The Chinese Remainder Theorem

The Chinese Remainder Theorem

Theorem: Suppose that $m_1, m_2, ..., m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, ..., a_r$ be integers. Then the system of congruences, $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 \times m_2 \times ... \times m_r$, which is given by:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r \pmod{M},$$

where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \le i \le r$.

Pf: Notice that $\gcd(M_i, m_i) = 1$ for $1 \le i \le r$. Therefore, the y_i all exist (determined easily from the extended Euclidean Algorithm). Now, notice that since $M_i y_i \equiv 1 \pmod{m_i}$, we have $a_i M_i y_i \equiv a_i \pmod{m_i}$ for $1 \le i \le r$. On the other hand, $a_i M_i y_i \equiv 0 \pmod{m_j}$ if $j \ne i$ (since $m_j \mid M_i$ in this case). Thus, we see that $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$.

If x_0 and x_1 were solutions, then we would have $x_0 - x_1 \equiv 0 \pmod{m_i}$ for all i, so $x_0 - x_1 \equiv 0 \pmod{M}$, i.e., they are the same modulo M.

Example

Find the smallest multiple of 10 which has remainder 2 when divided by 3, and remainder 3 when divided by 7.

We are looking for a number which satisfies the congruences, $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 7$, $x \equiv 0 \bmod 2$ and $x \equiv 0 \bmod 5$. Since, 2, 3, 5 and 7 are all relatively prime in pairs, the Chinese Remainder Theorem tells us that there is a unique solution modulo 210 ($= 2 \times 3 \times 5 \times 7$). We calculate the M_i's and y_i's as follows:

$M_2 = 210/2 = 105;$ $y_2 \equiv (105)^{-1} \pmod 2 = 1$

$M_3 = 210/3 = 70;$ $y_3 \equiv (70)^{-1} \pmod 3 = 1$

$M_5 = 210/5 = 42;$ $y_5 \equiv (42)^{-1} \pmod 5 = 3$ and

$M_7 = 210/7 = 30;$ $y_7 \equiv (30)^{-1} \pmod 7 = 4.$

So, $x \equiv 0(M_2y_2) + 2(M_3y_3) + 0(M_5y_5) + 3(M_7y_7) \equiv 0 + 2(70)(1) + 0 + 3(30)(4) \equiv 140 + 360 \equiv 500 \bmod 210 \equiv \mathbf{80}$.

Notes

Remark 1: The theorem is valid in much more general situations than we have presented here.

Remark 2: The condition given is sufficient, but not necessary for a solution. Necessary and sufficient conditions exist but we are not presenting them.

Remark 3: It is purported that Sun Tsu was aware of this result in the first century A.D.