THE CHINESE REMAINDER THEOREM

ERIC ALTENBURG

Abstract. We prove that an unknown can be found if it belongs to a system of linear congruences with coprime moduli.

This is done through the use of a constructive proof in which the solution is constructed for the system and then proven to be unique. There are three key concepts that help to arrive at a solution. The first is the simple idea of the greatest common divisor. The second is that integers are congruent to a modulo if their difference divides said modulo. The final idea is that of modular inverses. All of these work together to create a solution to a problem that has uses in areas like computer science where this theorem can be used to help break down large computations into more manageable smaller processes which increases efficiency.

1. Introduction

The earliest known reference to the problem that the Chinese Remainder Theorem aims to solve was found in China during the third century. It was there in which a Chinese mathematician by the name Sun-Tzu wrote a book titled *Sun-Tzu Suan-ching* which first proposed the problem as:

> There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three leftover; and by sevens, two left over. How many things are there? [2]

While this certainly sparked an interest in the problem, the book did not offer a solution or a proof to a solution. It was not until 1247 when another Chinese mathematician—Ch'in Chiu-shao—was able to offer a solution with a generalized result in his own book titled *Mathematical Treatise in Nine Sections* which was not translated to English until the 19th century by Alexander Wylie [6].

In terms of mathematical notation, the problem prompt from Sun-Tzu was simply a word problem, however, the Chinese Remainder Theorem relies on the idea of congruences among others. History aside, the theorem holds its own in the realm of Number theory, and it is important to note that there are three key concepts in which it relies on to warrant a proof. The first is the simple idea that two numbers have a greatest common divisor. The second is that two integers can be congruent to a modulo if the difference between the said integers divides this modulo. The final concept is the existence of modular inverses in certain congruences.

These aforementioned concepts will be used while proving the solution, therefore, to help ensure a solid understanding of the Chinese Remainder Theorem's base, we will thoroughly visit several definitions.

Finally, it is worth going over the proof strategy being used to get a sense of how the proof will flow. We first want to show the existence of the solution by providing a method of creating such a solution, then we will show that it is unique.

2. Background

In this section, we will review some fundamental background material before proceeding into the formal proof of the Chinese Remainder Theorem.

Definition 2.1. When elements of a set S have some property of equivalence defined on them, then S can be split into *equivalence classes*. For example, $[a]_n$ is the set of all integers that have the same remainder as a when divided by n [11].

Definition 2.2. If a and b are integers and $c > 0$, then we can write

$$a \equiv b \bmod c$$

if and only if $c|(b-a)$. This can also be read as "a is *congruent* to b modulo c" [4]. Additionally, it is worth noting that if $a \equiv b \bmod c$, then a and b belong to the same equivalence class.

Recall the concept of equivalence relations and how they must satisfy reflexivity, symmetry, and transitivity. To build on this, congruence modulo a number m is also an equivalence relation. The following properties hold for every $m \in \mathbb{N}^+$.

(1) Reflexive: $a \equiv a \pmod m$

(2) Commutative: If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.

(3) Transitive: If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

[1] [1]

Definition 2.3. The *greatest common divisor* (gcd) of two or more integers which are not all zero, is the largest possible integer that divides each of the integers. Given integers x, y, the greatest common divisor of x and y is written as $\gcd(x, y)$[8].

Definition 2.4. If a and b are integers and $c > 0$, then given that $c|a$ and $c|b$, we can say that $c|\gcd(a, b)$.

Definition 2.5. The *extended Euclidean algorithm* is an extension to the Euclidean algorithm which computes the greatest common divisor of two integers, a and m, along with the coefficients from Bézout's identity, integers s and t, such that

$$sa + tm = \gcd(a, m).$$

[12]

[1]The following definition has been adapted from lectures 28 and 29 from Professor Bhatt at Stevens Institute of Technology, Department of Computer Science.

Recall an integer multiplied by its inverse is 1. Similarly, in modular arithmetic we have modular inverses where an integer $a \bmod m$ has the inverse of a^{-1} such that $(a \cdot a^{-1}) \equiv 1 \pmod{m}$ or $(a \cdot a^{-1}) \bmod m = 1$[7].

