Journal of Applied Mathematics and Computation, 2021, 5(3), 219-224
https://www.hillpublisher.com/journals/JAMC/
ISSN Online: 2576-0653
ISSN Print: 2576-0645

On Some Algebraic Properties of the Chinese Remainder Theorem with Applications to Real Life

Elvis Adam Alhassan[1,2,*], Kaiyu Tian[1], Olivier Joseph Abban[1], Israel Enema Ohiemi[4,5], Michael Adjabui[2], Gabriel Armah[3], Simon Agyemang[2]

[1]School of Mathematical Sciences, Jiangsu University, Zhenjiang, Jiangsu, China.
[2]Faculty of Mathematical Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Upper East Region, Ghana.
[3]School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Upper East Region, Ghana.
[4]National Research Centre of Pumps, Jiangsu University, Zhenjiang, Jiangsu, China.
[5]Department of Mechanical Engineering, University of Nigeria, Nsukka, Nigeria.

How to cite this paper: Elvis Adam Alhassan, Kaiyu Tian, Olivier Joseph Abban, Israel Enema Ohiemi, Michael Adjabui, Gabriel Armah, Simon Agyemang. (2021) On Some Algebraic Properties of the Chinese Remainder Theorem with Applications to Real Life. *Journal of Applied Mathematics and Computation*, 5(3), 219-224.
DOI: 10.26855/jamc.2021.09.008

Received: August 18, 2021
Accepted: September 9, 2021
Published: September 18, 2021

***Corresponding author:** Elvis Adam Alhassan, School of Mathematical Sciences, Jiangsu University, Zhenjiang, Jiangsu, China; Faculty of Mathematical Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Upper East Region, Ghana.
Email: eaalhassan@cktutas.edu.gh

Abstract

The study sought to establish some algebraic properties of the Chinese Remainder Theorem. The Chinese Remainder Theorem is an ancient but important mathematical theorem that enables one to solve simultaneous equations with respect to different modulo and makes it possible to reconstruct integers in a certain range from their residues modulo to the pairwise relatively prime modulo and also construct libraries for manipulations on very large integers. The study seeks to find out some real life applications of the Chinese Remainder Theorem in our everyday life activities especially in trading and in information security and retrieval avoiding any leakages to invaders or intruders. The study presented proofs of some theorems vital in the real life applications of the Chinese Remainder Theorem. In the study, we identified that in the statement of the Principal Ideal Domain and that of Rings can be classified as some algebraic properties of the Chinese Remainder Theorem.

Keywords

Chinese Remainder Theorem, Principal Ideal Domain, Rings, Information Retrieval, Integer Factorization, Trial Division

1. Introduction

Simultaneous congruence has been the source of puzzles since antiquity. Chinese Mathematicians studied these puzzles and the schemes for solving them became known as the Chinese Remainder Theorem (CRT).

Crisan and Pollac [1] used the method of Hooley to prove that the roots of some function f having degree of at least 2 and no multiple roots are equidistributed modulo some k as k varies over the integers for which the congruence is solvable.

Exponential sums involving multiplicative inverses were established on explicit coprimality conditions of summation and detected using a further additive character [2].

According to Saurabh and Gaura [3], the Chinese Remainder Theorem is a theorem of number theory, which states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are relatively prime. The theorem was first discovered in the 3rd century AD by the Chinese Mathematician Sun Zi in Suan-

jing. The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers. According to Alhassan et al. [4], one of the most useful results of number theory is the Chinese Remainder Theorem. In essence, the CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli. Stallings [5] showed that the Chinese Remainder Theorem could also be applied to trading so as to maximize returns where retailers normally bid for reduction in prices of goods since they have to resell the commodities and make profit. They therefore price the goods in groups. Most often, some are added free to the retailers. In case there are more retailers, we can simplify their bid into linear congruence, applying the division and inverse property in determining the best bid so as to maximize profit.

2. Exploration of CRT

Theorem 2.1

The Chinese Remainder Theorem denoted by CRT states that if $n_1, n_2, \dots, n_p$ are integers that are pairwise coprime are any integers then the system of p congruence is given by

$$\begin{gathered} X \equiv X \equiv a_1 (mod\ n_1) \\ X \equiv a_2 (mod\ n_2) \\ X \equiv a_3 (mod\ n_3) \\ \dots \\ X \equiv a_p (mod\ n_p) \end{gathered}$$

has a unique solution that satisfy the given system of congruence given by

$$X = \sum_1^p a_i\, m_i y_i (mod\ M)$$

Proof

Let $x_i \equiv a_i (mod\ n_i)$ for $i = 1, 2, \dots, p$ where $M = n_1 n_2 \dots n_p$ with the $\gcd(n_i, n_j) = 1$ and $i \neq j$ so that M is the least common multiple of the n_i. Let $m_i = \frac{M}{n_i}, y_i = m_i{}^{-i} (mod\ n_i)$. The modular y_i exist because n_i does not divide m_i and also the $\gcd(n_i, n_j) = 1$ when $i \neq j$ then $m_i y_i \equiv 1 (mod\ n_i)$. Since n_i divides m_i when $j \neq i$ then $m_i y_i \equiv 1\ (mod\ n_i)$ for $j \neq i$ Hence, $X = \sum_1^p a_i\, m_i y_i\ (mod\ M)$ for which hold for all congruence.

