The Chinese Remainder Theorem

THEOREM (The Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_r$.

EXAMPLE: Solve the system

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Solution: We use Theorem 1 from Section 4.1 to rewrite the first congruence as an equality, namely, $x = 5t + 1$, where t is an integer. Inserting this expression for x into the second congruence, we find that

$$\begin{aligned} 5t + 1 &\equiv 2 \pmod{6} \\ 5t &\equiv 1 \pmod{6} \end{aligned}$$

which can easily be solved to show that

$$t \equiv 5 \pmod{6}$$

Using Theorem 1 again, we write $t = 6u + 5$, where u is an integer. Hence,

$$x = 5(6u + 5) + 1 = 30u + 26$$

When we insert this expression for x into the third congruence, we obtain

$$\begin{aligned} 30u + 26 &\equiv 3 \pmod{7} \\ 30u &\equiv -23 \pmod{7} \end{aligned}$$

When this congruence is solved, we find that

$$u \equiv 6 \pmod{7}$$

Consequently, Theorem 1 tells us that $u = 7v + 6$, where v is an integer. Hence

$$x = 30(7v + 6) + 26 = 210v + 206$$

Translating this equality into a congruence, we find that

$$x \equiv 206 \pmod{210}$$

and this is the simultaneous solution.