Congruences of Integers

Contents

Congruences

Definitions

Definition 1 (Congruences)

Let a, b, and m be integers. To say that a *is congruent to* b *modulo* m (written $a \equiv b \mod m$) means that m divides $b - a$.

- Let $x, m \in \mathbb{Z}$. Then $x \equiv 0 \mod m$ iff m divides x.
- For each integer x,

$$\text{“}x \text{ is even.”} \iff x \equiv 0 \mod 2$$
$$\text{“}x \text{ is odd.”} \iff x \equiv 1 \mod 2$$

- For all integers a and b, $a \equiv b \mod 0$ iff $a = b$.

Congruences as Relation

Theorem 2 (Congruence Is An Equivalence Relation)

Let $m \in \mathbb{Z}$. The relation of congruence modulo m satisfies the following properties:

1. *(Reflexivity) For each $a \in \mathbb{Z}$, $a \equiv a \mod m$.*
2. *(Symmetry) For all $a, b \in \mathbb{Z}$, if $a \equiv b \mod m$, then $b \equiv a \mod m$.*
3. *(Transitivity) For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.*

Balancing Congruences

Theorem 3 (Preserving Congruences)

Let $m, a_1, b_1, a_2, b_2 \in \mathbb{Z}$. *Suppose that* $a_1 \equiv b_1 \mod m$ *and* $a_2 \equiv b_2 \mod m$. *Then*

1. $a_1 + a_2 \equiv b_1 + b_2 \mod m$.
2. $a_1 a_2 \equiv b_1 b_2 \mod m$.

Interesting Behavior of Congruences

Let $m \in \mathbb{Z}$. Congruence modulo m shares many similarities with equality as seen in the previous slides. Differences?

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

- If $ab = 0$, then $a = 0$ or $b = 0$. (True)
- If $ab \equiv 0 \mod m$, then $a \equiv 0 \mod m$ or $b \equiv 0 \mod m$. (Not always true)

Let $u, v, w \in \mathbb{Z}$.

- If $w \neq 0$ and $uw = vw$, then $u = v$. (True)
- If $w \not\equiv 0$ and $uw \equiv vw \mod m$, then $u \equiv v \mod m$. (Not always true)

Question. For which m values is the second sentence in each paragraph true?

When m Is Prime

When m Is Prime

Let m be prime.

1. Let $a, b \in \mathbb{Z}$ such that $ab \equiv 0 \mod m$. Then $a \equiv 0 \mod m$ or $b \equiv 0 \mod m$.
2. Let $u, v, w \in \mathbb{Z}$ such that $w \not\equiv 0 \mod m$ and $uw \equiv vw \mod m$. Then $u \equiv w \mod m$.

Congruence Classes

Example. ($m = 2$) For each $x \in \mathbb{Z}$, $x \equiv 0 \mod 2$ or $x \equiv 1 \mod 2$:

- $x \equiv 0 \mod 2$: $\dots, -4, -2, 0, 2, 4, \dots$
- $x \equiv 1 \mod 2$: $\dots, -3, -1, 1, 3, \dots$

These two sets of integers are called the *congruence classes modulo 2*. Each integer belongs to exactly one of the two congruence classes.

Example. ($m = 3$) For each $x \in \mathbb{Z}$,

- $x \equiv 0 \mod 3$: $\dots, -9, -6, -3, 0, 3, 6, 9, \dots$
- $x \equiv 1 \mod 3$: $\dots, -8, -5, -2, 1, 4, 7, 10, \dots$
- $x \equiv 2 \mod 3$: $\dots, -7, -4, -1, 2, 5, 8, 11, \dots$

These three sets of integers are called the *congruence classes modulo 3*. Each integer belongs to exactly one of the three congruence classes.

Division Lemma

The Division Lemma (Euclid)

Let $m \in \mathbb{N}$. For each $x \in \mathbb{Z}$, there exists a unique $k \in \mathbb{Z}$ and a unique $r \in \{0, \ldots, m-1\}$ such that $x = mk + r$.

Using the division lemma, one can show that two integers x_1 and x_2 belong to the same congruence class modulo m if and only if they yield the same remainder upon division by m.

Congruence Class Criterion

Example 4

Let $m \in \mathbb{N}$, $x_1, x_2 \in \mathbb{Z}$, $k_1, k_2 \in \mathbb{Z}$, and $r_1, r_2 \in \{0, \ldots, m-1\}$ such that $x_1 = mk_1 + r_1$ and $x_2 = mk_2 + r_2$. Then $x_1 \equiv x_2 \mod m$ iff $r_1 = r_2$.