Lemma 2.6. *Let $a, m \in \mathbb{Z}$. If $\gcd(a, m) = 1$, then $a^{-1} \pmod{m}$ exists.* [1]

Proof. Knowing that the $\gcd(a, m) = 1$, we can use Definition 2.5 and apply the extended Euclidean algorithm to expand this greatest common denominator. Doing so gives $sa + tm = \gcd(a, m)$ where $s, t \in \mathbb{Z}$. This allows us to manipulate $\gcd(a, m) = 1$ where

$$\begin{aligned} \gcd(a, m) &= 1 \\ sa + tm &= 1 \\ tm &= 1 - sa. \end{aligned}$$

We can then use Definition 2.2 to create a congruence of

$$tm \equiv 1 - sa \pmod{m},$$

and using commutativity, we obtain

$$1 - sa \equiv tm \pmod{m}.$$

Because $m|tm$, we get

$$\begin{aligned} 1 - sa &\equiv 0 \pmod{m} \\ sa &\equiv 1 \pmod{m} \\ s &\equiv a^{-1} \pmod{m}. \end{aligned}$$

This shows that we can derive a modular inverse such that when multiplied by a given number, in our case s, we can arrive at the congruence of the said quantity being congruent to 1 modulo another number, our m. 1 □

3. Main result

This section outlines the formal proof for the Chinese Remainder Theorem. At first, we spend time constructing a valid solution to the problem, and then prove it to be unique.

Theorem 3.1. *If $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are pairwise relatively prime meaning that $\gcd(n_i, n_j) = 1$ for $i \neq j$, and $b_1, b_2, \ldots, b_k \in \mathbb{Z}$, then the system of linear congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

has a unique solution modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Proof. (Construction)

Let $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ and $N_i = \frac{N}{n_i}$ where N_i is simply N without a multiple of any given n_i.

Claim 3.2. $\gcd(N_i, n_i) = 1$

To show this claim holds, let's suppose that $d|N_i$ and $d|n_i$ where $d \in \mathbb{Z}$. Since all n_j are relatively prime, then d must divide some n in N that is not n_i.

This implies that $d|n_j$ for $j \neq i$.

Since $d|n_i$ and $d|n_j$, by Definition 2.4 we have $d|\gcd(n_i, n_j)$ implying that $d|1$ which must mean $d = 1$ proving our claim.

Now, by Lemma 2.6 since $\gcd(N_i, n_i) = 1$, N_i has an inverse $\pmod{n_i}$. Let x_i be the said inverse such that

$$\begin{aligned} N_i &\equiv x_i^{-1} \pmod{n_i} \\ x_i N_i &\equiv 1 \pmod{n_i}, \end{aligned} \tag{3.1}$$

and we note that

$$x_i N_i \equiv 0 \pmod{n_j} \text{ for } j \neq i. \tag{3.2}$$

We know this to be true because N_i is made of a multiple of n_j, therefore, it follows that $x_i N_i$ would be congruent to $0 \pmod{n_j}$.

Now to construct the solution, consider

$$x = X_1 N_1 b_1 + X_2 N_2 b_2 + \ldots + X_k N_k b_k$$

where each b_i is obtained from the original system of linear congruences. To satisfy each of the said linear congruences, we have to consider x to be modulo some n_i. With this there are two possible cases for a given term $(X_k N_k b_k)$. The first is when $k \neq i$, then with Equation 3.2, $X_k N_k$ will become 0 because $N_k|n_i$. The second case is when $k = i$, then with Equation 3.1, $X_k N_k$ will become 1 because X_k is the modulo inverse; this leaves $(1 \cdot b_k)$. The result of x when we consider it to be modulo some n_i is

$$\begin{aligned} x &\equiv 0 + \ldots + 0 + X_i N_i b_i + 0 \ldots + 0 \pmod{n_i} \\ x &\equiv b_i \pmod{n_i}, \quad \text{for all } 1 \leq i \leq k. \end{aligned}$$

(Uniqueness)

Having constructed a solution in the form of x, to show it is unique, suppose y and z are both solutions which gives $y \equiv b_i \pmod{n_i}$ and $z \equiv b_i \pmod{n_i}$ for all $1 \leq i \leq k$. Subtracting y from z then gives

$$\begin{aligned} z - y &\equiv b_i \pmod{n_i} - b_i \pmod{n_i} \\ z - y &\equiv (b_i - b_i) \pmod{n_i} \\ z - y &\equiv 0 \pmod{n_i}. \end{aligned}$$

This implies that $n_i|(z-y)$ for $1 \leq i \leq k$ which means $(z-y)$ must be a multiple for all the n_i's which are relatively prime, therefore, it must be a multiple of their product N. We can now rewrite this as $N|(z-y)$ and with Definition 2.2, $N|(z-y)$ implies

$$z \equiv y \pmod{N}.$$

This proves the uniqueness because given any two solutions, it must be that they are both congruent mod N, therefore, any solution will be congruent to the one that is already constructed.[10] □

4. Applications and discussion

There are several applications of the Chinese Remainder Theorem, though its main use is in the area of increasing efficiency.

