MTH223A LECTURE NOTES CHAPTER 1

Yvette Fajardo-Lim

Mathematics and Statistics Department
De La Salle University - Manila

Outline

Functions

Definition

Let X and Y be two nonempty sets. A **mapping or a function f from X to Y** *is a rule denoted by $f : X \to Y$ which assigns to each element x of X a* **unique** *element y of Y. In this case, we write $y = f(x)$ to mean that the value of f at x is y. y is called the* **image** *of x and x is the* **pre-image** *of y under f. The set X is called the* **domain** *of f and Y the* **codomain** *of f. The range of f is the set $\{f(x)|x \in X\}$.*

Functions

Example

The following equations define functions from $\mathbb{R}$ to $\mathbb{R}$.

1. *Given $2x + y = 3$, then the function $y = 3 - 2x$ defines the number y to be $3 - 2x$.*
2. *The formula $y = x^2$ defines the number y to be the square of the number x.*

Functions

Example

The following equations define functions from $\mathbb{R}$ to $\mathbb{R}$.

1. *Given $2x + y = 3$, then the function $y = 3 - 2x$ defines the number y to be $3 - 2x$.*
2. *The formula $y = x^2$ defines the number y to be the square of the number x.*

Functions

Example

The following equations define functions from $\mathbb{R}$ to $\mathbb{R}$.

1. *Given $2x + y = 3$, then the function $y = 3 - 2x$ defines the number y to be $3 - 2x$.*
2. *The formula $y = x^2$ defines the number y to be the square of the number x.*

Functions

Definition

A function f with domain D is said to be **one-to-one** *or* **injective** *if whenever $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in D$.*

Example

The function $f(x) = 3 - 2x$ where $f : \mathbb{R} \to \mathbb{R}$ is injective.

Functions

Definition

A function f with domain D is said to be **one-to-one** *or* **injective** *if whenever $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in D$.*

Example

The function $f(x) = 3 - 2x$ where $f : \mathbb{R} \to \mathbb{R}$ is injective.

Functions

Definition

A function $f : X \to Y$ is said to be **onto** *or* **surjective** *if $f(X) = Y$.*

Example

The function $f(x) = 3 - 2x$ where $f : \mathbb{R} \to \mathbb{R}$ is surjective.

Functions

Definition

A function $f : X \to Y$ is said to be **onto** *or* **surjective** *if $f(X) = Y$.*

Example

The function $f(x) = 3 - 2x$ where $f : \mathbb{R} \to \mathbb{R}$ is surjective.

Functions

Definition

A function f is said to be **bijective** *if it is both one-to-one and onto. A bijective function is also called a* **one-to-one correspondence**.

Example

The function $f(x) = 3 - 2x$ is a bijective function.

Functions

Definition

A function f is said to be **bijective** *if it is both one-to-one and onto. A bijective function is also called a* **one-to-one correspondence**.

Example

The function $f(x) = 3 - 2x$ is a bijective function.

Functions

Definition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** *$g \circ f$ of f and g is the function from X to Z defined by the equation $(f \circ g)(x) = f(g(x))$ for all $x \in X$.*

Example

Let $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = 3 - 2x$. Let $g : \mathbb{R} \to \mathbb{R}$ and $f(x) = x^2$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= 9 - 12x + 4x^2\end{aligned}$$

and

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= 3 - 2x^2\end{aligned}$$

Functions

Definition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** *$g \circ f$ of f and g is the function from X to Z defined by the equation $(f \circ g)(x) = f(g(x))$ for all $x \in X$.*

Example

Let $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = 3 - 2x$. Let $g : \mathbb{R} \to \mathbb{R}$ and $f(x) = x^2$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= 9 - 12x + 4x^2\end{aligned}$$

and

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= 3 - 2x^2\end{aligned}$$

Properties of Functions

Theorem

Properties of Functions

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Properties of Functions

Theorem

Properties of Functions

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Properties of Functions

Theorem

Properties of Functions

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Properties of Functions

Theorem

Properties of Functions

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Properties of Functions

Theorem

Properties of Functions

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Divisibility of Integers

Definition

An integer b is **divisible** *by an integer $a \neq 0$ if there exists another integer c such that $b = ac$. In symbols, we write $a|b$ if b is divisible by a, and $a \nmid b$ if b is not divisible by a.*

Example

1. $3|12$ *because there exists* $c = 4$ *such that* $12 = 3 \cdot 4$.
2. $3 \nmid 16$ *because there is no* $c \in \mathbb{Z}$ *such that* $16 = 3 \cdot c$.

