Congruences of Integers

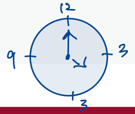
Contents

Congruences

Overview Section 4 (mathematical proofs)

- even and odd #'s
- rational and irrational #'s
- divisibility and prime numbers
- Congruences of integers

Definitions



Example $m = 12$

$4 \equiv 16 \mod 12$ because $12 \mid (16-4)$

Definition 1 (Congruences)

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

Example $m = 2$.

$0 \equiv 0 \mod 2$

$1 \equiv 1 \mod 2$

$2 \equiv 0 \mod 2$

$3 \equiv 1 \mod 2$

$4 \equiv 0 \mod 2$

$\vdots$

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

  $x \equiv 0 \mod m$ iff $m \mid (0 - x)$ iff $m \mid x$

  $(\exists k \in \mathbb{Z})(-x = km)$

  $x = -km = (-k)m$

- 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 $a = b$.

  $a \equiv b \mod 0$ iff $0 \mid (b - a)$ iff $b - a = 0$ iff $a = b$.

Congruences as Relation

Equality (=)

- $(\forall a)(a = a)$
- $(\forall a, b)(a=b \Rightarrow b=a)$
- $(\forall a,b,c)[(a=b) \wedge (b=c) \Rightarrow a=c]$

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 $a \equiv c \mod m$.*

HW

Proof of ①: Let $a \in \mathbb{Z}$ be arbitrary. Then m divides $a - a = 0$.

Hence $a \equiv a \mod m$.

Balancing Congruences

Equality $(=)$ $\quad a=b$

- $a+c=b+c$
- $ac=bc$

$a_1=b_1, \quad a_2=b_2$

- $a_1+a_2=b_1+b_2$
- $a_1a_2=b_1b_2$

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. $a_1a_2 \equiv b_1b_2 \mod m$.

Proof of ①: Since $a_1 \equiv b_1 \bmod m$, $m \mid (b_1-a_1)$, so

$$b_1 - a_1 = km \quad \text{for some } k \in \mathbb{Z}.$$

Since $a_2 \equiv b_2 \bmod m$, $m \mid (b_2-a_2)$, so

$$b_2 - a_2 = lm \quad \text{for some } l \in \mathbb{Z}.$$

Then

$$\begin{aligned}(b_1+b_2)-(a_1+a_2) &= b_1 + (b_2-a_1) - a_2 \\ &= b_1 + (-a_1+b_2) - a_2 \\ &= (b_1-a_1)+(b_2-a_2) \\ &= km + lm = (k+l)m.\end{aligned}$$

Since $k+l$ is an integer, $m \mid [(b_1+b_2)-(a_1+a_2)]$.

Hence,

$$a_1+a_2 \equiv b_1+b_2 \bmod m.$$

$\square$

Interesting Behavior of Congruences

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

Recall: $x \equiv 0 \mod m$ iff $m \mid x$.

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)

"there are values of m for which this is false."

$m = 6$ $\quad 2 \cdot 3 \equiv 0 \mod m$, but $2 \not\equiv 0 \mod m$ and $3 \not\equiv 0 \mod m$.

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

- 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)

$m = 6$ $\quad 5 \cdot 3 \equiv 7 \cdot 3 \mod m$, but $5 \not\equiv 7 \mod m$.

(because $21 - 15 = 6$, which is divisible by m).

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

Remark 4.50. Let p be prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

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 $u \equiv w \mod m$.

Recall: $x \equiv 0 \mod m$ iff $m \mid x$.

Proof of ①:

Since $ab \equiv 0 \mod m$, $m \mid ab$.

But then, by Rmk. 4.50, $m \mid a$ or $m \mid b$ because m is prime.

It follows that $a \equiv 0 \mod m$ or $b \equiv 0 \mod m$. $\square$

Congruence Classes

e.g. equiv. to saying

$x \equiv 2 \mod 2.$

4

6

$\vdots$

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

- $x \equiv 0 \mod 2$: $\ldots, -4, -2, 0, 2, 4, \ldots$ (even)
- $x \equiv 1 \mod 2$: $\ldots, -3, -1, 1, 3, \ldots$ (odd)

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 $x \in \mathbb{Z}$,

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

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

In general, there are m congruence classes modulo m and each $x \in \mathbb{Z}$ belongs to exactly one of them.

Division Lemma

aka (Euclid's) Division Algorithm

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 $x = mk + r$.

divisor quotient remainder

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.

$x \equiv 0 \mod m$ iff m divides x

iff the remainder left upon dividing x by m is 0

$\boxed{35 = 3 \cdot 11 + 2}$

$= 3 \cdot 10 + 5$

$= 3 \cdot 12 - 1$

$\vdots$

$$\begin{array}{r} 11 \\ 3\,\overline{)\,35} \\ 33 \\ \hline 2 \end{array}$$

$\underset{x}{35} = \underset{m}{3} \cdot \underset{k}{11} + \underset{r}{2}$

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 $r_1, r_2 \in \{0, \dots, m-1\}$ such that $x_1 = mk_1 + r_1$ and $x_2 = mk_2 + r_2$. Then $x_1 \equiv x_2 \mod m$ iff $r_1 = r_2$.

<u>Example</u>

$$m = 6. \quad x_1 = 5 = \underset{m}{6} \cdot \underset{k_j}{0} + \underset{r_j}{5}$$

$$x_2 = 11 = 6 \cdot 1 + 5$$

- $x_1 \equiv x_2 \mod 6$ because 6 divides $11 - 5 = 6$.
- $r_1 = 5 = r_2$.

<u>Observation</u> $m = 6$.

$$\begin{cases} x_1 = 5 = 6 \cdot 0 + 5 \\ x_2 = 13 = 6 \cdot 2 + 1 \end{cases}$$

Though $x_1 < x_2$, $r_1 > r_2$

We have $r_1 \leq r_2$ or $r_2 \leq r_1$.

Consider the case where $r_1 \leq r_2$; the other case is handled similarly.

Note

$$\underbrace{x_2 - x_1}_{\in \mathbb{Z}} = (mk_2 + r_2) - (mk_1 + r_1)$$

$$\vdots$$

$$= m\underbrace{(k_2 - k_1)}_{\in \mathbb{Z}} + (r_2 - r_1).$$

Here, $0 \leq r_1 \leq r_2 \leq m-1$. So

$$0 \leq r_2 - r_1 \leq r_2 \leq m-1$$

So $r_2 - r_1$ is the remainder left on dividing $x_2 - x_1$ by m.

Proof

$x_1 \equiv x_2 \mod m$

iff m divides $x_2 - x_1$

iff $r_2 - r_1 = 0$

iff $r_1 = r_2$ $\square$