MATH 253: CHINESE REMAINDER THEOREM

DAN YASAKI

1. Set-up

Theorem 1.1. *Let* $m = m_1 m_2 \cdots m_r$ *with* $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$. *Then the system*

$$\left\{ \begin{array}{lll} x & \equiv & a_1 \pmod{m_1} \\ x & \equiv & a_2 \pmod{m_2} \\ & \vdots & \\ x & \equiv & a_r \pmod{m_r} \end{array} \right\}$$

has a unique solution modulo m, *given by*

$$x = a_1 e_1 + a_2 e_2 + \cdots + a_r e_r, \quad \textit{where } e_i = t_i w_i,$$

with

$$w_i = \frac{m}{m_i} = \prod_{\substack{1 \leq j \leq r \\ j \neq i}} m_j \quad \textit{and} \quad t_i w_i \equiv 1 \pmod{m_i}.$$

Remark. Roughly speaking, the e_i is 1 in the $\bmod m_i$ direction and 0 in the $\bmod m_j$ direction for $i \neq j$.

Steps to solve CRT problem.

(1) Identify a_i and m_i.
(2) Compute m and w_i.
(3) Compute t_i, the inverse of w_i modulo m_i.
(4) There is a unique solution modulo m

$$x = a_1 t_1 w_1 + a_2 t_2 w_2 + \cdots + a_r t_r w_r.$$

2. Exercises

(1) (Note: This problem is outdated.) My younger son had 500 action figures before we moved to Greensboro. He has not bought any new ones, but he lost a few in the process of the move, and he wants to know how many he has now. He can only count accurately to 10, but he knows that you are a number theorist, and he has faith in you. He reports that there is an odd number left. When you tell him that is not enough information, he reports that there is 1 left over if he lines them up 5 at a time, 2 left over if he lines the up 7 at a time, and 3 left over if he lines them up 9 at a time. How many action figures does he have?
(2) Pick a secret number from 1 to 100. Make your own CRT type puzzle and put it on the board for others to solve.

3. Solution to (1)

Let x be the number of action figures my son has. Then

$$\begin{aligned} x &\equiv 1 \pmod 2 && \text{since } x \text{ is odd} \\ x &\equiv 1 \pmod 5 && \text{since there is 1 left over in rows of 5} \\ x &\equiv 2 \pmod 7 && \text{since there is 2 left over in rows of 7} \\ x &\equiv 3 \pmod 9 && \text{since there is 3 left over in rows of 9} \end{aligned}$$

Note that we can solve for x using CRT since

$$\gcd(2,5) = \gcd(2,7) = \gcd(2,9) = \gcd(5,7) = \gcd(5,9) = \gcd(7,9) = 1.$$

Let's follow the steps (1)–(4) given above.

(1) We identify a_i and m_i. We have

$$a_1 = 1, m_1 = 2 \quad a_2 = 1, m_2 = 5 \quad a_3 = 2, m_3 = 7 \quad a_4 = 3, m_4 = 9.$$

(2) We compute

$$\begin{aligned} m &= m_1 m_2 m_3 m_4 = 630 \\ w_1 &= m_2 m_3 m_4 = 315 \\ w_2 &= m_1 m_3 m_4 = 126 \\ w_3 &= m_1 m_2 m_4 = 90 \\ w_4 &= m_1 m_2 m_3 = 70. \end{aligned}$$

(3) t_1: The inverse of 315 modulo 2 is the same as the inverse of 1 modulo 2, which is 1 by inspection. Specifically, we choose $t_1 = 1$.

t_2: The inverse of 126 modulo 5 is the same as the inverse of 1 modulo 5, which is 1 by inspection. Specifically, we choose $t_2 = 1$.

t_3: The inverse of 90 modulo 7 is the same as the inverse of -1 modulo 7, which is -1. Specifically, we choose $t_3 = -1$ (Note: Some of you will instead say the inverse of 90 modulo 7 is the same as the inverse of 6 modulo 7, which is 6. That is fine as well. My way just keeps the numbers smaller if you are willing to use negative numbers.)

t_4: The inverse of 70 modulo 9 is the same as the inverse of 7 modulo 9, which is 4 by inspection. Specifically, $t_4 = 4$.

(4) We compute

$$\begin{aligned} x &\equiv a_1 t_1 w_1 + a_2 t_2 w_2 + a_3 t_3 w_3 + a_4 t_4 w_4 \pmod{630} \\ &\equiv (1 \cdot 1 \cdot 315) + (1 \cdot 1 \cdot 126) + (2 \cdot (-1) \cdot 90) + (3 \cdot 4 \cdot 70) \pmod{630} \\ &\equiv 1101 \pmod{630} \\ &\equiv 471 \pmod{630}. \end{aligned}$$

In other words, $x = 471 + 630k$ for some integer k. Since my son has less than 500 action figures, he must have 471.

Department of Mathematics and Statistics, The University of North Carolina at Greensboro, Greensboro, NC 27412, USA
E-mail address: d_yasaki@uncg.edu