Relations

Relations

A more formal way to refer to the kind of relation we will be discussing is to call it a **binary relation** because it is a subset of a Cartesian product of two sets. At the end of this section we define an n-ary relation to be a subset of a Cartesian product of n sets, where n is any integer greater than or equal to two. Such a relation is the fundamental structure used in relational databases. However, because we focus on binary relations in this text, when we use the term relation by itself, we will mean binary relation.

A relation L from the set A to a set B is defined to be $L \subset A \times B = \{(a,b) | a \in A, b \in B\}$ $A \times B \times C = \{(a,b,c) | a \in A, b \in B, c \in C\}$

Define a relation L from $\mathbb R$ to $\mathbb R$ as follows: For all real numbers x and y,

$$x L y \Leftrightarrow x < y$$
.

- 1. Is 57 *L* 53?
- 2. Is (-17) L (-14)?
- 3. Is 143 *L* 143?
- 4. Is (-35)L1?

Draw the graph of L as a subset of the Cartesian plane $\mathbb{R} \times \mathbb{R}$.

$$L = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x < y\}$$

Define a relation E from \mathbb{Z} to \mathbb{Z} as follows: For all $(m,n) \in \mathbb{Z} \times \mathbb{Z}$, $mEn \Leftrightarrow m-n$ is even.

- a. Is 4 E 0? Is 2 E 6? Is 3 E (-3)? Is 5 E 2?
- b. List five integers that are related by *E* to 1.
- c. Prove that if n is any odd integer, then $n \in \mathbb{Z}$ is $n = 2k + 1, n 1 = 2k \implies n \in \mathbb{Z}$

Example: Let
$$X = \{a, b, c\}$$
. Then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Define a relation S from $\mathcal{P}(X)$ to $\mathcal{P}(X)$ as follows: For all sets A and B in $\mathcal{P}(X)$ (i.e., for all subsets A and B of X),

 $A S B \iff A$ has at least as many elements as B.

- a. Is $\{a, b\}S\{b, c\}$?
- b. Is $\{a\}S\emptyset$?
- c. Is $\{b, c\}S\{a, b, c\}$?
- d. Is $\{c\}S\{a\}$?

```
Let A = \{2,3,4\} and B = \{2,6,8\} and let R be the "divides" relation from A to B: For all (x,y) \in A \times B, xRy \Leftrightarrow x|y
```

Find the relation R.

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$, $xRy \Leftrightarrow x|y$

Find the relation R.

Solution: $R = \{(2,2),\}$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$, $xRy \Leftrightarrow x|y$

Find the relation R.

Solution:
$$R = \{(2,2), (2,6), \}$$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$, $xRy \Leftrightarrow x|y$

Find the relation R.

Solution: $R = \{(2,2), (2,6), (2,8), \}$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$, $xRy \Leftrightarrow x|y$

Find the relation R.

Solution: $R = \{(2,2), (2,6), (2,8), (3,6), \}$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$, $xRy \Leftrightarrow x|y$

Find the relation R.

Solution: $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}.$

The Inverse of a Relation

If R is a relation from A to B, then a relation R^{-1} from B to A can be defined by interchanging the elements of all the ordered pairs of R.

Definition:

Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as follows:

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

OR

For all $x \in A$ and $y \in B$, $(y, x) \in R^{-1} \Leftrightarrow (x, y) \in R$.

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} .

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\},$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$

Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

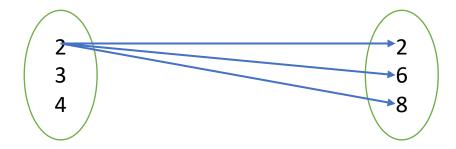
1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$



Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

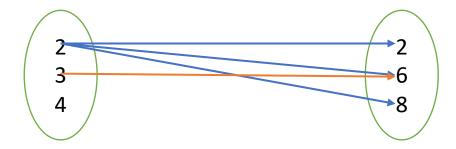
1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$



Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

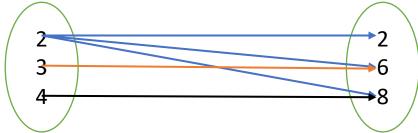
1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$



Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

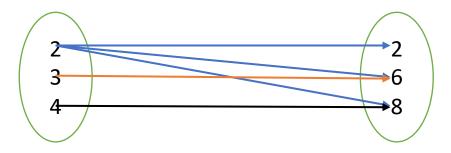
1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$



Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$ and let R be the "divides" relation from A to B: For all $(x,y) \in A \times B$,

$$xRy \Leftrightarrow x|y$$
.

