Solving simultaneous modular arithmetic equations

Dave Neary

January 2, 2021

1 The Chinese Remainder Theorem

Theorem 1.1. *The Chinese Remainder Theorem states that for $n_1, n_2, \cdots, n_k$ pairwise coprime integers greater than 1 (that is, $\gcd(n_i, n_j) = 1, i \neq j$) whose product is N, and integers $a_1, a_2, \cdots, a_k$ with $0 \leq a_i < n_i$, there is a unique integer x such that $0 \leq x < N$ and:*

$$\begin{aligned} x &\equiv a_1 \pmod{x_1} \\ x &\equiv a_2 \pmod{x_2} \\ &\vdots \\ x &\equiv a_k \pmod{x_k} \end{aligned}$$

2 Applying the theorem

We will apply the theorem using a construction method which can also be used to prove the existence and uniqueness of the number x with the following problem:

Question: What is the smallest positive integer that has remainders of 7, 4, and 3 when divided by 8, 9, and 13 respectively?

Since $\gcd(8, 9) = \gcd(8, 13) = \gcd(9, 13) = 1$ we are guaranteed by the Chinese Remainder Theorem that there will be an answer between 0 and $8 \times 9 \times 13 = 936$.

We can construct the solution with the following algorithm. We are given:

$$(m_1, m_2, m_3) = (8, 9, 13)$$
$$(r_1, r_2, r_3) = (7, 4, 3)$$

Define:

$$(M_1, M_2, M_3) = (m_2 \times m_3, m_1 \times m_3, m_1 \times m_2) = (117, 104, 72)$$

We use the extended Euclidean algoritm to find (N_1, N_2, N_3) such that:

$$1 = M_i N_i + m_i n_i, i \in \{1,2,3\}$$

Then we can calculate:

$$x = r_1 N_1 M_1 + r_2 N_2 M_2 + r_3 N_3 M_3 \pmod{m_1 \times m_2 \times m_3}$$

And since $M_i \equiv 0 \pmod{m_j}, i \neq j$, we are guaranteed that x will satisfy each of the congruence relations we want.

For M_1, m_1:

$$\begin{aligned} 117 &= 14 \times 8 + 5 & 5 &= 117 - 14 \times 8 \\ 8 &= 1 \times 5 + 3 & 3 &= 15 \times 8 - 117 \\ 5 &= 1 \times 3 + 2 & 2 &= 2 \times 117 - 29 \times 8 \\ 3 &= 1 \times 2 + 1 & 1 &= 44 \times 8 - 3 \times 117 \end{aligned}$$

Which yields $N_1 = -3$.

Similarly, for M_2, M_3, we get:

$$\begin{aligned} 1 &= 2 \times 104 - 23 \times 9 & N_2 &= 2 \\ 1 &= 2 \times 72 - 11 \times 13 & N_3 &= 2 \end{aligned}$$

Then we can calculate:

$$\begin{aligned} x &= r_1 N_1 M_1 + r_2 N_2 M_2 + r_3 N_3 M_3 \pmod{m_1 \times m_2 \times m_3} \\ x &= 7(-3)(117) + 4(2)(104) + 3(2)(72) \pmod{936} \\ x &= -1193 \pmod{936} = 679 \pmod{936} \end{aligned}$$

And we can find all solutions of these equations in integers by adding or subtracting multiples of the product of the modulos:

$$x = 679 + 936k, k \in \mathbb{Z}$$