Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

Exploring Algebraic Properties and the Applications of Chinese Remainder Theorem

Saskia Putri Maharani[1], Edi Kurniadi[2], Sisilia Sylviani[3,*]

[1,2,3] *Universitas Padjadjaran, Jl. Soekarno Km 21 Jatinangor, Kab. Sumedang, 45363, Indonesia*

[*] *Corresponding author: sisilia.sylviani@unpad.ac.id*

Copyright: ©2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License-(CC-BY-SA) (https://creativecommons.org/licenses/by-sa/4.0/)

Article Info

Article history:
Received: October 2024
Revised: December 2024
Accepted: December 2024
Available online: December 2024

Abstract

This research aims to identify the algebraic properties of the Chinese Remainder Theorem or CRT. Chinese Remainder Theorem is an ancient mathematical theorem that allows the solution of a system of simultaneous equations with different modules and allows the reconstruction of integers within a certain range of remainders modulo to relatively prime modulo. The method used in this research is literature study. This theorem allows for efficient processing and manipulation of integers with very large sizes. The proof of the theorems in Chinese Remainder Theorem is also presented in this research.

Keywords: Chinese Remainder Theorem; Rings; Principal Ideal Domain

I. Introduction

The Chinese Remainder Theorem or CRT is an important concept in number theory that originated in ancient Chinese mathematics [1]. This theorem arises as a solution to the problem of a system of simultaneous congruence equations. The Chinese Remainder Theorem is a number theory theorem which states that if a number of congruence equations satisfy certain conditions, then there is a unique solution and it may be possible to reconstruct the number in a relatively prime range modulo the modulo [1] [2] [3] [4] [5] [6] [7] [8].

The theorem was first invented in the third century by a Chinese mathematician, Sun Zi, in his book Suanjing to solve linear congruence problems [1]. The CRT is commonly applied to calculate large integers because it is possible to replace calculations over a certain range with the same calculations over smaller integers. In previous research, Crisan and Pollac used Hooley's method to prove the root distribution of polynomial functions modulo certain conditions [9]. Meanwhile, Saurabh and Gaura revealed that CRT allows the reconstruction of integers from their division remainders. This is very useful in performing calculations or computations with large numbers [10].

According to Stallings [11], CRT can be used in trade to maximize profit, as usually sellers will offer a lower price for goods as they will be resold for a profit. If there are more sellers, then their offers can be simplified to linear congruence, i.e. by applying the properties of division and inverse to determine the best offer to maximize profit.

In the 20th century, research on the Chinese Remainder Theorem grew rapidly, especially in the field of cryptography. In this field, CRT is used to improve the efficiency of the decryption process of messages that have been encrypted using a public key. This efficiency improvement is done because CRT allows solving complex cryptographic problems into smaller sub-problems that can be easily solved in parallel [12] [13] [14] [15]. Moreover, in the field of cryptography and information security, the Chinese Remainder Theorem can be used for information retrieval and information leakage prevention [16] [17] [18].

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

II. Preliminaries

A. Integer divisibility

An integer q is divisible by an integer $p \neq 0$ written $p|q$, if and only if there is an integer x such that $q = px$. If q is not divisible by p then it is written $p \nmid q$ [3] [5] [19].

Example:
$4|28$ because there is integer 7 such that $28 = 4 \times 7$.

The notation $p|q$ can be read as follows:
a. p divides q
b. q is divided by p
c. p is a factor of q
d. p is a divisor of q
e. q is a multiple of p

B. Greatest Common Divisor (GCD)

Suppose p and q are non-zero integers. The greatest common divisor (gcd) of p and q is the largest integer r such that $r|p$ and $r|q$. In this case we state that $\gcd(p, q) = r$ [5] [19].

C. Congruence

If p, q, m is an integer then p is called congruent with q modulo m if and only if m divides $-q$. Or in other words, it can be denoted by $p \equiv q(mod\ m) \Leftrightarrow m|p - q$ [5].

Example:
$26 \equiv 1\ (mod\ 5)$ because $5|26 - 1$ or $5|25$.

$30 \equiv 2\ (mod\ 7)$ because $7|30 - 2$ or $7|30$.

