Project 1: The Chinese Remainder Theorem

Evan Hughes

March 2023

Abstract

The Chinese Remainder Theorem (CRT) is an ancient result in number theory that provides a method to solve systems of linear congruences. It was developed as a means to solve practical problems related to modular arithmetic. In ancient China, the theorem was used to solve problems in calendar calculations, land division, and taxation. The theorem's usefulness extends beyond these practical applications, and it has become a foundational result in number theory, algebra, cryptography, and computer science.

This research paper provides an overview of the history and development of the Chinese Remainder Theorem, from its ancient origins to its modern formulations and applications. We explore the motivation behind the theorem's development, its applications in ancient China, and its significance in mathematics and computer science. We also investigate various extensions and generalizations of the theorem and discuss recent advances in the algorithmic and computational aspects of the theorem.

Introduction

The Chinese Remainder Theorem (CRT) is a mathematical result that provides a method to solve a system of linear congruences with pairwise relatively prime moduli. The theorem's origin can be traced back to ancient China, where it was developed as a solution to practical problems in modular arithmetic. The Chinese mathematical treatise Sunzi Suanjing, written in the 3rd century AD, contains the earliest known reference to the theorem. The theorem was further developed by the Chinese mathematician Qin Jiushao during the Song Dynasty (960-1279). Qin Jiushao's works, such as Mathematical Treatise in Nine Sections, demonstrated the theorem's applications in the fields of astronomy, calendar making, and music theory. The theorem's usefulness in these practical applications made it a fundamental result in ancient Chinese mathematics.

The theorem was further developed by the Ming Dynasty mathematician Zhu Shijie in his book Jade Mirror of Four Unknowns. Zhu Shijie provided a more general formulation of the theorem that extended its applications to solving systems of simultaneous congruences. This work established the CRT as a foundational result in Chinese mathematics and set the stage for its later development in Western mathematics.

The Chinese Remainder Theorem's ancient origins highlight the importance of mathematical discoveries in solving practical problems and advancing scientific knowledge. The Chinese calendar, for instance, was based on a 60-year cycle, and its computation required keeping track of both the lunar and solar cycles. The overlap between the cycles made it difficult to perform calculations. The CRT provided a method to divide a year into different components, each of which could be computed separately and then combined to determine the calendar date. The CRT was also used in land division, where it was essential to ensure that each person received an equal share of the land. The CRT was used to calculate the size of each plot so that each person received an equal share of the land. These practical applications demonstrate the theorem's utility and demonstrate how mathematical discoveries can be applied to solve real-world problems. The theorem's development in ancient China paved the way for its later applications in modern mathematics and computer science, demonstrating the timelessness of mathematical discoveries and their impact on our world.

Proof of the Chinese Remainder Theorem (CRT)

In order to prove the Chinese Remainder Theorem, we must prove 4 items with the following definitions:

> For each $i = 1, 2, \ldots, r$, *let* N_i be the product of all the moduli m_j for $j \neq i, N_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_r$.

The items we need to prove are as follows:

1. For each i, show that gcd $(N_i, m_i) = 1$, and that there are integers u_i and v_i

2. For each i, and j with $i \neq j$, show that $N_i u_i = 0 \mod m_j$

3. For each i, show that $N_i u_i = 1 \mod m_i$

4. Find a $\mathbb{Z}$-linear combination x of the $N_i u_i$ which solves the entire system of linear congruences,

$$\begin{aligned} x &= a_1 (\mod m_1) \\ x &= a_2 (\mod m_2) \\ &\vdots \\ x &= a_r (\mod m_r) \end{aligned}$$

To start we will prove (1), For each i, show that $\gcd(N_i, m_i) = 1$, and that there are integers u_i and v_i such that $N_i u_i + m_i v_i = 1$. First to show that the $\gcd(N_i, m_i) = 1$ we can show that the gcd of m_i and each element of N_i is 1. This is because N_i is the product of all the moduli m_j for $j \neq i$, and so each element of N_i is relatively prime to m_i. Because $\gcd(a, b) = \gcd(c, b) = 1 \implies \gcd(ac, b) = 1$ means that the gcd of N_i and m_i is 1. Now to show that there are integers u_i and v_i such that $N_i u_i + m_i v_i = 1$ we can use the already proven fact that $\gcd(N_i, m_i) = 1$ to show that $N_i u_i + m_i v_i = 1$ by using Bézout's lemma.

