

Chinese Remainder Theorem

Theorem. Suppose that m_1, m_2, \dots, m_r are pairwise relatively prime positive integers, and let a_1, a_2, \dots, a_r be integers. Then the system of congruences,

$$x \equiv a_k \pmod{M_k} \text{ for } k = 1, 2, \dots, r$$

has a unique solution modulo $M = M_1 \times M_2 \times \dots \times M_r$, which is given by:

$$x \equiv a_1 M_1 b_1 + a_2 M_2 b_2 + \dots + a_r M_r b_r \pmod{M},$$

where $M_k = M/m_k$ and $b_k \equiv (M_k)^{-1} \pmod{m_k}$ for $k = 1, 2, \dots, r$.

Proof. Notice that $\gcd(M_k, m_k) = 1$ for $k = 1, 2, \dots, r$. Therefore, every b_k exists (and can be determined easily from the extended Euclidean Algorithm). Now, notice that since $M_k b_k \equiv 1 \pmod{m_k}$, we have $a_k M_k b_k \equiv a_k \pmod{m_k}$ for $k = 1, 2, \dots, r$. On the other hand, $a_k M_k b_k \equiv 0 \pmod{m_j}$ if j is not k (since m_j divides M_k in this case). Thus, we see that $x \equiv a_k \pmod{m_k}$ for $k = 1, 2, \dots, r$. If there were two solutions, say x_0 , and x_1 , then we would have $x_0 - x_1 \equiv 0 \pmod{m_k}$ for $k = 1, 2, \dots, r$, 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,

$$x \equiv 2 \pmod{3}, x \equiv 3 \pmod{7}, x \equiv 0 \pmod{2} \text{ and } x \equiv 0 \pmod{5}.$$

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_k 's and b_k 's as follows:

$$M_1 = 210/2 = 105; b_1 \equiv (105)^{-1} \pmod{2} = 1$$

$$M_2 = 210/3 = 70; b_2 \equiv (70)^{-1} \pmod{3} = 1$$

$$M_3 = 210/5 = 42; b_3 \equiv (42)^{-1} \pmod{5} = 3$$

$$M_4 = 210/7 = 30; b_4 \equiv (30)^{-1} \pmod{7} = 4.$$

We have:

$$\begin{aligned} x &\equiv 0(M_1 b_1) + 2(M_2 b_2) + 0(M_3 b_3) + 3(M_4 b_4) \\ &= 0 + 2(70)(1) + 0 + 3(30)(4) = 140 + 360 \\ &= 500 \pmod{210} \equiv 80. \end{aligned}$$

California State University, East Bay

The Chinese mathematician Sun Tsu was aware of this result in the first century A.D.

♠ **The Extended Euclidean Algorithm.** This algorithm finds the inverse of a number $x \bmod (n)$. First we set $x_0 = x$ and $x_1 = n$. The quotient obtained at step k will be denoted by q_k . As we carry out each step of the Euclidean Algorithm, we will also calculate an auxiliary number, p_k . For the first two steps, the value of this number is given: $p_0 = 0$ and $p_1 = 1$. For the remainder of the steps, we recursively calculate

$$p_k \equiv p_{k-2} - p_{k-1}q_{k-2} \bmod (n).$$

Continue this calculation for one step beyond the last step of the Euclidean algorithm. The algorithm starts by dividing n by x .

Case 1. The last non-zero remainder occurs at step k , then if this remainder is 1, x has an inverse and it is p_{k+2} .

Case 2. The last non-zero remainder is not 1, then x does not have an inverse.

Example. Find the inverse of 15 *mod* 26.

First we set $x_0 = 15$ and $x_1 = 26$.

<i>Steps</i>	$x_{k+1} = q_k(x_k) + r_k$	$p_k \equiv p_{k-2} - p_{k-1}q_{k-2} \bmod n$
<i>Step 0</i>	$26 = 1(15) + 11$	$p_0 = 0$
<i>Step 1</i>	$15 = 1(11) + 4$	$p_1 = 1$
<i>Step 2</i>	$11 = 2(4) + 3$	$p_2 \equiv 0 - 1(1) \bmod 26 = 25$
<i>Step 3</i>	$4 = 1(3) + 1^\dagger$	$p_3 \equiv 1 - 25(1) \bmod 26 \equiv -24 \bmod 26 = 2$
<i>Step 4</i>	$3 = 3(1) + 0$	$p_4 \equiv 25 - 2(2) \bmod 26 = 21$
<i>Step 5</i>	<i>The inverse is found</i>	$p_5 \equiv 2 - 21(1) \bmod 26 \equiv -19 \bmod 26 = 7$

$\dagger r_3 = 1$, so the inverse of 15 modulo 26 exists.