdot 8) \cdot 1 \text{ by substitution} \\ &= 18 \cdot 9 - 156 \\ &= (330 - 156 \cdot 2) \cdot 9 - 156 \text{ by substitution} \\ &= \underbrace{330 \cdot 9 - 156 \cdot (-19)}_{\text{Linear Combination}} \end{aligned}$$

Logically, the linear combination of 330 and 156 reduces to 6.

Finding an Inverse Modulo n

Definition:
Given any integer a and positive integer n, if there exists an integer s such that $as \equiv 1 (\operatorname{mod} n)$, then s is **an inverse for a modulo n**.

Definition:
Integers a and b are **relatively prime**, if and only if, $\gcd(a, b) = 1$.
Additionally, a sequence of integers $a_1, a_2, \ldots, a_n$ may be **pairwise relatively prime** for all integers $i \geq 1$ and $j \leq n$ given that $i \neq j$.

Corollary 8.4.6:
Given relatively prime integers a and b, there must exist integers s and t such that $as + bt = 1$.

Example: Expressing 1 as a Linear Combination of Relatively Prime Integers
Show that 660 and 43 are relatively prime. Additionally, find a corresponding linear combination equal to 1.

- Again, we will use use Euclidean's algorithm:

$$\begin{aligned}
660 &= 43 \cdot 15 + 15 \\
43 &= 15 \cdot 2 + 13 \\
15 &= 13 \cdot 1 + 2 \\
13 &= 2 \cdot 6 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

- Thus, $\gcd(660, 43) = 1$.
- **Therefore, 660 and 43 are relatively prime.**
- Because the greatest common divisor is 1, then it follows that backtracking through the algorithm should yield a Linear Combination equal to 1.
- *Defining each remainder in terms of everything else:*

$$\begin{aligned}
15 &= 660 - 43 \cdot 15 \\
13 &= 43 - 15 \cdot 2 \\
2 &= 15 - 13 \cdot 1 \\
1 &= 13 - 2 \cdot 6
\end{aligned}$$

Continued on next page

Example: *Expressing 1 as a Linear Combination of Relatively Prime Integers Continued*

- Like the last example, we can now use continous substitutions to find the Linear Combination:

$$
\begin{aligned}
\gcd(660) = 1 & \\
&= 13 - 2 \cdot 6 \text{ by substitution} \\
&= 13 - (15 - 13) \cdot 6 \text{ by substitution} \\
&= 13 - 15 \cdot 6 + 13 \cdot 6 \\
&= 13 \cdot 7 - 15 \cdot 6 \\
&= (43 - 15 \cdot 2) \cdot 7 - 15 \cdot 6 \text{ by substitution} \\
&= 43 \cdot 7 - 15 \cdot 14 - 15 \cdot 6 \\
&= 43 \cdot 7 - 15 \cdot 20 \\
&= 43 \cdot 7 - (660 - 43 \cdot 15) \cdot 20 \text{ by substitution} \\
&= 43 \cdot 7 - 660 \cdot 20 + 43 \cdot 300 \\
&= \underbrace{43 \cdot 307 - 660 \cdot 20}_{\text{Linear Combination}}
\end{aligned}
$$

Corollary 8.4.7:
For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 (\bmod n)$, that is, an inverse for a modulo n.

RSA Cryptography

i dont know what is going on anymore 😭😭😭😭😭😭😭😭😭😭