2.1 Integer Factorization Based on CRT

Let $M = m_1 m_2 \dots m_n$. Let $u_1, n_2, \dots, u_n$ be now any n known positive integers $\leq m_1, m_2, \dots m_n$ respectively, then there is one and only one positive integer u such that $0 < u \leq m_j, u \equiv u_j \left(mod\ m_j\right), 1 \leq j \leq n$.

Now recalling the definition of Euler function, for any positive integer nn let $\emptyset(n)$ be the number of integers less than n and prime to n. If n is decomposed in prime factors as $n = p_1^{e_1} \dots p_s^{es}$ where $p_1, \dots, p_s$ are primes different from each other then $\emptyset(n) = n \prod_{i=1}^{s} (1 - \frac{1}{p_i}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$

In particular, in case n is itself a prime p, then $\emptyset(p) = p^{-1}$. As integer factorization is not quite trivial and the value of $\emptyset(n)$ will be quite large so far n is a little large which will influence the calculations in interesting problems. It may surpass the ability of a modern computer.

We reproduce now the constructive proof of CRT below:

Let us put

$$M_i = \frac{m^{\emptyset(mj)}}{mj}, 1 \leq j \leq n$$

Then by Euler theorem any integer u satisfy the congruence $u = (u_1 M_1 + u_2 M_2 + \dots + u_n M_n)\ mod\ m$ will satisfy also the congruence $u \equiv u_i (mod m_i), 1 \leq j \leq n$. As the uniqueness is evident, so this proves CRT.

2.2 Trial Division

Trial Division is the simplest algorithm for factoring integers. Assume that $p\ and\ q$ are nontrial factors of N such that $pq = N\ and\ p \leq q$. To perform the trial divisionalgorithm, one simply checks whether p/N for $p = 2, 3, 4, \dots, \lfloor \sqrt{N} \rfloor$. When such a divisor p is found, then it is also a factor and a factorization has been found for N.

The upper bound of $p \leq \lfloor \sqrt{N} \rfloor$ is provided by the theorem below:

Theorem 2.2

If N has nontrivial factors p, q with $pq = N \; and \; p \leq q$, then $p \leq N$.

Proof

Assume$p > N$. Then $q \geq p > N$ and $pq > N$, which contradicts the assumption that $pq = N$. Hence, $p \leq N$. If this algorithm is given composite number N, then it returns a pair of nontrivial factors p, q with $p \leq q$. Now p/N means is equivalent to $p \equiv 0(mod\ N)$ and so it can be implemented via modular arithmetic.

3. Results

3.1 Algebraic Properties of CRT

3.1.1 Statement for Principal Ideal Domains

For a Principal ideal domain R, the Chinese Remainder Theorem takes the following form:

If $u_1 \ldots u_k$ are elements of R which are pairwise coprime and u denotes the product $u_1 \ldots u_k$ then the quotient ring R/uR and the product ring $\frac{R}{u_1 R} \times \ldots \times \frac{R}{u_k R}$ are isomorphic via the isomorphism:

$$f: \frac{R}{uR} \to \frac{R}{u_1 R} \times \ldots \times \frac{R}{u_k} \text{ such that } f(x + uR) = (x + u_1 R \ldots x + u_k R) \; \forall \; x \in R$$

This map is well-defined and an isomorphism of rings; the inverse isomorphism can be constructed as follows: For each i, the elements $u_i \; and \; u/u_i$ are coprime and therefore there exist elements $r \; and \; s$ in R with $ru_i + \frac{su}{u_i} = 1$.

Set $e_i = s\frac{u}{u_i}$. Then it is clear that $e_i \equiv \delta_{ij}\,(mod\ u_i R)$. Thus, the inverse of f is the map:

$$g: \frac{R}{u_1 R} \times \ldots \times \frac{R}{u_k R} \to \frac{R}{uR} \text{ defined by } g(a_1 + u_1 R, \ldots, a_k + u_k R) = \sum_{i=1}^{k} a_i \, e_i + uR \; \forall \; a_1, \ldots, a_k \in R.$$

This statement is a straightforward generalization of the above theorem about integer congruencies: the ring Z of integers is a principal ideal domain, the surjectivity of the map f shows that every system of congruencies of the form: $x \equiv a_i (mod\ u_i) \; \forall \; i = 1, \ldots, k$ can be solved for x and the the injectivity of the map f shows that all the solutions x are congruent modulo u.

