Chinese Reminder Theorem

The *Chinese Reminder Theorem* is an ancient but important calculation algorithm in modular arithmetic. The Chinese Remainder Theorem enables one to solve simultaneous equations with respect to different moduli in considerable generality. Here we supplement the discussion in T&W, §3.4, pp. 76-78.

The problem

Here is the statement of the problem that the Chinese Remainder Theorem solves.

Theorem (Chinese Remainder Theorem). *Let* $m_1, \ldots, m_k$ *be integers with* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$. *Let* m *be the product* $m = m_1 m_2 \cdots m_k$. *Let* $a_1, \ldots, a_k$ *be integers. Consider the system of congruences:*

$$(*) \qquad \begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Then there exists exactly one $x \in \mathbf{Z}_m$ *satisfying this system.*

The algorithm

The solution to the system (*) may be obtained by the following algorithm.

Theorem (Chinese Remainder Theorem Algorithm). *We may solve the system (*) as follows.*

(1) For each $i = 1, \ldots, k$, *let* $z_i = m/mi = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$.

(2) For each $i = 1, \ldots, k$, *let* $y_i = z_i^{-1} \pmod{m_i}$. *(Note that this is always possible because* $\gcd(z_i, m_i) = 1$.*)*

(3) The solution to the system (*) is $x = a_1 y_1 z_1 + \cdots + a_k y_k z_k$.

Proof. Why does the Chinese Remainder Theorem algorithm work? The notation makes the proof surprisingly simple to state. Let's study $x = a_1 y_1 z_1 + \cdots + a_k y_k z_k$ and compute $x \pmod{m_1}$ for example. The same argument will work for $x \pmod{m_i}$ for $i > 1$. The key observation (and a very clever one too) is that $z_i \equiv 0 \pmod{m_1}$ when $i \neq 1$ since m_1 divides $z_i = m/mi = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$. Thus when we compute $x \pmod{m_1}$, we obtain $x \equiv a_1 y_1 z_1 \pmod{m_1}$. But $y_1 z_1 \equiv 1 \pmod{m_1}$ by (2), and we obtain $x \equiv a_1 \pmod{m_1}$. □

Example of the Chinese Remainder Theorem

Use the Chinese Remainder Theorem to find all solutions in $\mathbf{Z}_{60}$ such that

$$\begin{aligned} x &\equiv 3 \bmod 4 \\ x &\equiv 2 \bmod 3 \\ x &\equiv 4 \bmod 5. \end{aligned}$$

We solve this in steps.

Step 0 Establish the basic notation. In this problem we have $k = 3$, $a_1 = 3$, $a_2 = 2$, $a_3 = 4$, $m_1 = 4$, $m_2 = 3$, $m_3 = 5$, and $m = 4 \cdot 3 \cdot 5 = 60$.

Step 1 Implement step (1). $z_1 = m/m_1 = 60/4 = 3 \cdot 5 = 15$, $z_2 = 20$, and $z_3 = 12$.

Step 2 Implement step (2). We solve $z_i y_i \equiv 1 \bmod m_i$, $i = 1, 2, 3$. In this problem, we need to solve

$$\begin{aligned} 15y_1 &\equiv 1 \bmod 4 \\ 20y_2 &\equiv 1 \bmod 3 \\ 12y_3 &\equiv 1 \bmod 5. \end{aligned}$$

The y_i can be computed using the tally table version of the generalized Euclidean algorithm (cf. *Congruence Supplement*). For example, in the first equation for y_1, the tally method automatically solves $15y_1 + 4t = 1$ for y_1 and t, and we find that $y_1 = 3$. Continuing, we find that $y_1 = 3$, $y_2 = 2$, and $y_3 = 3$.

Step 3 Implement step (3). $x \equiv a_1 y_1 z_1 + a_2 y_2 z_2 + a_3 y_3 z_3 \pmod{60}$. Substituting, we obtain $3 \cdot 3 \cdot 15 + 2 \cdot 2 \cdot 20 + 4 \cdot 3 \cdot 12 = 359$ which reduces to $x \equiv 59 \pmod{60}$. $\square$

An application

The text (p. 74) emphasizes the opposite line of thought from the above. Now we wish to solve the equation $x \equiv a \pmod{m}$ where m is a multiple of two or more pairwise relatively prime integers. The Chinese Remainder Theorem Algorithm tells us that the x is precisely the solution to the modular system

$$(*) \qquad \begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Here the numbers m_i come by factoring $m = m_1 m_2 \cdots m_k$ where $\gcd(m_i, m_j) = 1$ whenever $i \neq j$.

Why do this? This is answered in the text (T&W, p. 77). By breaking the problem into simultaneous congruences mod each prime factor of m, we can recombine the resulting information to obtain an answer for each prime factor power of m. The advantage is that it is often easier to analyze congruences mod primes (or mod prime powers) than to work with composite numbers.

Example. Here is an example. Find a solution to $13x \equiv 1 \pmod{70}$. The two methods of solution are worthy of careful study.

Answer. We can do this particular example two ways. First notice that $13^{-1} = 27 \pmod{70}$ by the usual tally table generalization of the Euclidean algorithm. So the given problem is equivalent to $x \equiv 27 \pmod{70}$.

We can also do it by the Chinese Remainder Theorem. Now $70 = 2 \cdot 5 \cdot 7$. First solve

$$\begin{aligned} 13r_1 &\equiv 1 \bmod 2 \\ 13r_2 &\equiv 1 \bmod 5 \\ 13r_3 &\equiv 1 \bmod 7, \end{aligned}$$

obtaining $r_1 = 1$, $r_2 = 2$, and $r_3 = 6$. Now solve

$$\begin{aligned} x &\equiv r_1 = 1 \pmod{2} \\ x &\equiv r_2 = 2 \pmod{5} \\ x &\equiv r_3 = 6 \pmod{7} \end{aligned}$$

by the Chinese Remainder Theorem, obtaining $x = 27 \in \mathbf{Z}_{70}$ once more.