1. State explicitly which ordered pairs are in R and R^{-1} and draw arrow diagrams for R and R^{-1} . $R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\}, R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}$



$$R^{-1} = \{(y, x) \in B \times A | x | y\} = \{(y, x) | y = xq \text{ some } q \in \mathbb{Z}\}$$

Definition:

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

Let $A = \{3,4,5,6,7,8\}$ and define a relation R on A as follows: For all $x, y \in A$,

$$xRy \Leftrightarrow 2|(x-y).$$

Draw the directed graph of R.

Let $A = \{3,4,5,6,7,8\}$ and define a relation R on A as follows: For all $x, y \in A$,

$$xRy \Leftrightarrow 2|(x-y).$$

Draw the directed graph of R.

$$R = \{(3,3), (3,5), (3,7), (4,4), (4,6), (4,8), (5,3), (5,5), (5,7), (6,4), (6,6), (6,8), (7,3), (7,5), (7,7), (8,4), (8,6), (8,8)\}$$

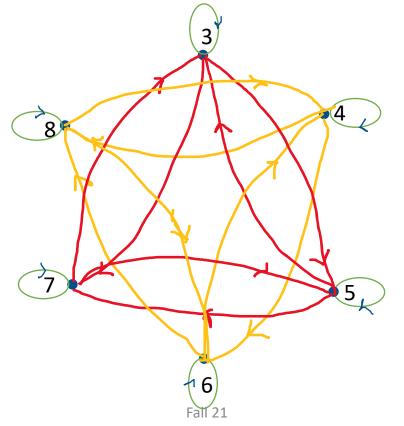
$$R = \{(3,3), (3,5), (3,7), (4,4), (4,6), (4,8), (5,3), (5,5), (5,7), (6,4), (6,6), (6,8), (7,3), (7,5), (7,7), (8,4), (8,6), (8,8)\}$$

8 • 4

7 • •₅

6

```
R = \{(3,3), (3,5), (3,7), (4,4), (4,6), (4,8), (5,3), (5,5), (5,7), (6,4), (6,6), (6,8), (7,3), (7,5), (7,7), (8,4), (8,6), (8,8)\}
```



Let R be a relation on a set A.

1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.

- 1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.
- 2. R is **symmetric** if, and only if, for all $x, y \in A$, if xRy then yRx.

- 1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.
- 2. R is **symmetric** if, and only if, for all $x, y \in A$, if xRy then yRx.
- 3. R is **transitive** if, and only if, for all $x, y, z \in A$, if xRy and yRz then xRz.

- 1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.
- 2. R is symmetric if, and only if, for all $x, y \in A$, if xRy then yRx.
- 3. R is **transitive** if, and only if, for all $x, y, z \in A$, if xRy and yRz then xRz. Or
- 1. R is reflexive \Leftrightarrow for all x in A, $(x, x) \in R$.

- 1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.
- 2. R is **symmetric** if, and only if, for all $x, y \in A$, if xRy then yRx.
- 3. R is **transitive** if, and only if, for all $x, y, z \in A$, if xRy and yRz then xRz. Or
- 1. R is reflexive \Leftrightarrow for all x in A, $(x, x) \in R$.
- 2. R is symmetric \Leftrightarrow for all x and y in A, if $(x, y) \in R$ then $(y, x) \in R$.

- 1. R is **reflexive** if, and only if, for all $x \in A$, $x \in A$, $x \in A$.
- 2. R is **symmetric** if, and only if, for all $x, y \in A$, if xRy then yRx.
- 3. R is **transitive** if, and only if, for all $x, y, z \in A$, if xRy and yRz then xRz. Or
- 1. R is reflexive \Leftrightarrow for all x in A, $(x, x) \in R$.
- 2. R is symmetric \Leftrightarrow for all x and y in A, if $(x, y) \in R$ then $(y, x) \in R$.
- 3. R is transitive \Leftrightarrow for all x, y and z in A, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

Let $A = \{0, 1, 2, 3\}$ and define relations R, S, and T on A as follows: $R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\},$

Is R reflexive? symmetric? transitive?

```
Let A = \{0, 1, 2, 3\} and define relations R, S, and T on A as follows: S = \{(0, 0), (0, 2), (0, 3), (2, 3)\},
```

Is S reflexive? symmetric? transitive?

