CSE 16 7-21-22

Thm

$a \equiv b \pmod m$ iff a and b have same remainder on div. by m.

Proof

($\Leftarrow$) done ←

($\Rightarrow$) Assume $a \equiv b \pmod m$ Then

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

$$\therefore \quad (a-b) = km \quad (\text{some } k \in \mathbb{Z})$$

Divide a and b by m to get

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

and

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

we must show $r_1 = r_2$.

Suppose $r_2 < r_1$. Then $0 \leq r_2 < r_1 < m$, hence

$$0 < r_1 - r_2 < m .$$

But

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

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

$\therefore$ $0 < (k - q_1 + q_2) < 1$

This is impossible, so that $r_2 \not< r_1$ hence $r_2 \geq r_1$. exercise: show $r_1 < r_2$ is also impossible, $\therefore r_1 \not< r_2 \therefore r_1 \geq r_2$

This shows $r_1 = r_2$, as required. ∎

Theorem

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

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

and

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

Then

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

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

i.e. we can add and multiply congruences.

Proof of (1):

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

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

$$\Rightarrow \quad a+b \equiv_m c+d. \qquad \blacksquare$$

Exercise: Prove Part (2).

Thm

Let $a, b, c, m \in \mathbb{Z}$ $(m>0)$. Then:

$$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

Proof:

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

$$\Rightarrow m \mid (a-c) \Rightarrow a \equiv_m c. \qquad \blacksquare$$

Rmk: This is called the transitive Property.

Exercise:

- for any $a, b, m \in \mathbb{Z}$ $(m>0)$:

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

(symmetric Property.)

- for any $a, m \in \mathbb{Z}$ $(m>0)$:

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

(reflexive Property.)

Ex (ch. 5 P. 136 #17)

If n is odd, then $8 \mid (n^2-1)$. equivalently

$$n^2 \equiv 1 \pmod{8}$$

Proof:

Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Then

$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 4k(k+1) + 1$$

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

Exactly one of k or $k+1$ is even

<u>case 1</u>: $k = 2l$ is even

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

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

<u>case 2</u>: $k+1 = 2l$ is even

exercise.

■

Ex. (Ch. 6 P. 144 #17)

Let $n \in \mathbb{Z}$. Then $4 \nmid (n^2+2)$. equivalently

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

note: $2 \equiv -2 \pmod 4$ since $4 \mid (2-(-2)) = 4$.

$\therefore$ this is also equiv. to

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

Proof: (contradiction)

Assume $4 \mid (n^2+2)$. Then $n^2+2 = 4k$

for some $k \in \mathbb{Z}$.

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

$\therefore \quad 2 \mid n^2$

$\therefore \quad 2 \mid n$

(exercise: $a \mid b \Rightarrow a^2 \mid b^2$.)

$\therefore \quad 4 \mid n^2$

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

$\therefore \quad 4l = 2(2k-1)$

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

But the LHS is even, while RHS is odd, which is a $\lightning$.

This $\lightning$ shows our assumption was false, hence $4 \nmid (n^2+2)$. ∎

Alternate Proof:

The possible remainders upon division by 4 are: 0, 1, 2, 3. Thus n satisfies exactly one of

① $n = 4k$
② $n = 4k+1$
③ $n = 4k+2$
④ $n = 4k+3$

} for some $k \in \mathbb{Z}$.

so

① $n = 4k \Rightarrow n^2 = 16k^2 = 4(\ )$

$\Rightarrow n^2 \equiv_4 0$

② $n = 4k+1 \Rightarrow n^2 = 16k^2 + 8k + 1$

$= 4(\ ) + 1$

$\Rightarrow n^2 \equiv_4 1$

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

$= 4(\ )$

$\Rightarrow n^2 \equiv_4 0$

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

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

$= 4(\ ) + 1$

$\Rightarrow n^2 \equiv_4 1$

∴ every $n \in \mathbb{Z}$ satisfies either

$n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

$\therefore$ no n satisfies $n^2 \equiv 2 \pmod 4$.

$\therefore$ all n satisfy: $n^2 \not\equiv 2 \pmod 4$. ∎

Rmk: We've also shown

$$n^2 \not\equiv 3 \pmod 4 \quad .$$

Chap. 7 non-conditional statements.
(i.e. not of the form: $P \to Q$)

Existence Proofs

Let $P(x)$ be a Prop. fcn. with universe $\mathcal{U}$.
A Proof of

$$\exists x \in \mathcal{U} : P(x)$$

is called an existence Proof.

There are 2 kinds of such proofs.

- Constructive

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

- non-constructive

  uses some other means, usually by contradiction (but not always.)

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 irrational

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

$x, y \in \mathbb{R} - \mathbb{Q}$ and

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

In both cases there exist $x, y \in \mathbb{R} - \mathbb{Q}$ with $x^y \in \mathbb{Q}$.

■

note: this was not constructive.

we relied on $\boxed{r \vee \neg r}$ is a tautology.

Note:

We can give a constructive Proof of

$$\exists\, x, y \in \mathbb{R} - \mathbb{Q} : x^y \in \mathbb{Q} .$$

next time.