cse 16 7-27-21

Defn

Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. We say that a and b are congruent modulo m iff

$$m \mid (a-b)$$

notation: $a \equiv b \pmod{m}$

Alt. notation: $a \equiv_m b$

Ex. $10 \equiv 7 \pmod{3}$ since $3 \mid 10-7 = 3$

$25 \equiv 11 \pmod{7}$ since $7 \mid 25-11 = 14$

$-13 \equiv 106 \pmod{17}$ " $17 \mid -13-106 = 119 = -7 \cdot 17$

$18 \not\equiv 5 \pmod{4}$ since $4 \mid 18-5 = 13$

Lemma 6

$a \equiv b \pmod m$ $\overset{\Rightarrow}{\underset{\Leftarrow}{\text{iff}}}$ $a = b + km$ for some $k \in \mathbb{Z}$

Proof: exercise.

Theorem

$a \equiv b \pmod m$ $\overset{\Rightarrow}{\underset{\Leftarrow}{\text{iff}}}$ a and b have the same remainder upon division by m.

Proof.

($\Leftarrow$). Assume a, b have same remainder upon div. by m. So

$$a = q_1 m + r \qquad (0 \le r < m)$$

and

$$b = q_2 m + r \qquad "$$

Then

$$a - b = (q_1 m + r) - (q_2 m + r)$$

$$= q_1 m - q_2 m$$

$$= (q_1 - q_2) m$$

$\therefore\ m \mid (a-b)$

$\therefore\ a \equiv b \pmod{m}$.

($\Longrightarrow$) Assume $a \equiv b \pmod{m}$. Then

$$m \mid (a-b)$$

$\therefore\ a - b = km$ for some $k \in \mathbb{Z}$

Divide a by m and b by m!

$$a = q_1 m + r_1 \qquad (0 \le r_1 < m)$$

and

$$b = q_2 m + r_2 \qquad (0 \le r_2 < m)$$

we must show $r_1 = r_2$.

Assume (to get a ⚠) that $r_2 < r_1$.

Then $0 \le r_2 < r_1 < m$, hence

$$0 < r_1 - r_2 < m$$

But

$$\begin{aligned} r_2 - r_1 &= (a - q_1 m) - (b - q_2 m) \\ &= (a - b) - q_1 m + q_2 m \\ &= km - q_1 m + q_2 m \\ &= (k - q_1 + q_2)\, m. \end{aligned}$$

$\therefore \quad 0 < (k - q_1 + q_2)m < m$

$\therefore \quad 0 < (k - q_1 + q_2) < 1 \qquad \dot{\times}$

This $\dot{\times}$ shows that $r_2 \not< r_1$

$\therefore \quad r_2 \geq r_1$. Exercise: show that $r_2 > r_1$ leads to a $\dot{\times}$, hence also $r_2 \not> r_1$, and hence $r_2 \leq r_1$.

We conclude $r_2 = r_1$, as required.

∎

Theorem

Let $a, b, c, d, m \in \mathbb{Z}$ $(m > 0)$, and

$$a \equiv c \pmod{m}$$

and $$b \equiv d \pmod{m}.$$

Then

(1) $a+b \equiv c+d \pmod{m}$

and

(2) $a \cdot b \equiv c \cdot d \pmod{m}$

i.e. we can add & mult. congruences like equations.

Proof of (1)

$$\left.\begin{array}{l} a \equiv_m c \implies m \mid (a-c) \\ b \equiv_m d \implies m \mid (b-d) \end{array}\right\} \implies m \mid (a-c)+(b-d)$$

$$\therefore \quad m \mid (a+b)-(c+d)$$

$$\therefore \quad a+b \equiv_m c+d$$

Exercise Prove (2).

Theorem

Let $a, b, c, m \in \mathbb{Z}$ $(m > 0)$. Then if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof.

$$\left.\begin{array}{l} a \equiv_m b \Rightarrow m \mid (a-b) \\ b \equiv_m c \Rightarrow m \mid (b-c) \end{array}\right\} \Rightarrow m \mid (a-b)+(b-c)$$

$$\therefore \quad m \mid (a-c)$$

$$\therefore \quad a \equiv c \pmod{m}$$

∎

Ex (ch. 5, p. 136, #17)

If $n \in \mathbb{Z}$ is odd, then $8 \mid (n^2 - 1)$.

Equivalently: $n^2 \equiv 1 \pmod 8$.

Proof:

Suppose n is odd. Then there exists $k \in \mathbb{Z}$ s.t. $n = 2k+1$. Thus

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 4k(k+1) + 1 \end{aligned}$$

$\therefore$ $n^2 - 1 = 4k(k+1)$.

