Chinese Remainder Theorem

Theorem 2.15 (Chinese Remainder Theorem) *Let $m_1, \ldots, m_n$ be pairwise relatively prime positive integers and let $b_1, \ldots, b_n$ be any integers. Then the system of linear congruences in one variable given by*

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \quad \vdots \\ x \equiv b_n \mod m_n \end{cases}$$

has a unique solution modulo $m_1 \cdots m_n$.

Proof. We first construct a solution. Let $M = m_1 \cdots m_n$ and, for each *i*, $M_i = M/m_i$. Note that $(M_i, m_i) = 1$ for every *i*. Thus,

$$M_i x_i \equiv 1 \bmod m_i$$

has a solution x_i. Define

$$x = b_1 M_1 x_1 + \cdots + b_n M_n x_n.$$

Since

$$m_i \mid M_j \quad \text{for all} \quad j \neq i,$$

we see that

$$x = b_1 M_1 x_1 + \cdots + b_i M_i x_i + \cdots + b_n M_n x_n \equiv b_i \pmod{m_i}.$$

To see the uniqueness, Let *x*' be another solution. Then $x \equiv x' \bmod m_i$ for each *i*. Noting that all m_i 's are pairwise relatively prime, we have that $x \equiv x' \bmod M$, i.e., the solution *x* is unique.

Donald Hazlewood and Carol Hazlewood
Wed Jun 5 14:35:14 CDT 1996