

## Congruences of Integers

# Contents

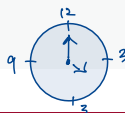
## ① Congruences

# Congruences

Overview Section 4 (mathematical proofs)

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

# Definitions



Example  $m = 12$

$4 \equiv 16 \pmod{12}$  because  $12 \mid (16-4)$

## Definition 1 (Congruences)

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

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

$$x \equiv 0 \pmod{m} \iff m \mid (0-x) \iff m \mid x$$

- For each integer  $x$ ,  
 $(\exists k \in \mathbb{Z})(-x = km)$   
 $x = -km = (-k)m$

$$\text{"}x \text{ is even.}" \iff x \equiv 0 \pmod{2}$$

$$\text{"}x \text{ is odd.}" \iff x \equiv 1 \pmod{2}$$

- For all integers  $a$  and  $b$ ,  $a \equiv b \pmod{0}$  iff  $a = b$ .

$$a \equiv b \pmod{0} \iff 0 \mid (b-a) \iff b-a=0 \iff a=b.$$

Example  $m = 2$ .

$$0 \equiv 0 \pmod{2}$$

$$1 \equiv 1 \pmod{2}$$

$$2 \equiv 0 \pmod{2}$$

$$3 \equiv 1 \pmod{2}$$

$$4 \equiv 0 \pmod{2}$$

$\vdots$

# 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  $a \in \mathbb{Z}$ ,  $a \equiv a \pmod{m}$ .
- 2 (Symmetry) For all  $a, b \in \mathbb{Z}$ , if  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ .
- 3 (Transitivity) For all  $a, b, c \in \mathbb{Z}$ , if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ .

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

# Balancing Congruences

Equality (=)

$$a = b$$

$$\bullet a + c = b + c$$

$$\bullet ac = bc$$

$$a_1 = b_1, \quad a_2 = b_2$$

$$\bullet a_1 + a_2 = b_1 + b_2$$

$$\bullet a_1 a_2 = b_1 b_2$$

## Theorem 3 (Preserving Congruences)

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

$$\textcircled{1} \quad a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

$$\textcircled{2} \quad a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

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

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

Since  $a_2 \equiv b_2 \pmod{m}$ ,  $m \mid (b_2 - a_2)$ , 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,

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

□

# Interesting Behavior of Congruences

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

Recall:  $x \equiv 0 \pmod{m}$  iff  $m \mid x$ .

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

- If  $ab = 0$ , then  $a = 0$  or  $b = 0$ . (True)
- If  $ab \equiv 0 \pmod{m}$ , then  $a \equiv 0 \pmod{m}$  or  $b \equiv 0 \pmod{m}$ . (Not always true)  
 $m=6$   $2 \cdot 3 \equiv 0 \pmod{6}$ , but  $2 \not\equiv 0 \pmod{6}$  and  $3 \not\equiv 0 \pmod{6}$ .  
"there are values of  $m$  for which this is false."

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

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

$m=6$   $5 \cdot 3 \equiv 7 \cdot 3 \pmod{6}$ , but  $5 \not\equiv 7 \pmod{6}$ .  
→ (because  $21 - 15 = 6$ , which is divisible by  $m$ ).

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

## When $m$ Is Prime

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

Proof of ①:

Recall:  $x \equiv 0 \pmod{m}$  iff  $m \mid x$ .

Since  $ab \equiv 0 \pmod{m}$ ,  $m \mid ab$ .

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

It follows that  $a \equiv 0 \pmod{m}$  or  $b \equiv 0 \pmod{m}$ .  $\square$



# Congruence Classes

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

- $x \equiv 0 \pmod{2}$ :  $\dots, -4, -2, 0, 2, 4, \dots$
- $x \equiv 1 \pmod{2}$ :  $\dots, -3, -1, 1, 3, \dots$

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  $x \in \mathbb{Z}$ ,

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

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