« Back to my Homepage

# Chinese Remainder Theorem

A look at its usage, proof, and applications.

## Introduction

Some time in the first century AD a Chinese mathematician by the name of Sun Zi published a book, *Sun Zi Suanjing*, or "The Arithmetical Classic of Sun Zi". In this book Sun Zi introduced a method of solving systems of linear congruences that became known as the Chinese Remainder Theorem.

The Chinese Remainder Theorem (abbreviated as "CRT") is easily understood with a riddle:

*An old woman goes to the market with a basket of eggs. She sets the basket down and a horse accidentally steps on it, crushing all the eggs. The rider offers to pay her for the damaged eggs and asks how many eggs did she have. She tells the rider that she cannot remember but that when she had taken all of the eggs out 3 at a time, there were 2 left in the basket. When she took them out 5 at a time, there were 3 left and when she took them out 7 at a time, there were 2 left. What is the smallest number of eggs she could have had?*

To understand how CRT works a few concepts should first be mentioned:

- The *mod* operator, which is used to mathematically define the CRT, is the same as the modulo (%) operator used in many


programming languages.

- In modular arithmetic if $a$ mod $m$ = $b$ mod $m$ this can be expressed as

$$a \equiv b \pmod{m},$$

where $m$ is a positive integer and $a$ and $b$ are integers. This is read as "$a$ is congrugent to $b$ mod $m$".

- A **linear congruence** is a congruence in the form

$$ax \equiv b \pmod{n},$$

where $n$ is a positive integer, $a$ and $b$ are integers, and $x$ is a variable.

- If $a$ and $n$ are relatively prime integers and $n > 1$, then an inverse of $a$ modulo $n$ exists. Furthermore, this inverse is unique modulo $n$. (That is, there is a unique positive integer $\bar{a}$ less than $n$ that is an inverse of $a$ modulo $n$ and every other inverse of $a$ modulo $n$ is congruent to $\bar{a}$ modulo $n$.)

- Two numbers are considered to be relatively prime (or coprime) if their greatest common divisor is 1. A list of numbers considered *pairwise relatively prime* if every two distinct integers $a$ and $b$ in the set are relatively prime (that is, have no common positive divisors other than 1). For example, the set $\{10, 7, 33, 13\}$ is pairwise relatively prime even though individually some of the numbers are composite.

- The up tack symbol ($\perp$) is used to indicate that two integers are coprime.

## Proof and Examples

The Chinese Remainder Theorem states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $n_i \perp n_j$ for all $i \neq j$. Then the system of linear congruences:

$x \equiv b_1 \pmod{n_1}$
$x \equiv b_2 \pmod{n_2}$
$\cdots$
$x \equiv b_r \pmod{n_r}$
has a simultaneous solution which is unique modulo $\prod_{i=1}^{r} n_i$.

To obtain the solution to the set of congruences:

$$x \equiv b_1 c_1 \frac{N}{n_1} + \cdots + b_r c_r \frac{N}{n_r} \pmod{N},$$

where $N = n_1 n_2 \cdots n_r$
and the $c_i$ are determined from
$c_i \frac{N}{n_i} \equiv 1 \pmod{n_i}$

## Proof

Let $N = \prod_{i=1}^{r} n_i$ and $N_k = \frac{N}{n_k}$ for $k = 1, 2, \ldots, r$

Because $n_i \perp n_k$ for each $i \neq k$, we have
$\gcd\{N_k, n_k\} = \gcd\{n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r, n_k\} = 1$

So, by the definition of linear congruence $N_k x \equiv 1 \pmod{n_k}$ has a unique solution modulo $n_k$.

Let this solution be $x_k$.

So, $N_k x_k \equiv 1 \pmod{n_k}$

Show that $x_0 = b_1 N_1 x_1 + b_2 N_2 x_2 + \cdots + b_r N_r x_r$ satisfies each of the congruences, then evaluate $x_0$ modulo $n_k$ for each $k = 1, 2, 3, \ldots, r$.

We start by noting that

$$i \neq k \implies \frac{n_k}{N_i} \text{ so } N_i \equiv 0 \pmod{n_k}$$

So, for each $k = 1, 2, \ldots, r$ we have $x_0 \equiv b_k N_k x_k$ because each of the remaining terms in the sum is congruent modulo $n_k$ to 0.

Finally, since $x_k$ was found such that $N_k x_k \equiv 1 \pmod{n_k}$ we have $x_0 \equiv b_k \pmod{n_k}$ as we claimed.

All we need to do now is show that this solution we have discovered is unique modulo $N$.

So, suppose that $x'$ is a second solution of the system.

That is, $x_0 \equiv x' \equiv b_k \pmod{n_k}$ for each $k = 1, 2, \ldots, r$.