Let $A = \{0, 1, 2, 3\}$ and define relations R, S, and T on A as follows: $T = \{(0,1), (2,3)\}.$

Is T reflexive? symmetric? transitive?

$$xRy \Leftrightarrow x = y$$
.

- a. Is *R* reflexive?
- b. Is *R* symmetric?
- c. Is *R* transitive?

$$xRy \Leftrightarrow x = y$$
.

- a. Is R reflexive? for all x in \mathbb{R} , is $(x, x) \in R$?
- b. Is *R* symmetric?
- c. Is R transitive?

$$xRy \Leftrightarrow x = y$$
.

- a. Is R reflexive? for all x in \mathbb{R} , is $(x, x) \in R$?
- b. Is R symmetric? for all x and y in A, if $(x, y) \in R$ then $(y, x) \in R$?
- c. Is *R* transitive?

$$xRy \Leftrightarrow x = y$$
.

- a. Is R reflexive? for all x in \mathbb{R} , is $(x, x) \in R$?
- b. Is R symmetric? for all x and y in A, if $(x, y) \in R$ then $(y, x) \in R$?
- c. Is R transitive? for all x, y and z in A, if $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$? $x = y \ and \ y = z \Rightarrow x = z$?

Define a relation T on \mathbb{Z} as follows: For all integers m and n, $mTn \Leftrightarrow 3|(m-n)$.

- a. Is T reflexive?
- b. Is T symmetric?
- c. Is T transitive?

Define a relation T on \mathbb{Z} as follows: For all integers m and n, $mTn \Leftrightarrow 3|(m-n)$.

- a. Is T reflexive? for all x in \mathbb{Z} , is $(x, x) \in T$?
- b. Is T symmetric?
- c. Is T transitive?

Define a relation T on \mathbb{Z} as follows: For all integers m and n, $mTn \Leftrightarrow 3|(m-n)$.

- a. Is T reflexive? for all x in \mathbb{Z} , is $(x, x) \in T$?
- b. Is T symmetric? for all x and y in \mathbb{Z} , if $(x,y) \in T$ then $(y,x) \in T$? $3|(x-y) \Rightarrow (x-y) = 3r \Rightarrow (y-x) = -3r = 3(-r)$ $\Rightarrow 3|(y-x) \Rightarrow (y,x) \in T$
- c. Is T transitive?

Define a relation T on \mathbb{Z} as follows: For all integers m and n, $mTn \Leftrightarrow 3|(m-n)$.

- a. Is T reflexive? for all x in \mathbb{Z} , is $(x, x) \in T$?
- b. Is T symmetric? for all x and y in \mathbb{Z} , if $(x, y) \in T$ then $(y, x) \in T$?
- c. Is T transitive? for all x, y and z in \mathbb{Z} , if $(x, y) \in T$ and $(y, z) \in T$ then $(x, z) \in T$? x y = 3r, y z = 3s, $x y + y z = 3r + 3s \Rightarrow x z = 3(r + s)$

Define a relation T on \mathbb{Z} as follows: For all integers m and n, $mTn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n \pmod{3}$

- a. Is T reflexive? for all x in \mathbb{R} , is $(x, x) \in R$?
- b. Is T symmetric? for all x and y in A, if $(x, y) \in R$ then $(y, x) \in R$?
- c. Is T transitive? for all x, y and z in A, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$?

Let A be the set of people living in the world today. A relation R is defined on A as follows: For all $p, q \in A$,

 $p R q \Leftrightarrow p$ lives within 100 miles of q.

Is the relation reflexive, symmetric, transitive or none of these?

Equivalence Relation

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

Let S be the set of all digital logic circuits with a fixed number n of inputs. Define a relation E on S as follows: For all circuits C_1 and C_2 in S,

 C_1E $C_2 \Leftrightarrow C_1$ has the same input/output table as C_2 .

If $C_1 E C_2$, then circuit C_1 is said to be equivalent to circuit C_2 . Prove that E is an equivalence relation on S.

Definition:

Suppose A is a set and R is an equivalence relation on 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 is related to a by R.

