Congruences of Integers

Contents

Congruences

Definitions

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 $b - a$.

$m = 2$

$0 \equiv 0 \mod 2$

$1 \equiv 1 \mod 2$

$2 \equiv 0 \mod 2$

$3 \equiv 1 \mod 2$

$\vdots$

- 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 $m \mid x$

- 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 $a = b$.

  $0 \mid (b - a) \iff b - a = 0 \iff a = b$

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 $a \equiv c \mod m$.*

cf Equality

$(\forall a)(a = a)$

$(\forall a, b)(a = b \Rightarrow b = a)$

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

Proof of ①: Let $a \in \mathbb{Z}$ be arbitrary. Then

$$a - a = 0 = 0 \cdot m.$$

That is, m divides $a - a$, so $a \equiv a \mod m$. $\square$

Balancing Congruences

cf Equality: Assum $(a_1 = b_1) \wedge (a_2 = b_2)$. Then
$a_1 + a_2 = b_1 + b_2$; $a_1 a_2 = b_1 b_2$

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. $a_1 a_2 \equiv b_1 b_2 \mod m$.

Proof of ①: Since $a_1 \equiv b_1 \mod m$, $m \mid (b_1 - a_1)$,
So $b_1 - a_1 = km$ for some integer k.
Since $a_2 \equiv b_2 \mod m$, $m \mid (b_2 - a_2)$,
so $b_2 - a_2 = lm$ for some integer l.
Then
$(b_1 - a_1) + (b_2 - a_2) = km + lm = (k+l)m$
Note that the LHS equals $(b_1 + b_2) - (a_1 + a_2)$

$m = 6$

$\begin{cases} 2 \equiv 7 \mod m, \\ 1 \equiv -4 \mod m \end{cases}$

- $\left.\begin{array}{l} 2 + 1 = 3 \\ 7 - 4 = 3 \end{array}\right\}$ $3 \equiv 3 \mod m$ ✓
- $\left.\begin{array}{l} 2 \cdot 1 = 2 \\ 7 \cdot (-4) = -28 \end{array}\right\}$ $2 \equiv -28 \mod m$ ✓

It follows that $m \mid \{(b_1+b_2)-(a_1+a_2)\}$, so

$$a_1+a_2 \equiv b_1+b_2 \mod m. \qquad \square$$

Interesting Behavior of Congruences

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

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)

$m = 6$: $2 \cdot 3 \equiv 0 \mod m$, 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 $w \not\equiv 0$ mod m and $uw \equiv vw \mod m$, then $u \equiv v \mod m$. (Not always true)

$18 - 6 = 12 = 2 \cdot 6 = 2 \cdot m$

$m = 6$: $2 \cdot 3 \equiv \underline{6 \cdot 3} \mod m$ but $2 \not\equiv 6 \mod m$.

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 $u \equiv w \mod m$.

Proof of ①

Since $ab \equiv 0 \mod m$, $m \mid ab$. But since m is prime, by Rmk 4.50, $m \mid a$ or $m \mid b$.

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

Congruence Classes

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

- $x \equiv 0 \mod 2$: $\ldots, -4, -2, 0, 2, 4, \ldots$ even / can also say $x \equiv 2 \mod 2$
- $x \equiv 1 \mod 2$: $\ldots, -3, -1, 1, 3, \ldots$ 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 $\longrightarrow \{0, 1, 2, \cdots, m-1\}$
and each $x \in \mathbb{Z}$ belongs to exactly one of them.

Division Lemma

(aka division algorithm)

$$\begin{array}{r|l} & k \\ \hline m\,) & x \\ & mk \\ \hline & r \end{array}$$

k → quotient

m → divisor

r → remainder

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 $x = mk + r$.

m: divisor, k: quotient, r: 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.

$m = 3$. $x = 14$

$x = \boxed{3 \cdot 4 + 2}$

$= 3 \cdot 3 + 5$

$= 3 \cdot 5 + -1$

$= \vdots$

Observation

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

iff the remainder left after dividing x by m is 0.

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 $r_1 = r_2$.

Observation We have $r_1 \le r_2$ or $r_2 \le r_1$.

Consider the case $r_1 \le r_2$; the other is handled similarly. Note that

$$x_2 - x_1 = (mk_2 + r_2) - (mk_1 + r_1)$$

$$= m(k_2 - k_1) + r_2 - r_1.$$

Here, $0 \le \underline{r_1 \le r_2} \le m-1$, and so

$0 \le r_2 - r_1 \le r_2 \le m-1$, so

$r_2 - r_1 \in \{0, 1, \ldots, m-1\}$.

$m = 6$

$x_1 = 10 = 6 \cdot \overset{k_1}{1} + \overset{r_1}{4}$

$x_2 = 13 = 6 \cdot \underset{k_2}{2} + \underset{r_2}{1}$

Note that $x_1 < x_2$, but $r_1 > r_2$.

Proof

$$x_1 \equiv x_2 \mod m \quad \text{iff} \quad m \text{ divides } x_2 - x_1$$

$$\text{iff} \quad r_2 - r_1 = 0$$

$$\text{iff} \quad r_1 = r_2 .$$

$\square$

the remainder obtained after ~~by~~ dividing $x_2 - x_1$ by m is 0