Divisibility of Integers

Definition

An integer b is **divisible** *by an integer $a \neq 0$ if there exists another integer c such that $b = ac$. In symbols, we write $a|b$ if b is divisible by a, and $a \not| b$ if b is not divisible by a.*

Example

1. $3|12$ *because there exists* $c = 4$ *such that* $12 = 3 \cdot 4$.
2. $3 \not| 16$ *because there is no* $c \in \mathbb{Z}$ *such that* $16 = 3 \cdot c$.

Divisibility of Integers

Definition

An integer b is **divisible** *by an integer* $a \neq 0$ *if there exists another integer c such that* $b = ac$. *In symbols, we write* $a|b$ *if b is divisible by a, and* $a \nmid b$ *if b is not divisible by a.*

Example

1. $3|12$ *because there exists* $c = 4$ *such that* $12 = 3 \cdot 4$.
2. $3 \nmid 16$ *because there is no* $c \in \mathbb{Z}$ *such that* $16 = 3 \cdot c$.

Divisibility of Integers

Definition

An integer b is **divisible** *by an integer $a \neq 0$ if there exists another integer c such that $b = ac$. In symbols, we write $a|b$ if b is divisible by a, and $a \nmid b$ if b is not divisible by a.*

Example

1. $3|12$ *because there exists* $c = 4$ *such that* $12 = 3 \cdot 4$.
2. $3 \nmid 16$ *because there is no* $c \in \mathbb{Z}$ *such that* $16 = 3 \cdot c$.

Divisibility of Integers

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Divisibility of Integers

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Divisibility of Integers

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Divisibility of Integers

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Divisibility of Integers

Theorem

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Divisibility of Integers

Theorem

1. *If* $a|b$ *then* $a|bc$ *for any integer* c.
2. *If* $a|b$ *and* $b|c$ *then* $a|c$ *for any integer* c.
3. *If* $a|b$ *and* $a|c$ *then* $a|(bx + cy)$ *for all integers* x *and* y.
4. *If* $a|b$ *and* $b|a$ *then* $a = \pm b$.
5. *If* $a|b$ *and* $a > 0, b > 0$ *then* $a \leq b$.
6. $a|b$ *if and only if* $ma|mb, m \neq 0$

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Illustration

1. *Since* $11|66$ *then theorem 1.2 part 1 tells us that* $11|330$ *because* $330 = 66 \cdot 5$.
2. *Since* $11|66$ *and* $66|198$ *then theorem 1.2 part 2 tells us that* $11|198$.
3. *Since* $3|21$ *and* $3|33$ *then theorem 1.2 part 3 tells us that* $3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6$.
4. *Since* $7|(-7)$ *and* $(-7)|7$ *then theorem 1.2 part 4 tells us that* $7 = -(-7)$.
5. *Since* $25|75$ *then theorem 1.2 part 5 tells us that* $25 < 75$.
6. *Theorem 1.2 part 6 tells us that* $8|64$ *if and only if* $16|128$.

Divisibility of Integers

Remark

If $a|b_i$ for $i = 1, 2, \ldots, n$ then $a| \sum_{i=1}^{n} b_i x_i$ for any integers $x_1, x_2, \ldots, x_n$. This is a generalization of theorem 1.2 part 3.

Theorem

The Division Algorithm. *If a and b are integers with $a > 0$, there exist unique integers q and r such that $b = aq + r$.*

Illustration

If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, since $133 = 21 \cdot 6 + 7$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$ since $-50 = 8(-7) + 6$.

Divisibility of Integers

Remark

If $a|b_i$ for $i = 1, 2, \ldots, n$ then $a|\sum_{i=1}^{n} b_i x_i$ for any integers $x_1, x_2, \ldots, x_n$. This is a generalization of theorem 1.2 part 3.

Theorem

The Division Algorithm. *If a and b are integers with $a > 0$, there exist unique integers q and r such that $b = aq + r$.*

Illustration

If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, since $133 = 21 \cdot 6 + 7$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$ since $-50 = 8(-7) + 6$.

Remark

If $a|b_i$ for $i = 1, 2, \ldots, n$ then $a|\sum_{i=1}^{n} b_i x_i$ for any integers $x_1, x_2, \ldots, x_n$. This is a generalization of theorem 1.2 part 3.

