Tue Oct 27

Chinese remainder theorem

$$X \equiv a_1 \pmod{m_1}$$
$$X \equiv a_2 \pmod{m_2}$$
$$X \equiv a_3 \pmod{m_3}$$

m's are pairwise relatively prime

a's are arbitrary

Define $m := m_1 m_2 m_3$

$$M_1 := m/m_1 = m_2 m_3$$
$$M_2 := m/m_2 = m_1 m_3$$
$$M_3 := m/m_3 = m_1 m_2$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

y_1: inverse

$$M_2 y_2 \equiv 1 \pmod{m_2}$$
$$M_3 y_3 \equiv 1 \pmod{m_3}$$

The solution

$$X := a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$

Therefore

$$X \equiv a_1 \underbrace{M_1 y_1}_{\equiv 1} \pmod{m_1}$$
$$X \equiv a_1 \pmod{m_1}$$

The remaining terms go away!

$$a_2 M_2 y_2 = a_2 m_1 m_3 y_2 = m_1 (a_2 m_3 y_2) \equiv 0 \pmod{m_1}$$

$$x \equiv a_2 M_2 y_2 \pmod{m_2}$$

$$\equiv 1$$

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

the rest of the terms of x go away when doing mod 2

$$a_3 M_3 y_3 = a_3 m_1 m_2 y_3$$

$$= m_2 (a_3 m_1 y_3)$$

$$\equiv 0 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

Solution: all integers congruent with x mod m

The solution is unique.

VERIFY the SOLUTION on the original equations!

If we had 2 solutions

$$\left.\begin{array}{l} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \\ \vdots \\ X \equiv a_k' \pmod{m_k} \end{array}\right\} \quad \left.\begin{array}{l} Z \equiv a_1 \pmod{m_1} \\ Z \equiv a_2 \pmod{m_2} \\ \vdots \\ Z \equiv a_k' \pmod{m_k} \end{array}\right.$$

Then

$$X - Z \equiv 0 \pmod{m_1}$$
$$X - Z \equiv 0 \pmod{m_2}$$
$$\vdots$$
$$X - Z \equiv 0 \pmod{m_k}$$

then

$$X - Z \equiv 0 \pmod{\underbrace{m_1 m_2 \ldots m_k}_{m}}$$

then

$$X \equiv Z \pmod{m}$$