Chinese Remainder Theorem

Jonathan Lam

April 4, 2020

This isn't about a proof of the existence or uniqueness, but states the result of the Chinese Remainder Theorem, a method to solve it, and justification for the method. Restating the explanation from Brilliant in my own words. (See `https://brilliant.org/wiki/chinese-remainder-theorem/`.)

Problem

Given a system of linear congruences:

$$\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
x &\equiv a_3 \pmod{n_3} \\
&\vdots \\
x &\equiv a_k \pmod{n_k}
\end{aligned}$$

where $\{n_i\}$ is pairwise coprime (i.e., pairwise/mutually relatively prime).

Result (Chinese Remainder Theorem)

There is a unique solution $x \in \mathbb{Z}_N$, where $N = \prod_{i=1}^{k} n_i$. (Thus, there is a periodic solution in $\mathbb{Z}$ with period N.)

Method

1. Compute N (as stated in the result):

$$N = \prod_{i=1}^{k} n_i$$

2. Compute y_i for each congruence relation:

$$y_i = \frac{N}{n_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k} n_j$$

3. Compute $z_i = y_i^{-1} \mod n_i$ for each congruence relation. (z_i exists since $\{n_i\}$ is pairwise coprime, and thus y_i and n_i are coprime.)
4. Compute x, the unique solution in $\mathbb{Z}_N$ to this system:
$$x = \left(\sum_{i=1}^{k} a_i y_i z_i \right) \mod N$$

In words:

1. Compute the product of all of the divisors.
2. For each congruence relation, calculate the product of all of the other divisors, and find the inverse of that product modulo the current divisor.
3. Sum the products of the a_i and the two numbers calculated in the previous step for each congruence relation.

Proof of method

(This isn't a proof of the CRT, but a proof that the method gives the correct answer.) We can find $x \mod n_i$:

$$x \equiv a_i y_i z_i + \sum_{\substack{j=1 \\ j \neq i}}^{k} a_j y_j z_j \pmod{n_i}$$

Since (by construction)

$$y_i z_i \equiv 1 \pmod{n_i}$$

then

$$a_i y_i z_i \equiv a_i \pmod{n_i}$$

For a different term j, $n_i | y_j$ by construction. Thus:

$$y_j \equiv 0 \pmod{n_i}$$

and thus

$$a_j y_j z_j \equiv 0 \pmod{n_i}$$

Thus $x \equiv a_i \pmod{n_i}$.

Further comments

Two details are left unclear:

- What happens when $\{n_i\}$ is not pairwise coprime? See `https://math.stackexchange.com/questions/1644677`.
- Calculate inverse modulo n_i using extended Euclidean algorithm (general case solves all linear Diophantine equations)?