One such example of its use is in the case of parallel computing. Suppose there is a large computation that involves the computer performing operations such as adding, subtracting, multiplying, and potentially dividing integers that a part of a finite set S which will be given. What we can do is choose prime numbers $p_1, p_2, \ldots, p_r$ that do not divide any elements of S, and their product $p_1 \cdot p_2 \cdot \ldots \cdot p_r$ is larger than the answer of our computation. Then split the computation over r processors, where the ith one computes the answer modulo p_i. Finally, we can use the Chinese Remainder Theorem to help combine the values to obtain the answer to the computation [9].

Another key area in which the theorem is widely used is in the field of Cryptography and the Rivest-Shamir-Adleman (RSA) cryptosystem as an optimization tool. To show the idea behind its utility for RSA, let M be some message, C be the ciphertext, $N = PQ$ be the RSA modulus, and D be the decryption key. Computing C^D requires a lot of processing power as D is large, and doing any operations modulo N are the same in that N is large too. But with the theorem, we can find M by splitting it into different messages like so,

$$\begin{aligned} M_P &= M \bmod P \\ M_Q &= M \bmod Q. \end{aligned}$$

To compute M_P and M_Q, we can use Fermat's Little Theorem which simply states that if p is prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p; it is also expressed as $a^p \equiv a \pmod{p}$. Solving, we find that

$$\begin{aligned} M_P &= M \bmod P \\ &= (C^D \bmod N) \bmod P \\ &= C^D \bmod P \\ &= C^{D \bmod (P-1)} \bmod P. \end{aligned}$$

Now, let $D_P = D \bmod (P-1)$. We can then compute D_P during the key generation to compute

$$M_P = C^{D_P} \bmod P,$$

and this follows the same for M_Q[3].

References

[1] Bhatt, Sandeep. "Lecture28_29-1". Stevens Institute of Technology, Department of Computer Science.

[2] Dence, Joseph B.; Dence, Thomas P. (1999), *Elements of the Theory of Numbers*, Academic Press, ISBN 9780122091308.

[3] Großschädl, Johann. "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip." ACSAC 2000: 384-393 https://www.acsac.org/2000/papers/48.pdf.

[4] Hausner, Melvin. "Quantitative Reasoning: Computers, Number Theory and Cryptography." New York University, Department of Mathematics. https://www.math.nyu.edu/~hausner/congruence.pdf.

[5] Ireland, Kenneth; Rosen, Michael (1990), A Classical Introduction to Modern Number Theory (2nd ed.), Springer-Verlag, ISBN 0-387-97329-X.

[6] Katz, Victor J. (1998), *A History of Mathematics / An Introduction* (2nd ed.), Addison Wesley Longman, ISBN 978-0-321-01618-8.

[7] Khan Academy. "Modular Inverses." https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-inverses.

[8] Long, Calvin T. (1972), *Elementary Introduction to Number Theory* (2nd ed.), Lexington: D. C. Heath and Company, LCCN 77171950.

[9] Mathoverflow Contributors. "Applications of the Chinese remainder theorem." Mathoverflow, https://mathoverflow.net/questions/10014/applications-of-the-chinese-remainder-theorem.

[10] Penn, Michael. "Number Theory — Chinese Remainder Theorem Proof." Film, video. YouTube, 2019. https://www.youtube.com/watch?v=EolotL9HN8k.

[11] Reluga, Tim. "Linear Congruence Class Theory." Pennsylvania State University, Department of Mathematics. http://www.personal.psu.edu/tcr2/311w/congruenceTheoremGuide.pdf.

[12] Wikipedia Contributors. "Extended Euclidean Algorithm." Wikipedia, https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm.

I pledge my honor that I have abided by the Stevens Honor System. - Eric Altenburg