Modular Arithmetic

Ian Ludden

Learning Objectives

By the end of this lesson, you will be able to:

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definition of congruence modulo n and equivalence classes ($\mathbb{Z}_n$).

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definition of congruence modulo n and equivalence classes ($\mathbb{Z}_n$).
- Compare elements of $\mathbb{Z}_n$.

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definition of congruence modulo n and equivalence classes ($\mathbb{Z}_n$).
- Compare elements of $\mathbb{Z}_n$.
- Perform modular arithmetic (efficiently) by hand.

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.
For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.

$\exists m \in \mathbb{Z} \quad (a-b) = m \cdot n$

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.
For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.
Equivalent condition: $a = b + \underline{kn}$ for some $k \in \mathbb{Z}$.

$a - b = kn$

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.

For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.

Equivalent condition: $a = b + kn$ for some $k \in \mathbb{Z}$.

Shorthand: $a \equiv b \pmod{n}$.

"mod"

equivalence

$a \equiv b \pmod{n}$

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.
For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.
Equivalent condition: $a = b + kn$ for some $k \in \mathbb{Z}$.
Shorthand: $a \equiv b \pmod{n}$.

Examples

- $3 \equiv 13 \pmod{2}$ $\quad 3-13=-10$ and $2 \mid (-10)$

$13 \% 2 == 1$

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.
For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.
Equivalent condition: $a = b + kn$ for some $k \in \mathbb{Z}$.
Shorthand: $a \equiv b \pmod{n}$.

Examples

- $3 \equiv 13 \pmod{2}$
- $-4 \not\equiv 4 \pmod{6}$

$(-4-4) = -8$ $\qquad 6 \nmid (-8)$

Congruence modulo n

Definition

Let $n \in \mathbb{Z}$, $n > 1$.
For $a, b \in \mathbb{Z}$, we say that a ***is congruent to*** b ***modulo*** n if $n \mid (a - b)$.
Equivalent condition: $a = b + kn$ for some $k \in \mathbb{Z}$.
Shorthand: $a \equiv b \pmod{n}$.

Examples

- $3 \equiv 13 \pmod{2}$
- $-4 \not\equiv 4 \pmod{6}$
- $-4 \equiv 24 \pmod{7}$

$-4 - 24 = -28$

$7 \mid (-28)$

Equivalence Classes

Definition

The ***equivalence class*** of $m \pmod{n}$ is the set of all integers congruent to m mod n (including m), written $[m]$.

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \ldots\}$

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \dots\}$
- $[1] = \{1, 6, 11, 16, 21, 26, -4, -9, \dots\}$

$-4 = 5 \cdot (-1) + 1$

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \ldots\}$
- $[1] = \{1, 6, 11, 16, 21, 26, -4, -9, \ldots\}$
- $[2] = \{2, 7, 12, 17, -3, -48, 32, \ldots\}$

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \ldots\}$
- $[1] = \{1, 6, 11, 16, 21, 26, -4, -9, \ldots\}$
- $[2] = \{2, 7, 12, 17, -3, -48, 32, \ldots\}$
- $[3] = \{-12, 33, 8, 3, -2, \ldots\}$

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \ldots\}$
- $[1] = \{1, 6, 11, 16, 21, 26, -4, -9, \ldots\}$
- $[2] = \{2, 7, 12, 17, -3, -48, 32, \ldots\}$
- $[3] = \{-12, 33, 8, 3, -2, \ldots\}$
- $[4] = \{-6, -1, 4, 9, \ldots\}$

Equivalence Classes

Definition

The ***equivalence class*** of m (mod n) is the set of all integers congruent to m mod n (including m), written $[m]$.
Equivalent definition: the set of all integers with the same remainder as m when divided by n.

Examples

Fix $n = 5$. Then,

- $[0] = \{0, 5, 10, 15, 20, 25, -5, -10, 30, \ldots\}$
- $[1] = \{1, 6, 11, 16, 21, 26, -4, -9, \ldots\}$
- $[2] = \{2, 7, 12, 17, -3, -48, 32, \ldots\}$
- $[3] = \{-12, 33, 8, 3, -2, \ldots\}$
- $[4] = \{-6, -1, 4, 9, \ldots\}$
- $[-7] = \{-7, -2, 3, 8, \ldots\} = [3]$

$a, b \in \mathbb{Z}$

$a \in [b] \longleftrightarrow [a] = [b]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

$\mathbb{Z}$, $+$, $/$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

Rules

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

$n = 5$

Rules

Addition: $[a] + [b] = [a + b]$

$[1] + [3] = [1+3] = [4]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

$n=5$

$[1]\cdot[4] = [1\cdot 4] = [4]$

Rules

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

$-5\ \boxed{-4}\ -3\ -2\ -1\ 0\ \boxed{1}\ 2\ 3\ 4\ 5\ \boxed{6}\ 7 \ldots$

$[0] = [5] = [-105]$

0's family 5's family -105's family

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

Rules

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

Examples

Fix $n = 7$.

$a = b + kn$

- $[3] + [5] = [8] = [1]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

<u>Rules</u>

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

Examples

Fix $n = 7$.

- $[3] + [5] = [8] = [1]$
- $[2] - [4] = [-2] = [5]$

$[2] + [-4] = [2 + (-4)]$

$= [-2]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

<u>Rules</u>

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

Examples

Fix $n = 7$.

- $[3] + [5] = [8] = [1]$
- $[2] - [4] = [-2] = [5]$
- $[4] \cdot [3] = [12] = [5]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

Rules

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

Examples

Fix $n = 7$.

- $[3] + [5] = [8] = [1]$
- $[2] - [4] = [-2] = [5]$
- $[4] \cdot [3] = [12] = [5]$
- $[51] \cdot [-4] = [2] \cdot [3] = [6]$

-204

210

$[49+2]$

Definition

For a fixed integer $n > 1$, the collection of sets $\{[0], [1], \ldots, [n-1]\}$ along with the following rules for arithmetic is called ***the integers modulo*** n, written $\mathbb{Z}_n$.

$x^4 = x \cdot x \cdot x \cdot x$

Rules

Addition: $[a] + [b] = [a + b]$

Multiplication: $[a] \cdot [b] = [a \cdot b]$

$[6] \cdot [6] \cdot [6] \cdot [6] \cdot \ldots \cdot [6]$

Examples

Fix $n = 7$.

$(-1)^{2k} = 1 \qquad (-1)^{2k+1} = -1$

- $[3] + [5] = [8] = [1]$
- $[2] - [4] = [-2] = [5]$
- $[4] \cdot [3] = [12] = [5]$
- $[51] \cdot [-4] = [2] \cdot [3] = [6]$
- $[6]^{173} = [-1]^{173} = [(-1)^{173}] = [-1] = [6]$

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definition of congruence modulo n and equivalence classes ($\mathbb{Z}_n$).
- Compare elements of $\mathbb{Z}_n$.
- Perform modular arithmetic (efficiently) by hand.