3.1.2 Statement for General Rings

The general form of the Chinese Remainder Theorem, which implies all the statements given above, can be formulated for Commutative rings and Ideals. If R is a commutative ring and $I_1, \ldots, I_k$ are ideals of R that are pairwise coprime (meaning that $I_i + I_j = R \; \forall \; i \neq j$), then the product I of these ideals is equal to their intersection and the quotient ring R/I is isomorphic to the product ring: $\frac{R}{I_1} \times \frac{R}{I_2} \ldots \times \frac{R}{I_k}$ via the isomorphism $f: \frac{R}{I} \to \frac{R}{I_1} \times \ldots \times \frac{R}{I_k}$ such that: $f(x + 1) = (x + I_1, \ldots, x + I_k) \; \forall \; x \in R$.

Here is a version of the theorem where R is not required to be commutative:

Let R be any ring with 1 (not necessarily commutative) and $I_1, \ldots, I_k$ be pairwise coprime 2-sided ideals. Then the canonical R-module homomorphism:

$$R \to \frac{R}{I_1} \times \ldots \times \frac{R}{I_k}$$

is onto with kernel $I_1 \cap \ldots \cap I_k$. Hence, $\frac{R}{I_1 \cap \ldots \cap I_k} \approx \frac{R}{I_1} \times \ldots \times \frac{R}{I_k}$ (as R-modules).

3.2 Real Life Applications of CRT

3.2.1 CRT in Trading

A flood eroded the warehouse of a rice manufacturing company in Navrongo, Ghana and destroyed all the bag of rice at the warehouse. The government through National Disaster Management Organization decided to compensate the rice manufacturing company by paying for the damages. When the organization asked the rice manufacturing company how many bags of rice they had in the warehouse, they could not remember the exact quantity but all they could remember was that when they took them all out two at a time, there was one bag left. The same happened when they picked them all out three, four, five, and six at a time, but when they took them all out seven at a time they came out even. Problems of this kind are all examples of what universally became known as the Chinese Remainder Theorem. In Mathematical parlance, the problem can be stated as finding n, given its remainders of division by several numbers. When the bags were all taken out 2 at a time, the remainder was 1. We can write the expression:

$$2k + 1 \tag{1}$$

to represent the solutions. Dividing this expression by 3 the remainder is 2

$$\frac{2k + 2}{3}$$

We can see that when it gives a remainder 2, clearly this value will be$k = 2$. Clearly it means that we will now have the expression in Eq. (1) written as:

$$2K + 1 = 5$$

A solution by dividing by 2 and 3 will arrive at the following new equation

$$5 + 2.3k = 5 + 6.k \tag{2}$$

This equation results in 1 when divided by 2 and results in 2 when divided by 3, for all integers *k*. We will now require the following expression:

$$\frac{5 + 6.k}{4} \tag{3}$$

which will give a remainder 3 and further rewriting (3) we will get;

$$1 + k + \frac{1+2k}{4} \tag{4}$$

Clearly, we will now have *k* = 1 and hence (2) will now become

$$5 + 6.k = 11$$

So far we have a number 11, which when divided by 2 gives 1 and when divided by 3 gives 2 and when divided by 4 gives 3 as required.

We can preserve these results by writing the new equation:

$$11 + 3.4.k = 11 + 12.k \tag{5}$$

And thus because 3.4 = 12 is divisible by 2, 3 and 4 so our number will give the required results for that which is divisible by 2, 3 and 4 for all values of k.

We now require that division by 5 will give a remainder 4, ie $\frac{11+12.k}{5}$

$$\frac{11 + 12.k}{5} = 2 + 2.k + \frac{1 + 2.k}{5}$$

which further gives a remainder 4 so by testing $k = 4$ and from (5) we have;

$$11 + 12.4 = 59$$

Our next equation will hold because $3.4.5 = 60$ is divisible by 2,3,4,5

$$59 + 3.4.5.k = 59 + 60k \tag{6}$$

We require that this gives a remainder 5 when divided by 6 ie $\frac{59+60.k}{6}$, for all integers *k*

Our final equation which comes out even when divided by 7 is

$$59 + 3.4.5.k \tag{7}$$

Because 3.4.5 = 60 is divisible by 2,3,4,5,6 we rewrite (7) and require that: $\frac{59+60.k}{7}$.

