CSE 16 2-17-22

Lemma 6

$a \equiv b \pmod m$ iff $a = b + km$ for some $k \in \mathbb{Z}$.

Proof: exercise.

Theorem

$a \equiv b \pmod m$ iff a and b have the same remainder upon division by m.

Proof.

($\Leftarrow$) Assume a, b have same rem. on div. by m. Then

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

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

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 $k \in \mathbb{Z}$.

Now divide a, b by m to get

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

and

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

we must show $r_1 = r_2$.

suppose $r_1 \neq r_2$. Then either $r_1 < r_2$ or $r_1 > r_2$. Say $r_2 < r_1$. We then have $0 \le r_2 < r_1 < m$, and 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

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

$$\therefore \quad 0 < k - q_1 + q_2 < 1,$$

which is impossible. A similar contradiction arises if $r_1 < r_2$ (exercise).

It follows that $r_1 = r_2$. ∎

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

and

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

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 (hw)

Prove Part (2).

more exercises

for $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

- $a \equiv a \pmod m$
- $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$.

Thm

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.

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

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

Ex. (ch. 5 #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. $n = 2k+1$, and

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

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

Case 1: k is even, i.e. $k = 2l$ (some $l \in \mathbb{Z}$)

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

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

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

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

exercise.

∎

<u>Ex.</u> (ch. 6 P. 144 #17)

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

<u>equivalently</u>: $n^2 \not\equiv -2 \pmod 4$

<u>note</u> $2 \equiv -2 \pmod 4$, so another

<u>equivalent stmt</u>: $n^2 \not\equiv 2 \pmod 4$.

<u>Proof</u>

Assume $4 \mid (n^2+2)$. 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 $l \in \mathbb{Z}$)

$\therefore 4k-2 = 4l$

$\therefore 2k-1 = 2l$

But LHS is odd while RHS is even. This ※ shows our assumption was false, hence

$$4 \nmid (n^2+2)$$

∎

Alternate Proof:

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

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

- $n = 4k+1 \Rightarrow n^2 = (16k^2 + 8k + 1)$
  $= 4(\cdot) + 1 \Rightarrow \boxed{n^2 \equiv_4 1}$
- $n = 4k+2 \Rightarrow n^2 = 16k^2 + 16k + 4$
  $= 4(\cdot) \Rightarrow \boxed{n^2 \equiv_4 0}$
- $n = 4k+3 \Rightarrow n^2 = 16k^2 + 24k + 9$
  $= 4(\cdot) + 1 \Rightarrow \boxed{n^2 \equiv_4 1}$

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

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

So for all $n \in \mathbb{Z}$:

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

Rmk

we've also shown that

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

Chap 7 : non-conditional stmts.

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.

There are 2 categories of such proofs.

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

- **non-constructive**

uses some other means, often contradiction (not always.)

Ex.

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

Proof.

consider $\sqrt{2}^{\sqrt{2}}$. 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 both $x, y \in \mathbb{R} - \mathbb{Q}$, 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 either case there exist $x, y \in \mathbb{R} - \mathbb{Q}$ s.t. $x^y \in \mathbb{Q}$.

■

This was <u>not</u> constructive since we don't have a known pair $(x,y) \in (\mathbb{R}-\mathbb{Q})^2$ s.t. $x^y \in \mathbb{Q}$. Instead we relied on the tautology

$$R \vee \neg R$$

called: <u>law of excluded middle</u>.

<u>Fact</u> $\sqrt{2}^{\sqrt{2}}$ is actually irrational.

Proof is beyond this course.

we can prove this constructively though.

Lemma $\log_2(9)$ is irrational.

Proof.

Assume $\log_2(9) \in \mathbb{Q}$, so that

$$\log_2(9) = \frac{a}{b}$$

for some $a, b \in \mathbb{Z}$. Then

$$2^{\log_2(9)} = 2^{\frac{a}{b}}$$

$$\therefore \quad 9 = 2^{a/b}$$

$$\therefore \quad 9^b = \left(2^{a/b}\right)^b = 2^{\frac{a}{b} \cdot b}$$

$$\therefore \quad 9^b = 2^a$$

But LHS is odd and RHS is even, so ⚡.

$\therefore \log_2(9) \notin \mathbb{Q}$.

Constructive Proof of

$$\exists (x, y) \in (\mathbb{R} - \mathbb{Q})^2 : x^y \in \mathbb{Q}$$

Proof

Let $x = \sqrt{2}$ and $y = \log_2(9)$. Then

$$x^y = \ldots\ldots$$

next time