

## Section 4.3 - Sun-Tsu's Thm 1

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

$$x \equiv 1 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

?

Check by looking at diff. #'s  $\equiv 3 \pmod{7}$   
and see if  $\equiv 1 \pmod{5}$

$$a_n = 3 + 7n$$

n	0	1	2	3	4	5	6
$a_n$	3	10	17	24	31	38	45
$\pmod{5}$	3	0	2	4	1 ✓	3	0

$x = 31$  satisfies

$$x \equiv 3 \pmod{7}$$

$$x \equiv 1 \pmod{5}$$

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

$$x = 31, 66, 101$$

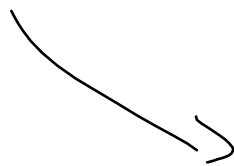
$$x = 3 + 7(4 + 5k) \quad k \in \mathbb{Z}$$

$$x = 31 + 35k$$

$$x \equiv 31 \pmod{35}$$



$$x \equiv 3 \pmod{7}$$



$$x \equiv 1 \pmod{5}$$

---

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

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

has a unique soln  $x \pmod{m_1 \dots m_r}$

↳ also called the Chinese Remainder Thm.

Pf: Define  $M = m_1 \cdots m_r$

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

$$\text{Observe } (L_k, m_k) = 1$$

$$\text{Hence } \exists y_k \in \mathbb{Z} : L_k y_k \equiv 1 \pmod{m_k}$$

$$\text{So } a_k L_k y_k \equiv a_k \pmod{m_k}$$

$$\text{Define } x = a_1 L_1 y_1 + a_2 \overset{\substack{\uparrow \\ \text{mult. of } m_1}}{L_2 y_2} + \cdots + a_r \overset{\substack{\uparrow \\ \text{mult. of } m_r}}{L_r y_r}$$

$$\text{Observe: } x \equiv a_1 L_1 y_1 \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 L_2 y_2 \equiv a_2 \pmod{m_2}$$

$\vdots$

$$x \equiv a_r \pmod{m_r}$$

Next: show uniqueness. (mod  $M$ )

Suppose  $y \equiv a_1 \pmod{m_1}, \dots, y \equiv a_k \pmod{m_k}$

Goal: show  $y \equiv x \pmod{M}$

Note  $y \equiv a_1 \equiv x \pmod{m_1} \rightarrow m_1 \mid y - x$   
 $\vdots$   
 $y \equiv a_r \equiv x \pmod{m_r} \rightarrow m_r \mid y - x$

Since  $m_1, \dots, m_r$  are pairwise rel.

prime,  $m_1 \dots m_r \mid y - x \rightarrow y \equiv x \pmod{M}$

---

Ex: Solve  $x \equiv 1 \pmod{2}$

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

Note 2, 3, 5 are pairwise rel. prime

$$M = \underset{m_1}{2} \cdot \underset{m_2}{3} \cdot \underset{m_3}{5} = 30$$

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

① Solve  $L_k y_k \equiv 1 \pmod{m_k}$

$$15 y_1 \equiv 1 \pmod{2} \quad (\text{apply: if } a \equiv b \pmod{m} \text{ then } ac \equiv bc \pmod{m})$$

$$1 \cdot y_1 \equiv 1 \pmod{2} \leftarrow \underline{y_1 = 1}$$

$$10 y_2 \equiv 1 \pmod{3}$$

$$y_2 \equiv 1 \pmod{3} \leftarrow y_2 = 1$$

$$6 y_3 \equiv 1 \pmod{5}$$

$$y_3 \equiv 1 \pmod{5} \leftarrow y_3 = 1$$

Since  $15 \equiv 1 \pmod{2}$   
then  $15 y_1 \equiv y_1 \pmod{2}$

Also  $15 y_1 \equiv 1 \pmod{2}$

$y_1$

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

$$= 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 15 + 20 + 18 = 53$$