§5.3 The Chinese Remainder Theorem

Having considered single linear congruences in §5.1, we now turn to systems of linear congruences

\[ a_1x \equiv b_1 \pmod{m_1} \]
\[ a_2x \equiv b_2 \pmod{m_2} \]
\[ \vdots \]
\[ a_s x \equiv b_s \pmod{m_s}. \]

We are interested in integer solutions to this system. Such a system does not always have solutions.

\[ \text{Ex. } \begin{cases} 5x \equiv 1 \pmod{6} \text{ has no solution} \smallskip \\ x \equiv 1 \pmod{14} \end{cases} \]

So it is necessary to require that all the \( m_1, m_2, \ldots, m_s \) are pairwise coprime.

\[ \text{Ex. } \text{Replace } 3x \equiv 11 \pmod{2275} \text{ by a system of linear congruences} \]
\[ 2275 = 5^2 \cdot 7 \cdot 13. \]

By the Fund. of Arithmetic, \( 3x \equiv 11 \pmod{2275} \) can be
replaced by the system

\[ 3x \equiv 11 \pmod{23} \]
\[ 3x \equiv 11 \pmod{71} \]
\[ 3x \equiv 11 \pmod{13} \]

**Thm 5.5 (The Chinese Remainder Theorem)**

Suppose \( m_1, m_2, m_3, \ldots, m_s \) are pairwise coprime. Let \( M = m_1 m_2 \cdots m_s \), and suppose that \( a_1, a_2, \ldots, a_s \) are integers such that \( \gcd(a_i, m_i) = 1 \) for each \( i \). Then the \( s \) congruences

\[ a_1 x \equiv b_1 \pmod{m_1} \]
\[ a_2 x \equiv b_2 \pmod{m_2} \]
\[ \quad \vdots \]
\[ a_s x \equiv b_s \pmod{m_s} \]

have a simultaneous solution that is unique modulo \( M \).

**Proof.** First we find integers \( c_1, c_2, \ldots, c_s \) such that

\[ a_i c_i \equiv b_i \pmod{m_i} \]

Let \( n_i = M / m_i \). We have \( \gcd(n_i, m_i) = 1 \). Hence,

there exist \( \overline{n_i} \) such that \( n_i \overline{n_i} \equiv 1 \pmod{m_i} \).

Now we construct the number

\[ x_0 = c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + \cdots + c_s n_s \overline{n_s} \]
We can check that $x_0$ is a solution to the system since:

$$a_i x_0 \equiv a_i c_i \pmod{m_i} \quad \forall i \in \{1, 2, \ldots, r\}$$

$$\equiv \frac{a_i c_i \pmod{m_i}}{a_i c_i \pmod{m_i}} \quad \forall i \in \{1, 2, \ldots, r\}$$

$$\equiv b_i - 1 \pmod{m_i}$$

Any other solution must be congruent to $x_0$ modulo $M$.

---

**Ex** Solve the system

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$x \equiv 23 \pmod{105}$

---

**Ex** Solve the system

$$\begin{cases} 3x \equiv 1 \pmod{5} \\ 4x \equiv 6 \pmod{14} \\ 5x \equiv 11 \pmod{3} \end{cases}$$