III. Results

THEOREM 1 [5] [21]**.** Suppose $m_1, m_2, m_3, \dots, m_n$ are the positive integers that are pairwise coprime such that $\gcd(m_i, m_j) = 1$, for $i \neq j$. Then the linear congruence system:

$$\begin{aligned} x &\equiv a_1(mod\ m_1) \\ x &\equiv a_2(mod\ m_2) \\ x &\equiv a_3(mod\ m_3) \\ &\dots \\ x &\equiv a_n(mod\ m_n) \end{aligned}$$

has a unique solution modulo $M$where $M = m_1 m_2 m_3 \dots m_n$.

PROOF. Suppose $= m_1 m_2 m_3 \dots m_n = m_1 m_2 m_3 \dots m_{k-1} m_k m_{k+1} \dots m_n$.
For each $i = 1, 2, 3, \dots, n$, assume:

$$M_i = \frac{M}{m_i} = m_1 m_2 m_3 \cdots m_{i-1} m_{i+1} \cdots m_n. \quad (1)$$

Since $\gcd(M_i, m_i) = 1$ which implies $M_i y \equiv 1(mod\ m_i)$ has a solution y_i. Because M_i is defined as the result of multiplying all integers m_i except m_i itself, M_i includes m_j as a factor for $j \neq i$. This means that M_i is a multiple of m_j for $j \neq i$. Therefore, $M_i \equiv 0(mod\ m_j)$ for $j \neq i$.
Suppose $\bar{x} = \sum_{i=1}^{n} a_i M_i y_i \ (mod\ m_j)$ is a general solution to the given system of linear congruencies. Thus, we have:

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

$$\bar{x} = \sum_{i=1}^{n} a_i M_i y_i \ (mod\ m_j).$$
$$= a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_j M_j y_j + \cdots + a_n M_n y_n \ (mod\ m_j)$$
$$\equiv \quad 0 \quad + \quad 0 \quad + \cdots + a_j M_j y_j + \cdots + \quad 0 \quad (mod\ m_j)$$
$$\equiv a_j M_j y_j (mod\ m_j)$$
$$\bar{x} \equiv a_j (mod\ m_j).$$

The supposition is true so it is proved that $\bar{x}$ is a general solution of the given linear congruence system. Next, it will be proved that $\bar{x}$ is a unique solution.
Suppose $\bar{x}_1$ and $\bar{x}_2$ are solutions of the linear congruence system $\bar{x} \equiv a_j (mod\ m_j)$ for each j. Such that,

$$\bar{x}_1 \equiv a_j (mod\ m_j)$$
$$\bar{x}_2 \equiv a_j (mod\ m_j).$$

By performing the subtraction operation on the two linear congruence systems, we get:

$\Leftrightarrow \bar{x}_1 - \bar{x}_2 \equiv 0 \ (mod\ m_j)$
$\Leftrightarrow m_j | \bar{x}_1 - \bar{x}_2$
$\Leftrightarrow [m_1, m_2, m_3, \dots, m_n] | \bar{x}_1 - \bar{x}_2$
$\Leftrightarrow m_1 m_2 m_3 \dots m_n | \bar{x}_1 - \bar{x}_2$
$\Leftrightarrow M | \bar{x}_1 - \bar{x}_2$
$\Leftrightarrow \bar{x}_1 - \bar{x}_2 \equiv 0 \ (mod\ M)$
$\Leftrightarrow \bar{x}_1 \equiv \bar{x}_2 \ (mod\ M).$

It is proven that $\bar{x}$ is the unique solution of the linear congruence system.

The following are the algebraic properties of the Chinese Remainder Theorem:

A. Statement for Principal Ideal Domains

For a principal ideal domain R, CRT can be stated as follows:

If $u_1, u_2, \dots, u_k$ are element in R that are pairwise coprime, and u is the product $u_1, u_2, .., u_k$, then the quotient ring $\frac{R}{uR}$ and the product ring $\frac{R}{u_1 R} \times \frac{R}{u_2 R} \times \dots \times \frac{R}{u_k R}$ are isomorphic through the following isomorphism:

$$f: \frac{R}{uR} \to \frac{R}{u_1 R} \times \frac{R}{u_2 R} \times \dots \times \frac{R}{u_k R} \tag{2}$$

with $f(x + uR) = (x + u_1 R, x + u_2 R, \dots, x + u_k R)$ for any x in R. This mapping is well defined and forms a ring isomorphism [22].