Theorem

The Division Algorithm. *If a and b are integers with $a > 0$, there exist unique integers q and r such that $b = aq + r$.*

Illustration

If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, since $133 = 21 \cdot 6 + 7$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$ since $-50 = 8(-7) + 6$.

Divisibility of Integers

Definition

The integer a is called a **common divisor** *of the integers b and c if $a|b$ and $a|c$.*

Remark

1. *If b and c are not both zero then they have only a finite number of common divisors since any nonzero integer has only a finite number of divisors.*
2. *If $b = 0$ and $c = 0$, then every integer $a \neq 0$ is a common divisor of b and c.*

Divisibility of Integers

Definition

The integer a is called a **common divisor** *of the integers b and c if $a|b$ and $a|c$.*

Remark

1. *If b and c are not both zero then they have only a finite number of common divisors since any nonzero integer has only a finite number of divisors.*
2. *If $b = 0$ and $c = 0$, then every integer $a \neq 0$ is a common divisor of b and c.*

Divisibility of Integers

Definition

The integer a is called a **common divisor** *of the integers b and c if $a|b$ and $a|c$.*

Remark

1. *If b and c are not both zero then they have only a finite number of common divisors since any nonzero integer has only a finite number of divisors.*
2. *If $b = 0$ and $c = 0$, then every integer $a \neq 0$ is a common divisor of b and c.*

Divisibility of Integers

Definition

The integer a is called a **common divisor** *of the integers b and c if $a|b$ and $a|c$.*

Remark

1. *If b and c are not both zero then they have only a finite number of common divisors since any nonzero integer has only a finite number of divisors.*
2. *If $b = 0$ and $c = 0$, then every integer $a \neq 0$ is a common divisor of b and c.*

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Divisibility of Integers

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Divisibility of Integers

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Divisibility of Integers

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Divisibility of Integers

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Divisibility of Integers

Example

1. *If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.*
2. *If $b = 0$ and $c = 0$, there are infinite number of common divisors.*

Definition

The positive integer a is said to be the **greatest common divisor** *of b and c if*

1. $a|b$ and $a|c$
2. $d|b$ and $d|c \Rightarrow d|a$

We write (b, c) to denote the greatest common divisor of b and c.

Example

From example 1.7, if $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$. Hence, $(4, 6) = 2$.

Remark

If $(b, c) = g$ then there exists integers x and y such that $g = bx + cy$.

Example

Since $(4, 6) = 2$ then $2 = 4 \cdot 2 + 6(-1)$ where $x = 2$ and $y = -1$.

Divisibility of Integers

Example

From example 1.7, if $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$. Hence, $(4, 6) = 2$.

Remark

If $(b, c) = g$ then there exists integers x and y such that $g = bx + cy$.

Example

Since $(4, 6) = 2$ then $2 = 4 \cdot 2 + 6(-1)$ where $x = 2$ and $y = -1$.

Divisibility of Integers

Example

From example 1.7, if $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$. Hence, $(4, 6) = 2$.

Remark

If $(b, c) = g$ then there exists integers x and y such that $g = bx + cy$.

Example

Since $(4, 6) = 2$ then $2 = 4 \cdot 2 + 6(-1)$ where $x = 2$ and $y = -1$.

Theorem

The greatest common divisor of b and c can be characterized in the following ways:

1. *it is the least positive value of $bx + cy$ where x and y ranges over all integers;*
2. *it is the positive common divisor of b and c that is divisible by every common divisor.*

Definition

If $(a, b) = 1$ then a and b are **relatively prime** *and if $(a_1, a_2, \ldots, a_n) = 1$ then $a_1, a_2, \ldots, a_n$ are* **relatively prime**.

Theorem

The greatest common divisor of b and c can be characterized in the following ways:

1. *it is the least positive value of $bx + cy$ where x and y ranges over all integers;*
2. *it is the positive common divisor of b and c that is divisible by every common divisor.*

Definition

If $(a, b) = 1$ then a and b are **relatively prime** *and if $(a_1, a_2, \ldots, a_n) = 1$ then $a_1, a_2, \ldots, a_n$ are* **relatively prime**.

Divisibility of Integers

Theorem

The greatest common divisor of b and c can be characterized in the following ways:

1. *it is the least positive value of $bx + cy$ where x and y ranges over all integers;*
2. *it is the positive common divisor of b and c that is divisible by every common divisor.*

Definition

If $(a, b) = 1$ then a and b are **relatively prime** *and if $(a_1, a_2, \ldots, a_n) = 1$ then $a_1, a_2, \ldots, a_n$ are* **relatively prime**.