Exactly one of k and $k+1$ is even.

Case 1: k is even, so $k = 2\ell$, $\ell \in \mathbb{Z}$.

$$\therefore \quad n^2 - 1 = 4 \cdot 2\ell \cdot (2\ell + 1)$$
$$= 8 \cdot \ell(2\ell + 1)$$

$$\therefore \quad 8 \mid (n^2 - 1) \; .$$

Case 2: $k+1$ is even. (exercise)

■

Ex. (ch. 6, p. 144, #17)

For all $n \in \mathbb{Z}$: $4 \nmid (n^2 + 2)$.

Equivalently: $n^2 \not\equiv -2 \pmod 4$

Since $-2 \equiv 2 \pmod 4$, also equiv. to

$$n^2 \not\equiv 2 \pmod 4$$

Proof.

Assume (to get a $\not\!\!\downarrow$) $4 \mid (n^2+2)$.

Then $n^2+2 = 4k$ (some $k \in \mathbb{Z}$).

$\therefore\ n^2 = 4k-2 = 2(2k-1)$

$\therefore\ 2 \mid n^2$

$\therefore\ 2 \mid n$

$\therefore\ 4 \mid n^2$ (exercise: $a \mid b \Rightarrow a^2 \mid b^2$)

$\therefore\ n^2 = 4l$ (some $l \in \mathbb{Z}$).

$\therefore\ 4k-2 = n^2 = 4l$

$\therefore\ 2k-1 = 2l$

But this is impossible since LHS is odd while RHS is even

$\therefore\ 4 \nmid (n^2+2)$ ∎

Alternate Proof:

Prove the eq. fact $n^2 \not\equiv 2 \pmod 4$

The possible remainders on div. by 4 are: 0, 1, 2, 3. Thus each $n \in \mathbb{Z}$ satisfies exactly one of the following

- $n = 4k \Rightarrow n^2 = 16k^2 = 4(\ ) \Rightarrow \boxed{n^2 \equiv_4 0}$
- $n = 4k+1 \Rightarrow n^2 = 16k^2 + 8k + 1$
  $= 4(\ ) + 1$
  $\Rightarrow \boxed{n^2 \equiv_4 1}$
- $n = 4k+2 \Rightarrow n^2 = 16k^2 + 16k + 4$
  $= 4(\ )$
  $\Rightarrow \boxed{n^2 \equiv_4 0}$

- $n = 4k+3 \Rightarrow n^2 = 16k^2 + 24k + 9$

$$= (16k^2 + 24k + 8) + 1$$

$$= 4(\quad) + 1$$

$$\Rightarrow \boxed{n^2 \equiv_4 1}$$

Therefore, every $n \in \mathbb{Z}$ satisfies

$$n^2 \equiv 0 \pmod 4 \quad \text{or} \quad n^2 \equiv 1 \pmod 4.$$

Hence, no integer satisfies

$$n^2 \equiv 2 \pmod 4$$

$\therefore$ $n^2 \not\equiv 2 \pmod 4$ for all $n \in \mathbb{Z}$.

■

Chapter 7 : non-conditional statements

i.e. not of the form $P \Rightarrow Q$.

Existence Proofs

Let $P(x)$ be a propositional fcn. with universe U. A proof of

$$\exists x \in U : P(x)$$

is called an existence proof.

Two kinds of existence proofs

- Constructive

  find, construct, or display a a particular $a \in U$ s.t. $P(a)$ is true.

- non-constructive

  Proceed in some other way, usually by Contradiction.

Ex.

There exist $x, y \in \mathbb{R} - \mathbb{Q}$ such that

$$x^y \in \mathbb{Q}.$$

Proof.

Consider the real number $\sqrt{2}^{\sqrt{2}}$.

This number is either rational or it is not.

Case 1 $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.

Let $x = y = \sqrt{2}$. Then $x, y \in \mathbb{R} - \mathbb{Q}$ and $x^y = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.

Case 2 $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} - \mathbb{Q}$.

Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then both $x, y \in \mathbb{R} - \mathbb{Q}$. But

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$$

In either case1 or case2,
there exist $x, y \in \mathbb{R} - \mathbb{Q}$
with $x^y \in \mathbb{Q}$. ∎

Rmk
This was not a constructive Proof.
We never displayed $x, y \in \mathbb{R} - \mathbb{Q}$
s.t. $x^y \in \mathbb{R}$. Instead we
relied on the fact that

$$R \vee \sim R$$

is a tautology. Called the
Law of Excluded Middle.

note in fact $\sqrt{2}^{\sqrt{2}}$ is irrational

Proof is difficult and a little long.

We can give a constructive existence proof of last Thm.

next time - - - - .