The inverse isomorphism can be constructed as follows: For each i, the elements u_i and $\frac{u}{u_i}$ are coprime, so there exist elements r and s in R such that $r u_i + \frac{su}{u_i} = 1$. Let $e_i = \frac{su}{u_i}$. Then it follows that $e_i \equiv \delta_{ij} \ (mod\ u_i R)$. Therefore the inverse of f is the mapping:

$$g: \frac{R}{u_1 R} \times \frac{R}{u_2 R} \times \dots \times \frac{R}{u_k R} \to \frac{R}{uR} \tag{3}$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

defined by $g(a_1 + u_1R, a_2 + u_2R, \dots, a_k + u_kR) = \sum_{i=1}^{k} a_i e_i + uR$ for all $a_1, a_2, \dots, a_k \in R$.

This statement directly generalizes the previously discussed theorem about integer congruencies: the ring of integers, $\mathbb{Z}$, is a principal ideal domain. The surjectivity of the map f confirms that any system congruencies in the form $x \equiv a_i \ (mod\ u_i)$ for all $i = 1,2, \dots, k$ has a solution for x, and the injectivity of f shows that all such solutions x are congruent modulo u.

B. Statement for General Rings

The generalized form of the Chinese Remainder Theorem, encompassing all prior statements, can be framed for commutative rings and ideals. If R is a commutative ring and $I_1, I_2, \dots, I_k$ are ideals of R that are pairwise coprime (meaning $I_i + I_j = R$ for $i \neq j$), then the product of these ideals is equal to their intersection, and the quotient ring $\frac{R}{I}$ is isomorphic to the product ring $\frac{R}{I_1} \times \frac{R}{I_2} \times \dots \times \frac{R}{I_k}$ via the isomorphism:

$$f: \frac{R}{I} \to \frac{R}{I_1} \times \frac{R}{I_2} \times \dots \times \frac{R}{I_k} \tag{4}$$

with $f(x + I) = (x + I_1, x + I_2, \dots, x + I_k)$ for all x in R.
There is also a version of the theorem applicable when R is not required to be commutative: Let R be any ring with unity not necessarily commutative) and let $I_1, I_2, \dots, I_k$ be pairwise coprime two-sided ideals. Then the canonical R-module homomorphism:

$$R \to \frac{R}{I_1} \times \frac{R}{I_2} \times \dots \times \frac{R}{I_k} \tag{5}$$

is surjective with kernel $I_1 \cap I_2 \cap \dots \cap I_k$. Thus, $R/(I_1 \cap I_2 \cap \dots \cap I_k) \approx \frac{R}{I_1} \times \frac{R}{I_2} \times \dots \times \frac{R}{I_k}$ (as R-modules).

The following are also given real-world applications of CRTs:

A. CRT in Trading

Floods hit the storehouse of a grain production company in Navrongo, Ghana and damaged all the sacks of grain in the storehouse. The government, through the National Disaster Management Organization, then decided to provide compensation to the grain production company by covering the losses. When the organization asked the rice production company how many sacks of rice they had in the storehouse, they were unable to remember the actual number, but what they did remember was that when they took out two sacks of rice at a time, there was only one sack left. Likewise, when they took out three, four, five, and six bags at a time, but when they took out seven bags at a time, there was an even number. Problems like these are examples of the Chinese Remainder Theorem. In mathematical language, we can write the expression below to describe the solution:

Condition 1: When the bags taken out two at the time, there is only one bag left.

$$x \equiv 1 \ (mod\ 2).$$

Condition 2: When the bags taken out three at the time, there is only one bag left.

$$x \equiv 1 \ (mod\ 3).$$

Condition 3: When the bags taken out four at the time, there is only one bag left.

$$x \equiv 1 \ (mod\ 4).$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

Condition 4: When the bags taken out five at the time, there is only one bag left.

$$x \equiv 1 \ (mod\ 5).$$

Condition 5: When the bags taken out six at the time, there is only one bag left.

$$x \equiv 1 \ (mod\ 6).$$

Condition 6: When the bags taken out seven at the time, there are even numbers bag left. Which means,

$$x \equiv 0 \ (mod\ 7).$$

This means,

$$x \equiv 1 \ (mod\ 2) \Leftrightarrow x = 2k + 1$$

$$x \equiv 1 \ (mod\ 3) \Leftrightarrow x = 3k + 1$$

$$x \equiv 1 \ (mod\ 4) \Leftrightarrow x = 4k + 1$$

$$x \equiv 1 \ (mod\ 5) \Leftrightarrow x = 5k + 1$$

$$x \equiv 1 \ (mod\ 6) \Leftrightarrow x = 6k + 1$$

$$x \equiv 0 \ (mod\ 7) \Leftrightarrow x = 7k + 0.$$

From conditions $1 - 5$, we observe that $x \equiv 1$ for each modulus $2, 3, 4, 5,$ and 6. This means that x leaves a remainder of 1 when divided by any of these numbers. To calculate x, we have to find the least common multiple (lcm) of $2, 3, 4, 5,$ and 6.