So each $n_k$ divides $x' - x_0$.

But because each of the moduli are pairwise coprime, we have

$$\prod_{i=1}^{r} \frac{n_i}{x'} - x_0$$

That is

$$x' \equiv x_0 \pmod{\prod_{i=1}^{r} n_i}$$

as we wanted to show. Q.E.D.

## Solution to the Old Woman and the Eggs Riddle

This problem can be expressed as a system of congruences

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

To solve for $x$, let $N = 3 \cdot 5 \cdot 7 = 105$

$$\frac{N}{3} = 35$$

$$\frac{N}{5} = 21$$

$$\frac{N}{7} = 15$$

Here we see that 2 is an inverse of $\frac{N}{3} = 35$ modulo 3 because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$; 1 is an inverse of $\frac{N}{5} = 21$ modulo 5, because $21 \equiv 1 \pmod 5$; and 1 is an inverse of $\frac{N}{7} = 15 \pmod 7$, because $15 \equiv 1 \pmod 7$. The solution to this system are those $x$ such that

$$x \equiv b_1 c_1 \frac{N}{n_1} + \cdots + b_r c_r \frac{N}{n_r} \pmod N,$$

$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$

$$= 233 \equiv 23 \pmod{105}$$

The answer is 23 eggs.

## Applications

The Chinese Remainder Theorem (or CRT) has applications in many fields, the foremost of which are computing, cryptography, and coding theory.

***Applications in Computing***

In computing the CRT gave rise to *modular technique* and has been adapted into a generalized technique for signal and image processing referred to as *homomorphic image computing*.

In computing the Chinese Remainder Algorithm (or CRA) is basically a divide-and-conquer technique that can be used to develop other divide-and-conquer techniques. A complex problem can be divided into smaller problems and solved independently, allowing for parallel processing. Afterwards the smaller problems can be combined by CRT to obtain a solution to the original

problem. This is demonstrated in linear feedback shift register synthesis problem for sequences over $Z/(m)$.

Cyclic convolution and Fourier transform are an important part of digital signal processing, as well as computer science and mathematics. There is a variety of algorithms for calculating cyclic convolution and discrete Fourier transform that attempt to rearrange one dimension arrays into multi-dimension arrays with shorter lengths. One of the most effective ways to do this is through the CRT and CRA.

***Applications in Coding Theory and Cryptography***

In coding theory, detection and correction of errors is done by adding redundancy to data that is sent via a noisy channel or in a computer. The CRT remainder techniques are useful in developing code that detects errors.

In cryptography, the CRT is used in secret sharing through error-correcting code. The CRT is itself a secret-sharing scheme without any need for modification:

Let $m_1, m_2, \cdots m_t$ be $t$ pairwise relatively prime integers, and $m = \prod_{i=1}^{t} m_i$. Suppose we have have a secret which is an integer $s$ with $0 \leq s < m$. The secret $s$ can be shared among $t$ parties as follows. Let $P_1, P_2, \cdots P_t$ denote the $t$ parties that will share the secret. We give $P_i$ the residue $s_i = s \pmod{m_i}$ the information known only to $P_i$. By the CRT the $t$ pieces of information $s_i$ are sufficient to determine the original secret $s$, but with anything less than $t$ number of residue $s_i$ cannot determine the original $s$.

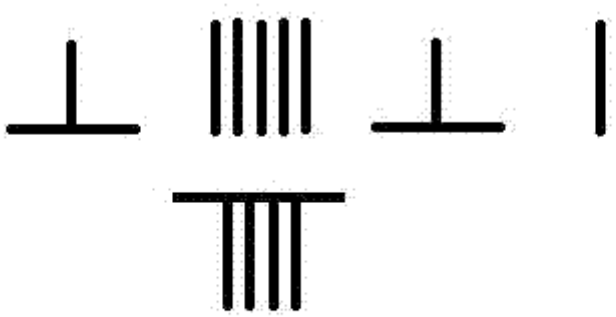
Other tyes of secret-sharing schemes are also implemented with the CRT.

## Conclusion

The Chinese Remainder Theorem seems to have been known throughout Asia since the *Sun Zi Suanjing* first appeared in the 1st century AD. Although Sun Zi did not provide a complete proof, mathematicians in India, such as Aryabhata, went on to provide a complete algorithm for solving this problem. It's amazing to see how many ancient

mathematical techniques, like the CRT and Euclidian algebra continue to find so many applications today.

**Fun Fact:** This is Sun Zi's division algorithm for 6561/9 using counting rods. The units are vertical, tens are horizontal, the hundreds are vertical with lines above.



*(LaTeX formatting provided by the awesome MathJax library.*