LECTURE 6

(Wednesday OCT. 9, 2019)

Chinese Remainder Theorem (CRT):

EX Solve the system of congruences: $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{6} \end{cases}$

No solutions: $x \equiv 2 (4)$ forces x to be even; $x \equiv 3 (6)$ implies x must be odd !

– Problem is $GCD(4,6) > 1$.

Thm. (CRT) Given two coprime integers $M, N > 0$. For any two $a, b \in \mathbb{Z}$, the system

$$x \equiv a \pmod{M} \wedge x \equiv b \pmod{N}$$

has solutions. Moreover, any two solutions are congruent modulo MN.

PROOF. First, the general solution to $x \equiv a (M)$ is $x = a + Mt$ as $t \in \mathbb{Z}$ varies.

Want $a + Mt \equiv b \pmod{N}$.

I.e., $Mt \equiv b - a \ (N)$.

$t \equiv M^*(b-a) \pmod{N}$.

since $GCD(M,N) = 1$, M has a multiplicative inverse mod N:

$$MM^* \equiv 1 \pmod{N}$$

in $\mathbb{Z}$.

∞ many such t.

– existence ✓

Uniqueness? Suppose x_1 and x_2 solve the system.
Then $x_1 - x_2 \equiv 0\ (M)$ and $x_1 - x_2 \equiv 0\ (N)$.
I.e., $x_1 - x_2$ is a common multiple of M, N,
therefore a multiple of $\mathrm{LCM}(M,N) = MN$

$\uparrow$

M, N coprime $\square$

EX Find the general solution to the system:

$$x \equiv 1 \pmod 5 \quad \wedge \quad x \equiv 3 \pmod 7$$

(note: 5, 7 are coprime)

1^{st} congruence gives $x = 1 + 5t$, $t \in \mathbb{Z}$.

Here t must satisfy $1 + 5t \equiv 3 \pmod 7$

$$5t \equiv 2 \pmod 7$$

$$\times 3$$

$$t \equiv 6 \pmod 7$$

$$t = 6 + 7s, \quad s \in \mathbb{Z}.$$

ASIDE: Inverse of 5 modulo 7?

$$5 \cdot 3 \equiv 1 \pmod 7$$

Combined,

$$x = 1 + 5(6 + 7s) = \underline{\underline{31 + 35s}}.$$

(ex. $x = -39, -4, 31, 66 \ldots$)