The Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$X \equiv a_1 \pmod{m_1}$

$X \equiv a_2 \pmod{m_2}$

. . .

$X \equiv a_n \pmod{m_n}$

CRT states that the above equations have a unique solution of the moduli are relatively prime.

$X = (a_1M_1\,M_1^{-1} + a_2M_2M_2^{-1} + \ldots + a_nM_nM_n^{-1}) \bmod M$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod{3}$

$X \equiv 3 \pmod{5}$

$X \equiv 2 \pmod{7}$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod{3}$

$X \equiv 3 \pmod{5}$

$X \equiv 2 \pmod{7}$

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

The Chinese Remainder Theorem

$X \equiv a_1 \pmod{m_1}$	$X \equiv 2 \pmod{3}$
$X \equiv a_2 \pmod{m_2}$	$X \equiv 3 \pmod{5}$
$X \equiv a_3 \pmod{m_3}$	$X \equiv 2 \pmod{7}$

The Chinese Remainder Theorem

$X \equiv a_1 \pmod{m_1}$	$X \equiv 2 \pmod{3}$
$X \equiv a_2 \pmod{m_2}$	$X \equiv 3 \pmod{5}$
$X \equiv a_3 \pmod{m_3}$	$X \equiv 2 \pmod{7}$

Solution:

$$X = (a_1M_1M_1^{-1} + a_2M_2M_2^{-1} + a_3M_3M_3^{-1}) \bmod M$$

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	M
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	M
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	M
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

Solution:

$$M = m_1 \times m_2 \times m_3$$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	$M=105$
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

Solution:

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$M = 105$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 =$	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	$M_2 =$	M_2^{-1}	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 =$	M_3^{-1}	

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 =$	M_1^{-1}	$M = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 =$	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	$M_3 =$	M_3^{-1}	

$$M_1 = \frac{M}{m_1}$$

$$M_2 = \frac{M}{m_2}$$

$$M_3 = \frac{M}{m_3}$$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 =$	M_1^{-1}	
$a_2 = 3$	$m_2 = 5$	$M_2 =$	M_2^{-1}	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 =$	M_3^{-1}	

$$M_1 = \frac{M}{m_1}$$

$$M_1 = \frac{105}{3}$$

$$M_1 = 35$$

$$M_2 = \frac{M}{m_2}$$

$$M_2 = \frac{105}{5}$$

$$M_2 = 21$$

$$M_3 = \frac{M}{m_3}$$

$$M_3 = \frac{105}{7}$$

$$M_3 = 15$$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	M_1^{-1}	$M=105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	M_3^{-1}	

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

$35 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod 5$

$21 \times 1 = 1 \bmod 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

$35 \times 2 = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod 5$

$21 \times 1 = 1 \bmod 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

The Chinese Remainder Theorem

Given		To Find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$M = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

Solution:

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod{3}$

$X \equiv 3 \pmod{5}$

$X \equiv 2 \pmod{7}$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (2x35x2 + 3x21x1 + 2x15x1) \bmod 105$$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	$M = 105$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$$

$$= 233 \bmod 105$$

The Chinese Remainder Theorem

Example 1: Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$M = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

Solution:

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$X = 23$