LECTURE 6
(Wednesday Oct. 9, 2019)
Chinese Remainder Theorem (CRT):

Ex. Solve the system of congruences:

\[
\begin{align*}
&x \equiv 2 \pmod{4} \\
&x \equiv 3 \pmod{6}
\end{align*}
\]

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

\[
x \equiv a \pmod{M} \land x \equiv b \pmod{N}
\]

has solutions. Moreover, any two solutions are congruent modulo \( MN \).

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

Want \( a + Mt \equiv b \pmod{N} \). Since \( \gcd(M, N) = 1 \), I.e., \( Mt \equiv b - a \pmod{N} \), \( M \) has a multiplicative inverse \( \pmod{N} \):

\[
M M^* \equiv 1 \pmod{N} \quad \text{A in } \mathbb{Z}.
\]

\( t = M^*(b - a) \pmod{N} \). \( \leq \) many such \( t \). \( \leftarrow \) existence.
Uniqueness? Suppose \( x_1 \) and \( x_2 \) solve the system. Then \( x_1 - x_2 \equiv 0 \pmod{M} \) and \( x_1 - x_2 \equiv 0 \pmod{N} \).

I.e., \( x_1 - x_2 \) is a common multiple of \( M, N \), therefore a multiple of \( \text{LCM}(M, N) \). \[ \uparrow \]

**EX.** Find the general solution to the system:

\[
x \equiv 1 \pmod{5} \land x \equiv 3 \pmod{7}
\]

(Note: \( 5, 7 \) are coprime)

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

Hence, \( t \) must satisfy \( 1 + 5t \equiv 3 \pmod{7} \)

\[
5t \equiv 2 \pmod{7} \\
5t \equiv 2 + 7 \equiv 9 \equiv 2 \pmod{7}
\]

Hence \( t \equiv 6 \pmod{7} \).

\[ t = 6 + 7s, \ s \in \mathbb{Z} \]

\[ x = 1 + 5(6 + 7s) = 31 + 35s. \]

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