Section 4.3 – Sun-Tsu's Thm I

Q: Are there any $x \in \mathbb{Z}$ satisfying

$$x \equiv 1 \mod 5$$
$$x \equiv 3 \mod 7$$

?

Check by looking at diff. #s $\equiv 3 \mod 7$ and see if $\equiv 1 \mod 5$

$a_n = 3 + 7n$

n	0	1	2	3	4	5	6
a_n	3	10	17	24	31	38	45
mod 5	3	0	2	4	1 ✓	3	0

$x = 31$ satisfies $x \equiv 3 \mod 7$, $x \equiv 1 \mod 5$

Q. Any other solns? if so, can you classify them?

$X = 31, 66, 101$

$x = 3 + 7(4 + 5k)$ $\quad k \in \mathbb{Z}$

$x = 31 + 35k$

$x \equiv 31 \mod 35$

$x \equiv 3 \mod 7$ $\qquad$ $x \equiv 1 \mod 5$

Thm (Sun-Tsu): Let $m_1, \ldots, m_r$ be pairwise rel. prime pos. ints. Then

$$x \equiv a_1 \mod m_1$$
$$x \equiv a_2 \mod m_2$$
$$\vdots$$
$$x \equiv a_r \mod m_r$$

has a unique sol'n mod $m_1 \cdots m_r$

↳ also called the Chinese Remainder Thm.

Pf: Define $M = m_1 \cdots m_r$

$$L_k = \frac{M}{m_k} = m_1 \cdots m_{k-1} m_{k+1} \cdots m_r$$

Observe $(L_k, m_k) = 1$

Hence $\exists\, y_k \in \mathbb{Z} : L_k y_k \equiv 1 \mod m_k$

So $a_k L_k y_k \equiv a_k \mod m_k$

Define $x = a_1 L_1 y_1 + a_2 L_2 y_2 + \cdots + a_r L_r y_r$

($L_2 y_2$: mult. of m_1; $L_r y_r$: mult. of m_1)

Observe: $x \equiv a_1 L_1 y_1 \equiv a_1 \mod m_1$

$x \equiv a_2 L_2 y_2 \equiv a_2 \mod m_2$

$\vdots$

$x \equiv a_r \mod m_r$

Next: Show uniqueness. (mod M)

Suppose $y \equiv a_1 \bmod m_1, \ldots, y \equiv a_k \bmod m_k$

Goal: show $y \equiv x \bmod M$

Note $y \equiv a_1 \equiv x \bmod m_1 \longrightarrow m_1 \mid y - x$

$\vdots$ $\qquad\qquad$ $\vdots$

$y \equiv a_r \equiv x \bmod m_r \longrightarrow m_r \mid y - x$

Since $m_1, \ldots, m_r$ are pairwise rel. prime, $m_1 \cdots m_r \mid y - x \longrightarrow y \equiv x \bmod M$

($M = m_1 \cdots m_r$)

Ex: Solve $x \equiv 1 \bmod 2$

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

Note 2, 3, 5 are pairwise rel. prime

$M = 2 \cdot 3 \cdot 5 = 30$

$m_1 \quad m_2 \quad m_3$

$\rightarrow \quad L_1 = 15, \quad L_2 = 10, \quad L_3 = 6$

① Solve $L_k y_k \equiv 1 \mod m_k$

$15 y_1 \equiv 1 \mod 2$ (apply: if $a \equiv b \mod m$ then $ac \equiv bc \mod m$)

$\updownarrow$

$1 \cdot y_1 \equiv 1 \mod 2 \leftarrow y_1 = 1$

Since $15 \equiv 1 \mod 2$

then $15 y_1 \equiv 1 y_1 \mod 2$

also $15 y_1 \equiv 1 \mod 2$

$\| \quad \|$

y_1

$10 y_2 \equiv 1 \mod 3$

$y_2 \equiv 1 \mod 3 \leftarrow y_2 = 1$

$6 y_3 \equiv 1 \mod 5$

$\updownarrow$

$y_3 \equiv 1 \mod 5 \leftarrow y_3 = 1$

$x = a_1 L_1 y_1 + a_2 L_2 y_2 + a_3 L_3 y_3$

$= 1 \cdot 15 \, 1 + 2 \, 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 15 + 20 + 18$

$= 53$