It is certain to note that when it comes out even it will mean that;

$$8 + 8k + \frac{3+4.k}{7} \tag{8}$$

When *k* = 1 and it comes out even, our new number will therefore be:

$$59 + 60 = 119$$

Therefore, the minimum number of bags of rice in the warehouse is 119

3.2.2 CRT in Information Retrieval or Leakage

Confidential information shared between people can be retrieved using the Chinese Remainder Theorem if one of them should misplace the information or die untimely. Below is an illustration of how CRT is used to retrieve information. Consider a confidential message to be in the form of an integer, $K = 1000$ and shared into three distinct messages

among three people in such a way that K can be retrieved by working together the secret messages of three people but not by the participation of fewer people. We thus, choose the pairwise coprime say, $p_i$such that cube-root of $K < p_i\ much\ < square-root\ of\ K, implies, 10 < p_i much < 31.6$. We choose $p_1 = 11,\ p_2 = 13,\ p_3 = 17$.

Finding the residues of Kmodulo $p_i$we get;

$$x = 10 mod 11$$
$$x = 12 mod 13$$
$$x = 14 mod 17$$

With the help of the partition messages, the secret message $x = K$ can be retrieved as follows: we find

$$M = p_1 \times p_2 \times p_3 = 11 \times 13 \times 17$$
$$M_1 = \frac{2431}{11} = 221$$
$$M_2 = \frac{2431}{13} = 187$$
$$M_3 = \frac{2431}{17} = 143$$

Using the Chinese Remainder Theorem we will compute,

$$221K_1 = 1 mod 11,\ K_1 = 221^{-1} mod 11\ \Rightarrow K_1 = 1$$
$$187K_2 = 1 mod 13,\ K_2 = 40^{-1} mod 13\ \Rightarrow K_2 = 8$$
$$143K_3 = 1 mod 17,\ K_3 = 35^{-1} mod 17\ \Rightarrow K_3 = 5$$

$x = 10 \times 221 \times 1 + 12 \times 187 \times 8 + 14 \times 143 \times 5 = 30172(mod 2431) = 1000$ which is the desired confidential message.

Now if one of the people is perished, by the use of the Chinese Remainder Theorem, the full message can be retrieved using the available secret messages of the remaining two people.

$$x = 10 mod 11$$
$$x = 12 mod 13$$
$$M = 11 \times 13 = 143, M_1 = \frac{143}{11} = 13, M_2 = \frac{143}{13} = 11$$

Now using the Chinese Remainder Theorem, we compute;

$$13 \times K_1 = 1 mod 11, K_1 = 12^{-1} mod 11 \Rightarrow K_1 = 6$$
$$11 \times K_2 = 1 mod 13, K_2 = 11^{-1} mod 13 \Rightarrow K_2 = 6$$
$$x = 10 \times 13 \times 6 + 12 \times 11 \times 6 = 1572(mod 143) = 142$$

Generating the required message we compute
$142 + (143 \times i), i = 1,2,3 \ldots$ yielding the integers; 285,428,571,714,857,1000 ...

Thus, $p_1 = 11,\ p_2 = 13$ are much $< \sqrt{K}$

The usefulness of this application is that it prevents loss of valuable information.

4. Conclusions

The Chinese Remainder Theorem which has been described as one of the theorems as a result of congruencies in number theory and its generalization in Abstract Algebra. In its basic form, the Chinese Remainder Theorem determines a number$n$ that when divided by some given divisors give some remainders.

In conclusion, with the help of the Chinese Remainder Theorem, the only knowledge to guide with two remaining secret messages to get what we desire is the solution of the form:

$$142 + (143 \times i).$$

It can further be concluded that the Chinese Remainder Theorem has a lot of uses in our everyday life activities.

References

[1] Crisan, V. and Pollack, P. (2020). The smallest root of a polynomial congruence, Math. Res. Lett., 27(1).

[2] Dartyge, C. and Martin, G. (2019). Exponential sums with reducible polynomials. Discrete Anal https://doi.org/10.19086/da.10793.

[3] Saurabh, S. and Gaurav, A. (2010). Use of Chinese Remainder Theorem to generate random numbers for Cryptography. International Journal of Applied Engineering Research. Volume 1, No. 2, pp. 168-174.

[4] Alhassan, E. A., Simon, K. N., Bunyan, J. M., and Gregory, A. (2014). On some algebraic properties of the Euclidean algorithm with applications to real life. Research Journal of Mathematics and Statistics, 6(4): 49-55.

[5] Stallings, W. (1999). Cryptography and Network Security: Principles and Practice. (2nd ed.). New Jersey: Prentice-Hall.