Integers Modulo n

Carmen M. Wright, Ph.D.

Jackson State University

2017

FACT: If you divide a number by a number smaller than its absolute value, you will get either a zero or positive remainder.

$$22/7 \to 22 = 3 \cdot 7 + 1$$

$$45/9 \to 45 = 5 \cdot 9 + 0$$

$$-17/5 \to -17 = (-4) \cdot 5 + 3$$

Division Algorithm

Theorem

Division Algorithm. *Let n and $d \geq 1$ be integers. There exist uniquely determined integers q and r such that*

$$n = qd + r \qquad \textit{and} \qquad 0 \leq r < d.$$

Division Algorithm (cont.)

Note: q is called the quotient; r is called the remainder

e.g.

$$22/7 \to 22 = 3 \cdot 7 + 1$$

So $n = 22$,

$$q = 3 \text{ is the quotient,}$$
$$d = 7 \text{ is the divisor,}$$
$$r = 1 \text{ is the remainder.}$$

Case: When $r = 0$ in $n = qd + r$, or $n = qd$.

Definition

Let d and n be in $\mathbb{Z}$. Then $d|n$ means that there exists an q in $\mathbb{Z}$ such that $n = qd$. The following are equivalent statements:

Case: When $r = 0$ in $n = qd + r$, or $n = qd$.

Definition

Let d and n be in $\mathbb{Z}$. Then $d|n$ means that there exists an q in $\mathbb{Z}$ such that $n = qd$. The following are equivalent statements:

1. d is a **divisor** (or **integral divisor**, or **factor**) of n in $\mathbb{Z}$.

Case: When $r = 0$ in $n = qd + r$, or $n = qd$.

Definition

Let d and n be in $\mathbb{Z}$. Then $d|n$ means that there exists an q in $\mathbb{Z}$ such that $n = qd$. The following are equivalent statements:

1. d is a **divisor** (or **integral divisor**, or **factor**) of n in $\mathbb{Z}$.
2. n is a **multiple** (or **integral multiple**) of d in $\mathbb{Z}$.

e.g. $5|25$, $7|21$, $3 \nmid 5$

Also, $1|n$ and $n|0$ for all integers n.

Congruence modulo n

Let $n \geq 2$.
The integers a and b are said to be **congruent modulo** n if $n|(a-b)$. In this case we write $a \equiv b \pmod{n}$ and refer to n as the **modulus**.

Congruence modulo n

Let $n \geq 2$.
The integers a and b are said to be **congruent modulo** n if $n|(a-b)$. In this case we write $a \equiv b \pmod{n}$ and refer to n as the **modulus**.
It is related to the idea of the division algorithm: $a = nq + b$ is equivalent to $a - b = nq$, and indeed $n|(a-b)$.

Let $n \geq 2$.
The integers a and b are said to be **congruent modulo** n if $n|(a-b)$. In this case we write $a \equiv b \pmod{n}$ and refer to n as the **modulus**.
It is related to the idea of the division algorithm: $a = nq + b$ is equivalent to $a - b = nq$, and indeed $n|(a-b)$.

$$5 \equiv 8 \pmod{3}$$

$$20 \equiv 1 \pmod{19}$$

$$-5 \equiv 15 \pmod{10}$$

Congruence modulo n (cont.)

The congruence modulo n relation is an equivalence relation on $\mathbb{Z}$. That is, for any $a, b, c \in \mathbb{Z}$,

The congruence modulo n relation is an equivalence relation on $\mathbb{Z}$. That is, for any $a, b, c \in \mathbb{Z}$,

- $a \equiv a \pmod{n}$

The congruence modulo n relation is an equivalence relation on $\mathbb{Z}$. That is, for any $a, b, c \in \mathbb{Z}$,

- $a \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

The congruence modulo n relation is an equivalence relation on $\mathbb{Z}$. That is, for any $a, b, c \in \mathbb{Z}$,

- $a \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

If a is an integer, its equivalence class $[a]$ with respect to congruence modulo n is called its **residue class modulo** n, and we write for convenience:

$$\overline{a} = [a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}.$$

If a is an integer, its equivalence class $[a]$ with respect to congruence modulo n is called its **residue class modulo** n, and we write for convenience:

$$\bar{a} = [a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}.$$

Example For $n = 2$, there are two equivalence classes:

$$\bar{0} = [0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\}$$

$$\bar{1} = [1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\}$$

the even and odd integers, respectively.

Example For $n = 4$, there are four equivalence classes:

$$\overline{0} = [0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 4\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$

$$\overline{1} = [1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 4\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$

$$\overline{2} = [2] = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$

$$\overline{3} = [3] = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 4\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

Theorem

Given $n \geq 2$, $\overline{a} = \overline{b}$ *if and only if* $a \equiv b \pmod{n}$.

