Mon Feb 16 Ch4 - Ch5 Clean-up

Prop pg122 Sppse $a,b,c \in \mathbb{N}$, then

$$\text{lcm}(ca, cb) = c \cdot \text{lcm}(a,b)$$

- Help w/ #28 on HW5
- Clarity of strategy

Pf: Sppse $a,b,c \in \mathbb{N}$, $m = \text{lcm}(ca,cb)$, and and $n = c \cdot \text{lcm}(a,b)$. (We show $m \leq n \wedge m \geq n$)

(Show $m \geq n$.) $m = \text{lcm}(ca,cb)$ means - by definition - $\exists\, k_1, k_2 \in \mathbb{Z}$ s.t. $m = k_1 ca = k_2 cb$.
Dividing by c, we obtain $\frac{m}{c} = k_1 a = k_2 b$.
Since $k_1 a \in \mathbb{Z}$, $\frac{m}{c} \in \mathbb{Z}$. Since $\frac{m}{c} = k_1 a = k_2 b$, we know $\frac{m}{c}$ is a common multiple of a and b.
Thus, $\frac{m}{c} \geq \text{lcm}(a,b)$. Mult. by c gives $m \geq c \cdot \text{lcm}(a,b) = n$

(Show $n \geq m$). Let $d = \text{lcm}(a,b)$. By def $d = k_1 a = k_2 b$.
So $cd = k_1(ca) = k_2(cb)$. So cd as a common mult. of ca and cb So $n = c \cdot \text{lcm}(a,b) = cd \geq \text{lcm}(ac, bc)$.

Ch5 Def Congruence

<u>def</u>: $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

a and b <u>are congruent modulo n</u> if

$n \mid (a-b)$. Write $a \equiv b \pmod{n}$.

<u>Ex</u> $10 \equiv 28 \bmod 6$ b/c $10-28=-18$ and $6 \mid -18$

$25 \not\equiv 13 \bmod 7$ b/c $25-13=22$ and $7 \nmid 22$

<u>Prop</u>: $a \equiv b \bmod n$ if and only if the division algorithm gives the same remainder when a is divided by n and when b is divided by n

(ie Appy DA to get $a = q_1 n + r_1$ and $b = q_2 n + r_2$ then $a \equiv b \pmod{n} \iff r_1 = r_2$)

$\boxed{\text{Pf}}$ If $r_1 = r_2$, then $a-b = (q_1 - q_2)n$. So $n \mid a-b$.

If $a \equiv b \pmod{n}$, then $a \equiv b \pmod{n} \overset{\text{def mod}}{\Longrightarrow} n \mid (a-b) \overset{\text{def div.}}{\Longrightarrow} \exists k$

$kn = a-b \overset{\text{DA}}{\Longrightarrow} kn = (q_1 n - r_1) - (q_2 n - r_2) \overset{\text{alg}}{\Longrightarrow}$

$r_2 - r_1 = (k - q_1 + q_2)n$. WOLG, we can assume $r_2 - r_1 \geq 0$

DA $\Rightarrow$ $0 \leq r_2 - r_1 \leq r_2 < n$. But $n \mid r_2 - r_1$. So $r_1 - r_2 = 0$.

Props on pg 132

* Do this on your own.

① $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

$$a \equiv b \pmod{n} \Rightarrow a^2 \equiv b^2 \pmod{n}$$

*

② $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$

$$a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$$

step 1

Pf: (direct) Sppse $a \equiv b \pmod{n}$. By def of congruence $n \mid (a-b)$. By def of divis $n \cdot k = a-b$

Mult. by $a+b$ to get:

$$n\,k(a+b) = (a-b)(a+b)$$
$$= a^2 + b^2.$$

Obs. $k(a+b) = l \in \mathbb{Z}$.

step 3 get these together.

step 2

Thus, $n\,l = a^2 - b^2$ for $l \in \mathbb{Z}$.

Thus $n \mid (a^2 - b^2)$ by def of divis.

Thus, by def, $a^2 \equiv b^2 \pmod{n}$.

A note of caution:

Modular arithmatic (or algebra) does not have all the same rules as that in $\mathbb{R}$.

Ex ② on previous page is not reversible!

$$ac \equiv bc \pmod{n} \not\Rightarrow a \equiv b \pmod{n}$$

Ex] $2 \cdot 10 \equiv 2 \cdot 8 \equiv 0 \mod 4$

But $10 \equiv 2 \mod 4$ and $8 \equiv 0 \mod 4$.

So $10 \not\equiv 8 \pmod{4}$

Ex] You can't guarantee division works.

$2x \equiv 5 \mod 12$ or $5y \equiv 2 \mod 12$

It's tempting to say $x = \cancel{5/2}$ and $y = 2/5$

$12 \nmid (\underbrace{2x-5}_{\text{odd}})$

$y = 10$ is a soln

HW #6 #25 Fact from C2

- $a^k + a^{k-1} + \dots + a + 1 = \dfrac{a^{k+1} - 1}{a-1}$ ↙ Used to show $\sum a^k$ converges if $|a|<1$.

- Obtained algebraically from

$$(a-1)(a^k + a^{k-1} + \dots + a + 1) = a^{k+1} - 1$$

- (of course...) the same as

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + a + 1)$$

Summary Ch5

- Pf by contrapositive.

If P, then ☺ $\neq \xi$. (or ☺ $\not\equiv \xi$ or ☺ $\not< \xi$)

We don't have an algebra of not =.

Eg:

$$A \neq B \not\Rightarrow A^2 \neq B^2$$

$$f \neq g \not\Rightarrow f' \neq g'$$

- def of $a \equiv b \pmod n$

- Rules about writing proofs (FYI even more rigid than mine!) ← read this