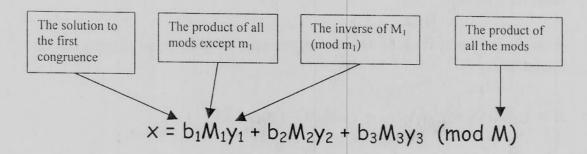
## Solving Systems of Linear Congruences Using the Chinese Remainder Theorem

example 1:  $x \equiv 2 \pmod{3}$   $x \equiv 3 \pmod{5}$  $x \equiv 2 \pmod{7}$ 

The solution can be found using the following equation:



<u>Step 1</u>: Start with the equations you want to solve. In order for the CRT to apply, the mods must be relatively prime, so check this. Then, calculate M (the mod for your answer) by multiplying the mods from the congruences.

In this example, the answer will be mod  $(3 \times 5 \times 7) = \text{mod } 105$ 

<u>Step 2</u>: For each equation,  $x \equiv b_k \pmod{m_k}$ , calculate  $M_k$  by finding the product of the mods from the OTHER congruences, ie.  $M_k = M/m_k$ . Set up the congruences to find the inverses of the  $M_k$ 's (mod  $m_k$ ).

$$35y_1 \equiv 1 \pmod{3}$$
  $21y_2 \equiv 1 \pmod{5}$   $15y_3 \equiv 1 \pmod{7}$ 

Step 3: Solve each of these for yk.

$$35y_1 \equiv 1 \pmod{3}$$
  $21y_2 \equiv 1 \pmod{5}$   $15y_3 \equiv 1 \pmod{7}$   $y_1 \equiv 2 \pmod{3}$   $y_2 \equiv 1 \pmod{5}$   $y_3 \equiv 1 \pmod{7}$ 

<u>Step 4</u>: For each equation multiply together the numbers  $b_k$  (occurring in the original equation), the  $M_k$  (the product of all the other mods) and the  $y_k$  found in step 3. Then add them all up.

$$x \equiv 2(35)(2) + 3(21)(1) + 2(15)(1) \pmod{105}$$
  
 $\equiv 233 \equiv 23 \pmod{105}$ 

In the general case, we are solving congruences of the form:

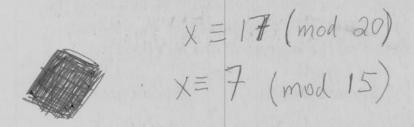
$$a_k x = b_k \pmod{m_k}$$

Now it is important to check that  $gcd(a_k,m_k)$  divides  $b_k$ . If it does, we have one or more solutions,  $c_1$ ,  $c_2$ , ...,  $c_d$  where  $d = gcd(a_k,m_k)$ . If it doesn't, we have no solutions.

A solution to a system of these congruences (if a solution exists) can be found using:

$$x = c_1 M_1 y_1 + c_2 M_2 y_2 + c_r M_r y_r \pmod{M}$$

(The M,  $M_k$ 's and  $y_k$ 's are as before. The  $c_k$ 's are solutions to the individual congruences.)



13 39