

The Chinese Remainder Theorem

Chinese Remainder Theorem Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers, i.e., $\gcd(m_i, m_j) = 1$ for $i \neq j$. The system

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

has a unique solution modulo $m = m_1 m_2 \cdots m_n$, i.e., there is a unique solution x with $0 \leq x < m$. Furthermore, all solutions are congruent modulo m .

We can construct a solution as follows.

1. Let $m = m_1 m_2 \cdots m_n$.
2. Let $M_k = \frac{m}{m_k}$ for all $k = 1, 2, \dots, n$.
3. For all $k = 1, 2, \dots, n$, find integers y_k such

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Since $\gcd(M_k, m_k) = 1$, we know that y_k exists. Euclid's extended algorithm can be used to find y_k .

4. The integer

$$a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

is a solution of the system.

The integer $x = (a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n) \pmod{m}$ is the unique solution with $0 \leq x < m$.

For example, let's find the smallest positive integer x such that

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 5 \pmod{7} \\x &\equiv 8 \pmod{11}\end{aligned}$$

1. $m = 3(7)(11) = 231$.
2. $M_1 = \frac{231}{3} = 77$, $M_2 = \frac{231}{7} = 33$, $M_3 = \frac{231}{11} = 21$.
3. We now find y_1, y_2 , and y_3 .

$$\begin{aligned}77y_1 &\equiv 1 \pmod{3} \longrightarrow y_1 = 2 \\33y_2 &\equiv 1 \pmod{7} \longrightarrow y_2 = 3 \\21y_3 &\equiv 1 \pmod{11} \longrightarrow y_3 = 10\end{aligned}$$

4. The smallest positive integer solution is then

$$\begin{aligned}x &= (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \pmod{m} \\&= (2(77)(2) + 5(33)(3) + 8(21)(10)) \pmod{231} \\&= 2483 \pmod{231} \\&= 173.\end{aligned}$$