Divisibility of Integers

Theorem

The greatest common divisor of b and c can be characterized in the following ways:

1. *it is the least positive value of $bx + cy$ where x and y ranges over all integers;*
2. *it is the positive common divisor of b and c that is divisible by every common divisor.*

Definition

If $(a, b) = 1$ then a and b are **relatively prime** *and if $(a_1, a_2, \ldots, a_n) = 1$ then $a_1, a_2, \ldots, a_n$ are* **relatively prime**.

Divisibility of Integers

Note that If $(a, b) = 1$ then we can also say that a and b are **coprime**, or a is prime to b.

Example

$(2, 5) = (3, 5) = 1$ *then* $2, 3$ *and* 5 *are relatively prime.*

Theorem

If $c|ab$ *and* $(c, a) = 1$ *then* $c|b$.

Illustration

$3|66$ where $(3, 11) = 1$, then $3|6$.

Divisibility of Integers

Note that If $(a, b) = 1$ then we can also say that a and b are **coprime**, or a is prime to b.

Example

$(2, 5) = (3, 5) = 1$ *then* $2, 3$ *and* 5 *are relatively prime.*

Theorem

If $c|ab$ *and* $(c, a) = 1$ *then* $c|b$.

Illustration

$3|66$ where $(3, 11) = 1$, then $3|6$.

Note that If $(a, b) = 1$ then we can also say that a and b are **coprime**, or a is prime to b.

Example

$(2, 5) = (3, 5) = 1$ *then* $2, 3$ *and* 5 *are relatively prime.*

Theorem

If $c|ab$ *and* $(c, a) = 1$ *then* $c|b$.

Illustration

$3|66$ where $(3, 11) = 1$, then $3|6$.

Divisibility of Integers

Note that If $(a, b) = 1$ then we can also say that a and b are **coprime**, or a is prime to b.

Example

$(2, 5) = (3, 5) = 1$ *then* 2, 3 *and* 5 *are relatively prime.*

Theorem

If $c|ab$ *and* $(c, a) = 1$ *then* $c|b$.

Illustration

$3|66$ where $(3, 11) = 1$, then $3|6$.

Theorem

The Euclidean Algorithm. *Given integers b and $c > 0$, we make a repeated application of the division algorithm to obtain a series of equations,*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} + 0. \end{aligned}$$

Then $(b, c) = r_j$, the last nonzero remainder in the division process. Values of x and y in $(b, c) = bx + cy$ can be obtained by writing each r_i as a linear combination of b and c.

Divisibility of Integers

Example

Find (963,657).

$$
\begin{aligned}
963 &= 657(1) + 306 \quad (1)\\
657 &= 306(2) + 45 \quad (2)\\
306 &= 45(6) + 36 \quad (3)\\
45 &= 36(1) + 9 \quad (4)\\
36 &= 9(4) + 0 \quad (5)
\end{aligned}
$$

Hence, (963,657)=9.

Divisibility of Integers

Example

Find x, y *such that* $9 = 963x + 657y$.

$$\begin{array}{rcll} 9 & = & 45 - 36 & \textit{from equation } 4 \\ & = & 45 - (306 - 45(6)) & \textit{from equation } 3 \\ & = & 45(7) - 306 & \\ & = & [657 - 306(2)](7) - 306 & \textit{from equation } 2 \\ & = & 657(7) - 306(15) & \\ & = & 657(7) - (963 - 657)(15) & \textit{from equation } 1 \\ & = & 963(-15) + 657(22) & \end{array}$$

Hence, $x = -15$ *and* $y = 22$

Divisibility of Integers

Theorem

If $p|ab$ where p is a prime, then $p|a$ or $p|b$. Generally, if $p|a_1 a_2 \ldots a_n$ then $p|a_i$ for some i.

Illustration

$11|(2 \cdot 121)$ *implies that* $11|121$ *since* $(2, 11) = 1$ *and* $5|(4 \cdot 9 \cdot 25)$ *implies that* $5|25$.

Divisibility of Integers

Theorem

If $p|ab$ where p is a prime, then $p|a$ or $p|b$. Generally, if $p|a_1a_2\ldots a_n$ then $p|a_i$ for some i.