Now we will prove (2), For each i, and j with $i \neq j$, show that $N_i u_i = 0 \mod m_j$. To show this we can use the fact that N_i is equal to the product of all the moduli m_j for

$j \neq i$. This means that $N_i u_i$ is always a multiple of m_j for $j \neq i$. This means that $N_i u_i = 0(\mod m_j)$.

Now we will prove (3), For each i, show that $N_i u_i = 1 \mod m_i$. In order for $N_i u_i = 1(\mod m_i)$ then $N_i u_i = km_i + 1$ for any integer k. Using the proof of (1) we know that $N_i u_i + m_i v_i = 1$. Which means that $N_i u_i = 1 - m_i v_i$. Through substitution we can see that $1 - m_i v_i = km_i + 1$. It follows that $km_i = -v_i m_i$. Because k can be any integer and $km_i = -v_i m_i$ then $k = -v_i$. This proves that for all i $N_i u_i = 1(\mod m_i)$.

Now we will prove (4), Find a $\mathbb{Z}$-linear combination x of the $N_i u_i$ which solves the entire system of linear congruences. To find a $\mathbb{Z}$-linear combination x of the $N_i u_i$ which solves the entire system of linear congruences we can use the fact that $N_i u_i = 1(\mod m_i)$ to show that $a_1(N_1 u_1) = a_1(\mod m_1)$, $a_2(N_2 u_2) = a_2(\mod m_2)$, $\ldots$, $a_r(N_r u_r) = a_r(\mod m_r)$. Now we can add all of these elements together to get $x = a_1(N_1 u_1) + a_2(N_2 u_2) + \ldots + a_r(N_r u_r)$. $x = a_y(\mod m_y)$ for all y because in a given $(\mod m_y)$ the only part that gives a value is $a_y(N_y u_y)$ and the rest of the linear combination , $a_1(N_1 u_1) + \cdots + a_{y-1}(N_{y-1} u_{y-1}) + a_{y+1}(N_{y+1} u_{y+1}) + \cdots a_r(N_r u_r) = 0$ as proven in (2) and (3). So this $\mathbb{Z}$-linear combination x of $N_i u_i$ solves the entire system of linear congruences,

$$\begin{aligned} x &= a_1(\mod m_1) \\ x &= a_2(\mod m_2) \\ &\vdots \\ x &= a_r(\mod m_r) \end{aligned}$$

Example Problems

Use the CRT to solve the linear congruence $17x = 9(\mod 276)$

Using the CRT $17x = 9(\mod 276)$ we can find x by using the following steps: First we need to break up this linear congruence into multiple coprime linear congruences.

$$\begin{aligned} 17x &= 9(\mod 3) \\ 17x &= 9(\mod 4) \\ 17x &= 9(\mod 23) \end{aligned}$$

This can be reduced to the following system of linear congruences:

$$x = 0(\mod 3)$$
$$x = 1(\mod 4)$$
$$x = 13(\mod 23)$$

Using the CRT this gives that $x = 105(\mod 276)$.

A gang of

17 bandits stole a chest of gold coins. When they tried to divide the coins equally among themselves, there were three left over. This caused a fight in which one bandit was killed. When the remaining bandits tried to divide the coins again, there were ten left over. Another fight started, and five of the bandits were killed. When the survivors divided the coins, there were four left over. Another fight ensued in which four bandits were killed. The survivors then divided the coins equally among themselves, with none left over. What is the smallest possible number of coins in the chest?
To write this out as a number problem gives

$$x = 3(\mod 17)$$
$$x = 10(\mod 16)$$
$$x = 4(\mod 11)$$
$$x = 0(\mod 7)$$

Using the CRT we know that x has a solution. We will start by solving the first 2 congruences then the last 2.
From the CRT we get that given 2 congruences, $x = a(\mod m)$ and $x = b(\mod n)$, a solution is given by $t = bmu + anv$.
With the first two congruences we get that $m = 17, n = 16, a = 3, b = 10$.
We also know that $17u + 16v = 1; u = 1, v = -1$.
Plugging these into the previous equation gives $t = 10(1)(17) + 3(-1)(16) = 122$.
So these two congruences give $x = 122(\mod 17 * 16)$.
Now the next two congruences give $m = 11, n = 7, a = 4, b = 0$ and $11u + 7v = 1; u = 2, v = -3$.

Plugging these into the previous equation gives $t = 0(2)(11) + 4(-3)(7) = -84$.

These two congruences give $x = -84(\mod 11 * 7)$.