In symbols:

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

```
Let A = \{0,1,2,3,4\} and define a 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)\}.
```

Draw the directed graph and show that it is an equivalence relation. Find the distinct equivalence classes of R.

$$[0] = \{0,4\}, [1] = \{1,3\},$$

 $[2] = \{2\}, [3] = \{1,3\},$
 $[4] = \{0,4\}$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} =$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{ n \in \mathbb{Z} | nR0 \} = \{ n \in \mathbb{Z} | 3 | (n-0) \}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3|(n-0)\}$$

= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z}\}

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3|(n-0)\}$$
$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z}\}$$
$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3|(n-1)\}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3|(n-0)\}$$

$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z}\}$$

$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3|(n-1)\}$$

$$= \{n \in \mathbb{Z} | n - 1 = 3q \text{ some } q \in \mathbb{Z}\}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3 | (n-0)\}$$

$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z} \}$$

$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3 | (n-1)\}$$

$$= \{n \in \mathbb{Z} | n-1 = 3q \text{ some } q \in \mathbb{Z} \}$$

$$= \{n \in \mathbb{Z} | n = 3q + 1 \text{ some } q \in \mathbb{Z} \}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3 | (n-0)\}$$

$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z} \}$$

$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3 | (n-1)\}$$

$$= \{n \in \mathbb{Z} | n-1 = 3q \text{ some } q \in \mathbb{Z} \}$$

$$= \{n \in \mathbb{Z} | n = 3q + 1 \text{ some } q \in \mathbb{Z} \}$$

$$[2] = \{n \in \mathbb{Z} | nR2\} = \{n \in \mathbb{Z} | 3 | (n-2)\}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3|(n-0)\}$$

$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z}\}$$

$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3|(n-1)\}$$

$$= \{n \in \mathbb{Z} | n-1 = 3q \text{ some } q \in \mathbb{Z}\}$$

$$= \{n \in \mathbb{Z} | n = 3q+1 \text{ some } q \in \mathbb{Z}\}$$

$$[2] = \{n \in \mathbb{Z} | nR2\} = \{n \in \mathbb{Z} | 3|(n-2)\}$$

$$= \{n \in \mathbb{Z} | n-2 = 3q \text{ some } q \in \mathbb{Z}\}$$

Let R be the relation of congruence modulo 3 on the set \mathbb{Z} of all integers. That is, for all integers m and n,

$$mRn \Leftrightarrow 3|(m-n) \Leftrightarrow m \equiv n(mod3).$$

$$[0] = \{n \in \mathbb{Z} | nR0\} = \{n \in \mathbb{Z} | 3 | (n-0)\}$$

$$= \{n \in \mathbb{Z} | n = 3q \text{ some } q \in \mathbb{Z}\} = \{n \in \mathbb{Z} | n \mod 3 = 0\}$$

$$[1] = \{n \in \mathbb{Z} | nR1\} = \{n \in \mathbb{Z} | 3 | (n-1)\}$$

$$= \{n \in \mathbb{Z} | n-1 = 3q \text{ some } q \in \mathbb{Z}\}$$

$$= \{n \in \mathbb{Z} | n = 3q+1 \text{ some } q \in \mathbb{Z}\} = \{n \in \mathbb{Z} | n \mod 3 = 1\}$$

$$[2] = \{n \in \mathbb{Z} | nR2\} = \{n \in \mathbb{Z} | 3 | (n-2)\}$$

$$= \{n \in \mathbb{Z} | n-2 = 3q \text{ some } q \in \mathbb{Z}\}$$

$$= \{n \in \mathbb{Z} | n = 3q+2 \text{ some } q \in \mathbb{Z}\} = \{n \in \mathbb{Z} | n \mod 3 = 2\}$$

Theorem:

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

Definition:

Let m and n be integers and let d be a positive integer. We say that m is congruent to n modulo d and write

$$m \equiv n \pmod{d}$$

if, and only if,

$$d \mid (m-n)$$
.

Symbolically:

$$m \equiv n \pmod{d} \Leftrightarrow d \mid (m-n)$$

Properties of Congruence Modulo n

Theorem:

Let a, b, and n be any integers and suppose n > 1. The following statements are all equivalent:

- 1. n|(a-b)
- 2. $a \equiv b \pmod{n}$
- 3. a = b + kn for some integer k
- 4. a and b have the same (nonnegative) remainder when divided by n
- 5. $a \mod n = b \mod n$