Illustration

$11|(2\cdot 121)$ *implies that* $11|121$ *since* $(2,11)=1$ *and* $5|(4\cdot 9\cdot 25)$ *implies that* $5|25$.

Equivalence Relations

Let S be a non-empty set. A relation on S is a statement about pairs of elements of S, which may be true for some pairs and false for others. For example, if $S = \mathbb{R}$, the statement $a \leq b$ is true for some choices of a and b (e.g. $a = 1, b = 3$) and false for others (e.g. $a = 5, b = 2$). We usually use $\sim$ to stand for a relation, and we write "$a \sim b$ " to mean "a is related to b under the relation $\sim$", and "$a \not\sim b$ " to mean "a is not related to b under the relation $\sim$"; thus for the relation of "less than or equal to" on $\mathbb{R}$ we have $2 \sim 7$ and $6 \not\sim 3$.

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a and b are related this way we say that they are **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Definition

An **equivalence relation** $\sim$ *on a set* S *is a relation that is:*

1. *Reflexive.*
   $a \sim a$ *for all* $a \in S$.
2. *Symmetric.*
   Whenever $a \sim b$, *then* $b \sim a$.
3. *Transitive.*
   If $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

If a *and* b *are related this way we say that they are* **equivalent** *under* $\sim$. *If* $a \in S$, *then the set of all elements of* S *that are equivalent to* a *is called the* **equivalence class** *of* a *denoted by* $[a]$. *In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Equivalence Relations

Example

Let $S = \{$ Algebra students $\}$, and let $a \sim b$ if a is in the same college as b. Clearly $\sim$ is reflexive since each Algebra student is in the same college as himself or herself. $\sim$ is also symmetric since if a is in the same college as b then b is in the same college as a. Lastly, $\sim$ is transitive since if a is in the same college as b, who is in the same college as c, then clearly a is in the same college as c. Therefore, $\sim$ is an equivalence relation on S. The equivalence class of a is the set of all Algebra students in the same college as a.

Equivalence Relations

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Equivalence Relations

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Equivalence Relations

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Equivalence Relations

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Equivalence Relations

Example

Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

1. *Reflexive.*
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.
2. *Symmetric.*
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

Equivalence Relations

Example

Let $S = \{(a, b) | a, b \in \mathbb{Z}^+\}$*, and let* $(a, b) \sim (c, d)$ *if* $a + d = b + c$*. Is* $\sim$ *an equivalence relation on* S*?*

Equivalence Relations

Example

Under the relation $\sim$ in the set $S = \{(a, b) | a, b \in \mathbb{Z}^+\}$, where $(a, b) \sim (c, d)$ if $a + d = b + c$, the equivalence classes are as follows:

$$
\begin{aligned}
[(1,1)] &= \{(a,b) | (a,b) \sim (1,1)\} \\
&= \{(a,b) | a + 1 = b + 1\} \\
&= \{(a,b) | a = b\} \\
&= \{(a,a) | a \in \mathbb{Z}^+\} \\
[(1,2)] &= \{(a,b) | (a,b) \sim (1,2)\} \\
&= \{(a,b) | a + 2 = b + 1\} \\
&= \{(a,b) | a + 1 = b\} \\
&= \{(a,a+1) | a \in \mathbb{Z}^+\} \\
&\vdots \\
[(1,n)] &= \{(a,b) | (a,b) \sim (1,n)\} \\
&= \{(a,b) | a + n = b + 1\} \\
&= \{(a,b) | a + (n-1) = b\} \\
&= \{(a,a+(n-1)) | a \in \mathbb{Z}^+\}
\end{aligned}
$$

Equivalence Relations

Example

$$
\begin{aligned}
[(2,1)] &= \{(a,b) \mid (a,b) \sim (2,1)\} \\
&= \{(a,b) \mid a+1 = b+2\} \\
&= \{(a,b) \mid a = b+1\} \\
&= \{(b+1,b) \mid b \in \mathbb{Z}^+\} \\
[(3,1)] &= \{(a,b) \mid (a,b) \sim (3,1)\} \\
&= \{(a,b) \mid a+1 = b+3\} \\
&= \{(a,b) \mid a = b+2\} \\
&= \{(b+2,b) \mid b \in \mathbb{Z}^+\} \\
&\vdots \\
[(n,1)] &= \{(a,b) \mid (a,b) \sim (n,1)\} \\
&= \{(a,b) \mid a+1 = b+n\} \\
&= \{(a,b) \mid a = b+(n-1)\} \\
&= \{(b+(n-1)), b \mid b \in \mathbb{Z}^+\}
\end{aligned}
$$

