Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.9, No.10, 2019

An Algorithm to Solve A System of Linear Congruences with Applications

Sisay Tadesse[1] Mesele Molla[2]

1 Department of Mathematics, College of Natural and Computational Sciences, Wolaita Sodo University,
PO box 138, Wolaita Sodo, St. 7, Ethiopia, Tel: +251 911554508 E-mail:sisaytdss137@gmail.com
2 Department of Mathematics, College of Natural and Computational Sciences, Wolaita Sodo University,
PO box 138, Wolaita Sodo, St. 7, EthiopiaTel: +251 911969459 E-mail: kussuro@gmail.com

ABSTRACT
In this paper, an algorithm as an alternative tool for solving system of linear congruences (SLC) is developed. this algorithm involves finding LCM of the moduli of reduced SLC, in view of cancellation law, identifying the largest moduli, and obtaining the solution of the linear congruence with largest modulus. Then it involves checking whether the solution satisfies the remaining linear congruences in the system of linear congruences. The advantage of this algorithm is the simplicity of its computation since it uses algebraic concepts which are easy to understand. Some illustrative examples are given to show the validity of this method for solving SLC's. The application of the developed algorithm on solving system of linear congruences is also used to solving higher order congruences (HOC) with composite moduli and system of higher order congruences (SHOC).
Key words/Phrases: Chinese Remainder Theorem (CRT)**,** linear congruences (LC), System of linear congruences (SLC), Applications to Higher order Congruences (HOC) and System of HOC with composite moduli.
DOI: 10.7176/MTM/9-10-05
Publication date: October 31st 2019

1. Introduction

Finding solutions to congruences has received remarkable attention in the past several decades. The problem has been studied intensively by numerous authors. There are several methods to solve linear congruences and system of linear congruences. In solving linear congruences, (Gold N.E, 2002) made use of remodularization method as a vehicle to characterize the condition under which the solution exist and then determine the solution space. (William Stein, 2009) also presented an approach which translate the given congruence ax=c (mod b) into Diophantine equation ax+by =c to solve the linear congruences. Koshy (2007) also Presented an algorithm making use of multiplicative inverses of a modulo min solving linear congruences. (Smarandache, 2007)developed a generalized algorithm in solving linear and system of linear congruences with more than one variable, on the basis of conditions under which existence of solutions and the number of them ascertained. (Polemer M. Cuarto, 2014) devised an algebraic algorithm for finding solutions of linear congruences, converting the given congruence into linear equation and solve algebraically. And he applied it in cryptography using the RSA cryptosystem. (John Frederic Chionglo, 2016)also made use of conversion of linear congruences to equivalent linear equations, and reduced the co-efficients of the induced variables, iteratively, until one of them reached unity. He used division algorithm in the reduction with respect to the smaller co-efficient in the successive equations; in such a way that the last larger co-efficient and the constant have got reduced. (Eugel Verdal, 2006) developed a method for solving non-linear congruences of higher degree reducing them into either linear or quadratic congruences.

Although there are already several approaches developed, finding solutions to system of linear congruences (SLC), higher order (HOC), and system of higher order congruences (SHOC) still remain pedagogically difficult. This is because the methods make use of complex algorithms. Thus, in this paper we strive to devise an algorithm for solving the anterior classes of congruences, that is advantageous over the already used ones that follow an exhaustive, gradual and incremental method which entertain a definite risk of computation complexity.

In this context, this piece of work can help Mathematics students especially the beginners who are taking up Number Theory to easily solve problems on system linear congruences since it uses the concept of algebraic principles which every Mathematics students is familiar with. Utilizing the algorithm presented in this paper will help them realize that Mathematics can be made simpler because the algorithm does not make use of complex

notations and operations which other algorithms do. Likewise, this would benefit Mathematics instructors and professors for this may serve as a reference material in teaching the concept of congruences in Number Theory.

This algorithm could also give programmers insights in developing a program based on this technique that can automatically solve problems on systems of linear congruences. This study would also provide input for future researchers who will conduct researches and studies related to the topic as this could be a basis for developing another algorithm that can solve problems on linear congruences, system of linear congruences (SLC), higher order (HOC), and system of higher order congruences (SHOC).

In the light of the foregoing perspectives, we felt the need of this algorithm. The study aims to develop an algebraic algorithm for solving system of linear congruences. Specifically, the study seeks to develop an alternative algorithm for solving system linear congruences; to validate the developed algorithm through illustrative examples; to apply the developed algorithm in solving HOC and System of HOC.

2. Preliminaries: Congruences

In order to effectively understand the concept of system linear congruences and higher order congruences, it will be necessary to become familiar with the following definitions, theorems and properties which will be used further in the development of this paper.