Theorem

Given $n \geq 2$, $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{n}$.

Note: For ease of notation, we will write $a \equiv b$ to mean $a \equiv b \pmod{n}$.

Proof:

Since this is "if and only if", there are two statements to prove.

Proof:

Since this is "if and only if", there are two statements to prove.

- Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.

Proof:

Since this is "if and only if", there are two statements to prove.

- Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
- Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.

Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then $x \equiv a$; so, as $a \equiv b$, we have

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then $x \equiv a$; so, as $a \equiv b$, we have $x \equiv b$ (by

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then $x \equiv a$; so, as $a \equiv b$, we have $x \equiv b$ (by transitivity) and hence $x \in \overline{b}$. This proves that $\overline{a} \subseteq \overline{b}$.

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then $x \equiv a$; so, as $a \equiv b$, we have $x \equiv b$ (by transitivity) and hence $x \in \overline{b}$. This proves that $\overline{a} \subseteq \overline{b}$. Since $b \equiv a$ (by symmetry),

Proof:

Recall, by definition

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}.$$

Statement 1: If $\overline{a} = \overline{b}$, then $a \equiv b$.
Suppose $\overline{a} = \overline{b}$. Since $a \in \overline{a}$, we have $a \in \overline{b}$, so $a \equiv b$.

Statement 2: If $a \equiv b$, then $\overline{a} = \overline{b}$.
Conversely, let $a \equiv b$. Since $\overline{a}$ and $\overline{b}$ are sets, we must show $\overline{a} \subseteq \overline{b}$ and $\overline{b} \subseteq \overline{a}$.
If $x \in \overline{a}$, then $x \equiv a$; so, as $a \equiv b$, we have $x \equiv b$ (by transitivity) and hence $x \in \overline{b}$. This proves that $\overline{a} \subseteq \overline{b}$. Since $b \equiv a$ (by symmetry), the proof is similar to show $\overline{b} \subseteq \overline{a}$.

Theorem

Let $n \geq 2$ be an integer.

1. *If $a \in \mathbb{Z}$, then $\overline{a} = \overline{r}$ for some r where $0 \leq r \leq n-1$.*
2. *The residue classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ modulo n are distinct.*

The set of all residue classes module n is denoted

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

and is called the set of **integers modulo** n.

Theorem

Let $n \geq 2$ be an integer.

1. *If $a \in \mathbb{Z}$, then $\overline{a} = \overline{r}$ for some r where $0 \leq r \leq n-1$.*
2. *The residue classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ modulo n are distinct.*

The set of all residue classes module n is denoted

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

and is called the set of **integers modulo** n.

- In $\mathbb{Z}_3$: $\overline{4} = \overline{1}, \quad \overline{-6} = \overline{0}, \quad \overline{29} = \overline{2}, \quad \overline{3} = \overline{0}.$

Theorem

Let $n \geq 2$ be an integer.

1. *If $a \in \mathbb{Z}$, then $\overline{a} = \overline{r}$ for some r where $0 \leq r \leq n-1$.*
2. *The residue classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ modulo n are distinct.*

The set of all residue classes module n is denoted

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

and is called the set of **integers modulo** n.

- In $\mathbb{Z}_3$: $\overline{4} = \overline{1}$, $\overline{-6} = \overline{0}$, $\overline{29} = \overline{2}$, $\overline{3} = \overline{0}$.
- In $\mathbb{Z}_{11}$: $\overline{16} = \overline{5}$, $\overline{-20} = \overline{2}$.

Adding and multiplying congruence module n:
Let $a, a_1, b, b_1 \in \mathbb{Z}$. If

$$a \equiv a_1 \pmod{n}$$
$$b \equiv b_1 \pmod{n}$$

Adding and multiplying congruence module n:
Let $a, a_1, b, b_1 \in \mathbb{Z}$. If

$$a \equiv a_1 \pmod{n}$$
$$b \equiv b_1 \pmod{n}$$

then

$$a + b \equiv a_1 + b_1 \pmod{n}$$
$$ab \equiv a_1 b_1 \pmod{n}$$

Hence, the arithmetic of $\mathbb{Z}$ extends naturally to $\mathbb{Z}_n$ as follows:

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a}\,\overline{b} = \overline{ab}$$

These operations are well-defined, that is, they do not depend on which generators are used for the residue classes $\overline{a}$ and $\overline{b}$.

Example: Operations in $\mathbb{Z}_9$

$$\overline{8} + \overline{7} = \overline{15} = \overline{6} \qquad \text{since} \qquad 15 \equiv 6 \pmod 9$$

$$\overline{8} \cdot \overline{7} = \overline{56} = \overline{2} \qquad \text{since} \qquad 56 \equiv 2 \pmod 9$$

Notational convention: When working in $\mathbb{Z}_n$ we frequently write the residue class $\overline{a}$ as a. When there is confusion, we revert to the formal $\overline{a}$ notation.