This leaves us with $x = 122(\mod 272)$ and $x = 70(\mod 77)$.

To reduce this one we get $m = 272, n = 77, a = 122, b = 70$ and $272u + 77v = 1; u = -15, v = 53$.

Plugging these into the previous equation gives $t = 70(-15)(272) + 122(53)(77) = 212282$.

This gives us $x = 212282(\mod 272 * 77)$ which reduces to $x = 2842(\mod 20944)$.

This means the smallest possible number of coins in the chest is 2842.

Let t_n be the nth trianglular number

defined as $t_n = 1 + 2 + \cdots + n$. For which values of n does t_n divide $t_1^2 + t_2^2 + \cdots + t_n^2$?

We know that $t_1^2 + t_2^2 + \cdots + t_n^2$ is equal $t_n \frac{(3n^3+12n^2+13n+2)}{30}$. So to find when t_n divides $t_1^2 + t_2^2 + \cdots + t_n^2$ we need to find when $\frac{(3n^3+12n^2+13n+2)}{30}$ is an integer, because that will give us t_n times an integer.

So we need to solve $(3n^3 + 12n^2 + 13n + 2) = 0(\mod 30)$. 30 can factor into $2 * 3 * 5$ so we can break this up into 3 linear congruences.

To start with $(\mod 2)$ we get $n^3 + n = 0(\mod 2)$, which is true for all integers n.

In $(\mod 3)$ we get $n + 2 = 0(\mod 3)$, which is only true if $n = 1(\mod 3)$.

Next in $(\mod 5)$ we get $3n^3 - 3n^2 + 3n - 3 = 0(\mod 5)$, which factors to $(n-1)(n^2 + 1) = 0(\mod 5)$, which means $n = 1, 2,$ or $3(\mod 5)$.

This leaves us with the conditions that $n = 1(\mod 3)$ and $n = 1, 2, 3(\mod 5)$.

To solve these congruences we can use the CRT.

To take the first 2 congruences we get $m = 3, n = 5, a = 1, b = 1$ and $3u + 5v = 1; u = 2, v = -1$.

This gives $t = 1(2)(3) + 1(-1)(5) = 1$. Which means $n = 1(\mod 15)$.

Next we will use the first and third congruences to get $m = 3, n = 5, a = 1, b = 2$ and $3u + 5v = 1; u = 2, v = -1$.

this gives $t = 2(2)(3) + 1(-1)(5) = 7$. Which means $n = 7(\mod 15)$.

Finally using the first and last congruences to get $m = 3, n = 5, a = 1, b = 3$ and $3u + 5v = 1; u = 2, v = -1$.

This gives $t = 3(2)(3) + 1(-1)(5) = 13$. Which means $n = 13(\mod 15)$.
So the solutions for when t_n divides $t_1^2 + t_2^2 + \cdots + t_n^2$ is when $n = 1, 7, 13(\mod 15)$.

Generalization to non-coprime moduli

To generalize the CRT to non-coprime moduli we can start by letting m, n, a, b be any integers, and $g = \gcd(m, n)$; $M = lcm(m, n)$ and consider the following system of linear congruences:

$$x = a(\mod m)$$
$$x = b(\mod n)$$

If $a = b(\mod g)$ then this system has a unique solution modulo $M = mn/g$. Otherwise, no solution. If we use Bezout's Lemma to write $g = um + vn$ then the solution is given by $x = \frac{avn+bum}{g}$

Conclusion

In conclusion, the Chinese Remainder Theorem has a rich history that dates back to ancient China. It was developed to solve practical problems in modular arithmetic, such as calendar making, land division, and music theory. The theorem's development in ancient China paved the way for its later applications in modern mathematics and computer science, demonstrating the timelessness of mathematical discoveries and their impact on our world. The CRT has since become a fundamental result in number theory, algebra, and cryptography.
Modern applications of the CRT include its use in coding theory, computer science, and physics. In coding theory, the CRT is used in the construction of error-correcting codes, which are essential for transmitting information over noisy channels. In computer science, the CRT provides a basis for many secure communication protocols, such as RSA encryption. In physics, the CRT is used in the study of the quantum mechanics of spin systems and in the computation of energy levels in complex systems.

Sources

- https://kconrad.math.uconn.edu/blurbs/ugradnumthy/crt.pdf
- https://people.math.harvard.edu/ knill/crt/lib/Kangsheng.pdf
- https://mathoverflow.net/questions/10014/applications-of-the-chinese-remainder-theorem