Partition

Definition

Let S be a set. A family $S_i, i = 1, \ldots n$ of subsets of S is called a **partition** *of S if the following are satisfied:*

1. $S_i \neq \emptyset$ for all i, $i = 1, \ldots, n$
2. $S_i \cap S_j = \emptyset$ for all $i \neq j$
3. $\bigcup_{i=1}^{n} S_i = S$

Partition

Definition

Let S be a set. A family $S_i, i = 1, \ldots n$ of subsets of S is called a **partition** *of S if the following are satisfied:*

1. $S_i \neq \emptyset$ *for all* $i, i = 1, \ldots n$
2. $S_i \cap S_j = \emptyset$ *for all* $i \neq j$
3. $\bigcup_{i=1}^{n} S_i = S$

Partition

Definition

Let S be a set. A family $S_i, i = 1, \ldots n$ of subsets of S is called a **partition** *of S if the following are satisfied:*

1. $S_i \neq \emptyset$ *for all* $i, i = 1, \ldots n$
2. $S_i \cap S_j = \emptyset$ *for all* $i \neq j$
3. $\bigcup_{i=1}^{n} S_i = S$

Partition

Definition

Let S be a set. A family $S_i, i = 1, \ldots n$ of subsets of S is called a **partition** *of S if the following are satisfied:*

1. $S_i \neq \emptyset$ *for all* $i, i = 1, \ldots n$
2. $S_i \cap S_j = \emptyset$ *for all* $i \neq j$
3. $\displaystyle\bigcup_{i=1}^{n} S_i = S$

Partition

Example

The equivalence classes in the previous examples partition the set S.

Remark

Any equivalence relation on S gives a partition of S and any partition gives rise to an equivalence relation by defining $a \sim b$ if and only if a and b belong to the same subset.

Partition

Example

The equivalence classes in the previous examples partition the set S.

Remark

Any equivalence relation on S gives a partition of S and any partition gives rise to an equivalence relation by defining $a \sim b$ if and only if a and b belong to the same subset.

Modular Arithmetic

Definition

Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, **a is congruent to b modulo n** *if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example

1. $21 \equiv 9 (\mathrm{mod}\ 4)$ *because* $21 = (5)(4) + 1$ *and* $9 = (2)(4) + 1$ *or equivalently* $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0 (\mathrm{mod}\ 5)$ *because* $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16 (\mathrm{mod}\ 3)$ *because* $1 - 16 = -15 = (-5)(3)$.

Modular Arithmetic

Definition

Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, ***a is congruent to b modulo n*** *if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example

1. $21 \equiv 9 \pmod 4$ *because* $21 = (5)(4) + 1$ *and* $9 = (2)(4) + 1$ *or equivalently* $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0 \pmod 5$ *because* $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16 \pmod 3$ *because* $1 - 16 = -15 = (-5)(3)$.

Modular Arithmetic

Definition

Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, **a is congruent to b modulo n** *if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example

1. $21 \equiv 9 \pmod 4$ *because* $21 = (5)(4) + 1$ *and* $9 = (2)(4) + 1$ *or equivalently* $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0 \pmod 5$ *because* $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16 \pmod 3$ *because* $1 - 16 = -15 = (-5)(3)$.

Modular Arithmetic

Definition

*Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, **a is congruent to b modulo n** if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example

1. $21 \equiv 9 \pmod 4$ *because* $21 = (5)(4) + 1$ *and* $9 = (2)(4) + 1$ *or equivalently* $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0 \pmod 5$ *because* $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16 \pmod 3$ *because* $1 - 16 = -15 = (-5)(3)$.

Definition

Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, **a is congruent to b modulo n** *if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example

1. $21 \equiv 9 \pmod 4$ *because* $21 = (5)(4) + 1$ *and* $9 = (2)(4) + 1$ *or equivalently* $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0 \pmod 5$ *because* $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16 \pmod 3$ *because* $1 - 16 = -15 = (-5)(3)$.

Modular Arithmetic

Theorem

The relation congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Example

If we take n=5, we obtain the following congruence classes:

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

We have $[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$, and the intersection of any two of these classes is empty.

Modular Arithmetic

Theorem

The relation congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Example

If we take n=5, we obtain the following congruence classes:

$$
\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}
$$

We have $[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$, and the intersection of any two of these classes is empty.