Chinese Remainder Theorem

Learning Objectives. By the end of class, students will be able to:

- Solve system of linear equations in one variable.
- Prove the Chinese Remainder Theorem. .

Example 1. Consider the system of linear equations

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 1 \pmod 8. \end{aligned}$$

A slow way to find an integer x that satisfies all three congruences is to write out the congruence classes:

$$\begin{aligned} &2, 2+5, 2+5(2), \boxed{2+5(3)}, \ldots \\ &3, 3+7, \boxed{3+7(2)}, 3+7(3), \ldots \\ &1, 1+8, 1+8(2), \boxed{1+8(3)}, \ldots \end{aligned}$$

and see what integers are on all three lists. In addition to being tedius, we this doesn't help find *all* such integers.

To find all such integers, define $M = 5(7)(8) = 280$, and $M_1 = \dfrac{M}{5} = 7(8), M_2 = \dfrac{M}{7} = 5(8), M_3 = \dfrac{M}{8} = 5(7)$. Then each M_i is relatively prime to M by construction. Thus, by **??** the congruences

$$\begin{aligned} M_1x_1 &\equiv 1 \pmod 5, & 7(8)x_1 &\equiv x_1 \equiv 1 \pmod 5 \\ M_2x_2 &\equiv 1 \pmod 7, & 5(8)x_2 &\equiv 5x_2 \equiv 1 \pmod 7 \\ M_3x_3 &\equiv 1 \pmod 8, & 5(7)x_3 &\equiv 3x_3 \equiv 1 \pmod 8 \end{aligned}$$

have solutions. Thus, $x_1 \equiv 1 \pmod 5, x_2 \equiv 3 \pmod 7$, and $x_3 \equiv 3 \pmod 8$.

Note that

$$\begin{aligned} M_1x_1(2) &= 56(1)(2) \equiv 2 \pmod 5, & M_2 &\equiv M_3 \equiv 0 \pmod 5 \\ M_2x_2(3) &= 40(3)(3) \equiv 3 \pmod 7, & M_1 &\equiv M_3 \equiv 0 \pmod 7 \\ M_3x_3(1) &= 35(3)(1) \equiv 1 \pmod 8, & M_1 &\equiv M_2 \equiv 0 \pmod 8 \end{aligned}$$

Thus,

$$x = M_1x_1(2) + M_2x_2(3) + M_3x_3(1) = 56(1)(2) + 40(3)(3) + 35(3)(1)$$

is a solution to all three congruences.

Learning outcomes:
Author(s): Claire Merriman

Theorem 1 (Chinese Remainder Theorem)**.** Let $m_1, m_2, \ldots m_k$ be pairwise relatively prime positive integers (that is, any pair $\gcd(m_i, m_j) = 1$ when $i \neq j$). Let $b_1, b_2, \ldots, b_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_k$. This solution has the form

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k,$$

where $M_i = \dfrac{M}{m_i}$ and $M_i x_i \equiv 1 \pmod{m_i}$.

Proof Let $m_1, m_2, \ldots m_k$ be pairwise relatively prime positive integers. We start by constructing a solution modulo $M = m_1 m_2 \ldots m_k$. By construction, $M_i = \dfrac{M}{m_i}$ is an integer. Since each the m_i are pairwise relatively prime, $(M_i, m_i) = 1$. Thus, by **??**, for each i there is an integer x_i where $M_i x_i \equiv 1 \pmod{m_i}$. Thus $M_i x_i b_i \equiv b_i \pmod{m_i}$. We also have that $(M_i, m_j) = m_j$ when $i \neq j$, so $M_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Let

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k.$$

Then $x \equiv M_i x_i b_i \equiv b_i \pmod{m_i}$ for each $i = 1, 2, \ldots, k$ and $x \equiv M_i x_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Thus, we have found a solution to the system of equivalences.

To show the solution is unique modulo M, consider two solutions x_1, x_2. Then $x_1 \equiv x_2 \pmod{m_i}$ for each $i = 1, 2, \ldots, k$. Thus $m_i \mid x_2 - x_1$. Since $(m_i, m_j) = 1$ when $i \neq j$, $M = [m_1, m_2, \ldots, m_k]$ and $M \mid x_2 - x_1$. Thus, $x_1 \equiv x_2 \pmod{M}$. ■