$$\text{lcm}(2,3,4,5,6) = 60.$$

We can conclude that x must satisfy:

$$x \equiv 1 \ (mod\ 60)$$

$$x = 60k + 1, \text{ for some } k \in \mathbb{Z}.$$

Then, substitute $x = 60k + 1$ into the sixth condition. We have,

$$60k + 1 \equiv 0 \ (mod\ 7)$$

$$60k \equiv -1 \ (mod\ 7)$$

$$60k \equiv 6 \ (mod\ 7)$$

$$k \equiv 5 \ (mod\ 7)$$

$$k = 7m + 5, \text{ for some } m \in \mathbb{Z}.$$

Now, to find x, we have to substitute $k = 7m + 5$ into the $x = 60k + 1$.

$$x = 60(7m + 5) + 1$$

$$= 420m + 300 + 1$$

$$= 420m + 301.$$

The smallest positive solution is when $m = 0$, so:

$$x = 420(0) + 301$$

$$= 301.$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 1 Issue 2 December, 2024, pp. 71-78
https://idjams.com/index.php/jms/index

Thus, the rice production company likely had 301 bags of rice in the warehouse.

B. CRT in Information Retrieval or Leakage

CRT can also be used to retrieve information that is shared between multiple people but not shared publicly. In other words, this information is confidential Let us illustrate how CRT can be used to retrieve information. Suppose the secret messages is given in the integers form, i.e. $K = 1000$. Then, K is divided as three different messages between three people such that the message may only get reconstructed if all three people work together. To ensure that each piece of the secret message is unique and can be recombined to reconstruct K, choose the pairwise coprime numbers $p_1 = 11, p_2 = 13$, and $p_3 = 17$. We can express the secret K in the form of a system of congruencies:

$$x \equiv 10 \ (mod\ 11)$$
$$x \equiv 12 \ (mod\ 13)$$
$$x \equiv 14 \ (mod\ 17).$$

Now, calculate the product of all moduli, which gives us:

$$\begin{aligned} M &= p_1 \times p_2 \times p_3 \\ &= 11 \times 13 \times 17 \\ &= 2431. \end{aligned}$$

For each prime p_i, calculate $M_i = \frac{M}{p_i}$:

$$M_1 = \frac{2431}{11} = 221$$
$$M_2 = \frac{2431}{13} = 187$$
$$M_3 = \frac{2431}{17} = 143.$$

Then, using the Chinese Remainder Theorem, for each M_i, find an integer y_i such that:

$$M_i y_i \equiv 1 \ (mod\ p_i).$$

So,

- For $M_1 = 221$, we have $221y_1 \equiv 1 \ (mod\ 11) \Rightarrow y_1 = 1$
- For $M_2 = 187$, we have $187y_2 \equiv 1 \ (mod\ 13) \Rightarrow y_2 = 8$
- For $M_3 = 143$, we have $143y_3 \equiv 1 \ (mod\ 17) \Rightarrow y_3 = 5$.

Now, using CRT, we can construct x or the secret message by combining each congruence:

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \ (mod\ M) \\ &= 10 \times 221 \times 1 + 12 \times 187 \times 8 + 14 \times 143 \times 5 \ (mod\ 2341) \\ &= 2210 + 17952 + 10010 \ (mod\ 2431) \\ &= 30172 \ (mod\ 2431) \\ &= 1000. \end{aligned}$$

Based on the results of x (which is equal to K), it can be concluded that CRT is able to reconstruct a secret message shared with three different people under the condition that the three people work together.

IV. Conclusion

The conclusion of this research shows that the Chinese Remainder Theorem (CRT) has significant algebraic properties. CRT allows solving systems of congruent equations with mutually prime moduli, as well as providing a unique solution of a system of linear congruences. In addition, CRT can also be used in daily life such as trading and information retrieval or leakage.

References

[1] H. P. Yoke and U. Libbredht, "Chinese Mathematics in the Thirteenth Century.," *Pac. Aff.*, vol. 46, no. 4, 1973, DOI: 10.2307/2755346.