Properties of $+$ and $\cdot$ in $\mathbb{Z}_n$

Theorem

- $\overline{a} + \overline{b} = \overline{a+b}$ *and* $\overline{a}\overline{b} = \overline{ab}$.
- $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ *and* $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$
- $\overline{a} + \overline{0} = \overline{a}$ *and* $\overline{a}\overline{1} = \overline{a}$
- $\overline{a} + \overline{-a} = \overline{0}$
- $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$

Note: $\overline{-a} = -\overline{a}$, *so subtraction in* $\mathbb{Z}_n$ *is defined by*

$$\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a-b}$$

$\mathbb{Z}$ versus $\mathbb{Z}_n$

- In $\mathbb{Z}$, $ab = 0$ implies $a = 0$ or $b = 0$.
- In $\mathbb{Z}_n$, $\overline{a} \cdot \overline{b} = \overline{0}$ does not imply $\overline{a} = 0$ or $\overline{b} = \overline{0}$.
- For example, in $\mathbb{Z}_6$, $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

$\mathbb{Z}$ versus $\mathbb{Z}_n$

- In $\mathbb{Z}$, $ab = 0$ implies $a = 0$ or $b = 0$.
- In $\mathbb{Z}_n$, $\overline{a} \cdot \overline{b} = \overline{0}$ does not imply $\overline{a} = 0$ or $\overline{b} = \overline{0}$.
- For example, in $\mathbb{Z}_6$, $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

- In $\mathbb{Z}$, for $a \neq 0$, $ab = ac$ implies $b = c$.
- In $\mathbb{Z}_n$, $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ does not imply $\overline{b} = \overline{c}$.
- For example, in $\mathbb{Z}_6$, $\overline{4} \neq \overline{0}$, and $\overline{4} \cdot \overline{2} = \overline{4} \cdot \overline{5}$ even though $\overline{2} \neq \overline{5}$.

Find the inverse of $\overline{16}$ in $\mathbb{Z}_{35}$ and use it to solve $\overline{16}x = \overline{9}$ in $\mathbb{Z}_{35}$.

By trial and error, we find that $\overline{11} \cdot \overline{16} = \overline{1}$ in $\mathbb{Z}_{35}$. Then $\overline{11}$ and $\overline{16}$ are inverses of each other. Then

$$\begin{aligned} \overline{16}x &= \overline{9} \\ \overline{11} \cdot \overline{16}x &= \overline{11} \cdot \overline{9} \\ \overline{1}x &= \overline{99} \\ x &= \overline{29} \end{aligned}$$

But is there a better way to find inverses? Maybe not every element has an inverse and we can ignore those.

Relatively prime

Definition

The integers m and n are said to be relatively prime if they have no common divisors.

- 3, 4
- 7, 9
- 4, 9
- 6, 35

For $n \geq 2$ and an integer a, a residue class $\overline{b}$ in $\mathbb{Z}_n$ is called an **inverse** of $\overline{a}$ if $\overline{b}\overline{a} = \overline{1}$ in $\mathbb{Z}_n$. If $\overline{a}$ has an inverse, that inverse is unique and we say $\overline{a}$ is **invertible**.

Theorem

Let a and n be integers with $n \geq 2$. Then $\overline{a}$ has an inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

For $n \geq 2$ and an integer a, a residue class $\overline{b}$ in $\mathbb{Z}_n$ is called an **inverse** of $\overline{a}$ if $\overline{b}\overline{a} = \overline{1}$ in $\mathbb{Z}_n$. If $\overline{a}$ has an inverse, that inverse is unique and we say $\overline{a}$ is **invertible**.

Theorem

Let a and n be integers with $n \geq 2$. Then $\overline{a}$ has an inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

Exercise: Find the elements in $\mathbb{Z}_9$ that have inverses. What are their inverses?

Exercise I

1. We know that $(a+b)^2 \neq a^2 + b^2$ for all integers a and b. Now prove the equality holds in $\mathbb{Z}_2$, i.e.$(a+b)^2 = a^2 + b^2$ when a and b are elements in $\mathbb{Z}_2$.
2. Prove: If $a \equiv a_1 \pmod{n}$ and $a \equiv b_1 \pmod{n}$, then $a + b \equiv a_1 + b_1 \pmod{n}$ and $ab \equiv a_1 b_1 \pmod{n}$.
3. When the positive integer P is divided by 7, the remainder is 5. What is the remainder when $5P$ is divided by 7?
4. If $a \equiv b \pmod{n}$ and $m|n$, show that $a \equiv b \pmod{m}$.
5. Find the remainder when 7^{112} is divided by 5.