[2] S. Iftene and F. Chelaru, "The General Chinese Remainder Theorem," *Int. J. Comput.*, 2014, DOI: 10.47839/ijc.6.1.423.

[3] J. A. Gallian, "*Contemporary Abstract Algebra*." Chapman and Hall/CRC, 2021, DOI: 10.1201/9781003142331.

[4] Q. Luo, "Research and application of Chinese remainder theorem," *Theor. Nat. Sci.*, vol. 9, no. 1, 2023, DOI: 10.54254/2753-8818/9/20240711.

[5] D. M. Burton, "*Elementary Number Theory,* " Seventh Edition, 2010.

[6] H. C. Tang, "Combined random number generator via the generalized Chinese remainder theorem," *J. Comput. Appl. Math.*, vol. 142, no. 2, 2002, DOI: 10.1016/S0377-0427(01)00424-1.

[7] M. Selianinau, "Computationally Efficient Approach to Implementation of the Chinese Remainder Theorem Algorithm in Minimally Redundant Residue Number System," *Theory Comput. Syst.*, vol. 65, no. 7, 2021, DOI: 10.1007/s00224-021-10035-y.

[8] E. A. Alhassan, K. Tian, O. J. Abban, I. Ohiemi, M. Adjabui, G. K. Armah, and S. Agyemang, "On Some Algebraic Properties of the Chinese Remainder Theorem with Applications to Real Life," *J. Appl. Math. Comput.*, vol. 5, no. 3, 2021, DOI: 10.26855/jamc.2021.09.008.

[9] V. Crişan and P. Pollack, "The Smallest Root of a Polynomial Congruence," *Math. Res. Lett.*, vol. 27, no. 1, 2020, DOI: 10.4310/mrl.2020.v27.n1.a4.

[10] S. Singh and G. Agarwal, "Use of Chinese Remainder Theorem to Generate Random Numbers for Cryptography," *Int. J. Appl. Eng. Res.*, vol. 1, no. 2, 2010.

[11] W. Stallings, "*Cryptography and Network Security: Principles and Practices*," Seventh Edition. Pearson, 2005.

[12] V. Keerthika, "Role of Chinese Remainder Theorem in Cryptography," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6, 2019, DOI: 10.35940/ijeat.E7522.088619.

[13] E. al. Yogesh Suryawanshi, "Chinese Remainder Theorem based Performance Analysis of RSA Cryptosystem," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 8, 2023, DOI: 10.17762/ijritcc.v11i8.9559.

[14] H. Mohamed, H. A. Abd, R. M. Hussien, R. S. Abdeldaym, A. Elkader, and R. Hussein, "Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem," *I.J. Electron. Inf. Eng.*, vol. 10, no. 1, 2019.

[15] W. Schindler, "A Timing Attack Against RSA with the Chinese Remainder Theorem," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2000, DOI: 10.1007/3-540-44499-8_8.

[16] M. A. Hadavi, R. Jalili, and L. Karimi, "Access Control Aware Data Retrieval for Secret Sharing based Database Outsourcing," *Distrib. Parallel Databases*, vol. 34, no. 4, 2016, DOI: 10.1007/s10619-015-7186-x.

[17] W. Du, M. Li, Y. Han, X. A. Wang, and Z. Wei, "A Homomorphic Signcryption-Based Privacy Preserving Federated Learning Framework for IoTs," *Secur. Commun. Networks*, vol. 2022, 2022, DOI: 10.1155/2022/8380239.

[18] X. Li, H. Chen, Y. Liu, and C. C. Chang, "Unordered Multisecret Sharing Based on Generalized Chinese Remainder Theorem," *Secur. Commun. Networks*, vol. 2020, 2020, DOI:

10.1155/2020/6073721.
[19] D. A. Lapele, "*Teori Bilangan*. " Widina Bhakti Persada Bandung, 2023.
[20] E. Kurniadi, E. Carnia, and N. Gusriani, "*Pengantar Teori Grup Hingga*." Tahta Media, 2021.
[21] J. C. Martzloff, "*A history of Chinese Mathematics*." Springer, 2006, DOI: 10.1007/978-3-540-33783-6.
[22] M. Komisarchik, "Chinese Remainder Approximation Theorem," *Topol. Appl.*, vol. 221, 2017, DOI: 10.1016/j.topol.2017.02.070.