2.1. Definition of congruences

Definition 2.1. For positive integer n, and for a, b∈Z, we say that a is congruent to b modulo n if n|(a-b), and we write a≡b (mod n). If n∤(a-b), then wed write a≢b (mod n).

Note 2.1. The relation a≡b (mod n) is called a congruence relation or simply, a congruence. The number n appearing in such congruence is called *modulus* of the congruence.

2.2. Basic properties congruences

Theorem 2.1. let a, b, c, and k are integers, then the following hold.

i. ***Reflexive Property***: If a is an integer, then a ≡a (mod n).
ii. ***Symmetric Property***: If a≡ b (mod n), then b≡ a (mod n).
iii. ***Transitive Property***: If a ≡ b (mod n) and b ≡ c (mod n), then a c (mod n).
iv. ***Simplification Property*****:** If k divides a, b and n, then a≡ b (mod n) is congruent to a/k ≡b/k (mod n/k)
v. ***Cancellation Property***: If gcd (k, n) = 1, then ak≡bk (mod n) is congruent to a≡ b (mod n). More generally, if d=gcd (k, n), then ak≡bk (mod n) if and only if a≡ b (mod n/d).
vi. ***Addition Property***: If a≡ b (mod n), then a + k≡b + k (mod n).
vii. ***Subtraction Property*****:** If a≡ b (mod n), then a - k≡ b - k (mod n)
viii. ***Multiplication Property*****:** If a ≡b (mod n), then ak≡bk (mod n)

2.3. Polynomial congruences

In any commutative ring with unity, the equation f(x) =0 with f(x)∈R[x] is called polynomial Equation. if deg f=1, it is called linear; if deg f=2, it is called quadratic; if deg f=3, it is called cubic, etc. In particular for $\mathbb{Z}_m$, we have the above terminologies. Instead of saying f(x) =0 is an equation in $\mathbb{Z}_m$, we sometimes write f(x) ≡0 (mod m) and we say it is congruence of degree n, n= deg f. When deg f=1, it is called a linear congruence, if deg f=2, quadratic congruence, etc. A higher degree congruence is a congruence with $deg\ f \geq 2$.

2.4. Solving Linear Congruences

For a positive integer n, and $a \in \mathbb{Z}$, we say that $a' \in \mathbb{Z}$ is a *multiplicative inverse* of a modulo n if $a\,a' \equiv 1(mod\ n)$.

Theorem 2.2. Let a, n∈$\mathbb{Z}$ with n>0. Then a has a *multiplicative inverse* modulo n if and only if a and n are relatively prime.

Note that the existence of multiplicative inverse of a modulo n depends only of the value of a modulo n; that is, if

a≡b (mod n), then a has an inverse if and only if b does. Indeed, by theorem 3, if $a \equiv b\ (mod\ n)$, then for any integer a', $aa' \equiv 1\ (mod\ n)$ if and only if $ba' \equiv 1\ (mod\ n)$.

Theorem2.3. Let a, b, n∈ $\mathbb{Z}$ with n>0, and let d=gcd (a, n). If $d|b$, the congruence ax≡ b (mod n) has a solution x_0; moreover, any integer x is a solution if and only if x≡x_0 (mod n/d).If $d \nmid b$, then the congruence ax≡$b\ (mod\ n)$has no solution z.

Corollary 2.4. Let a, b, n∈ $\mathbb{Z}$ with n>0. If a is relatively prime to n, then the congruence ax≡ b (mod n) has a solution x_0; moreover, any integer x is a solution if and only if x≡x_0 (mod n).

Example 2.1. Solve 6x≡7 (mod 8). Since (6,8) =2∤7, there are no solutions.
Example 2.2. Solve 3x ≡ 7(mod 4). Since (3,4) =1|7, there will be 1 solutions mod 4. We will find it in three different ways.

- **Using Linear Diophantine Equations:**3x≡7 (mod 4) implies 3x +4y =7 for some y. By inspection $x_0 = 1, y_0 = 1\ is$ is a particular solution. (3, 4) =1, so the general solution is
  x≡1 (mod 4)
- **Using the Euclidian algorithm.** Since (3, 4) =1, some linear combination of 3 and 4 is equal to 1. In fact, (-1).3+ 1.4 = 1.
- **Using inverse mod 4.** Here is the table of multiplication mod 4:

Table 1: multiplication modulo 4

*	*0*	*1*	*2*	*3*
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	**1**

We see that 3.3≡1 (mod 4), so, multiply the congruence by 3:3x≡ 7 (mod 4), x≡21≡1(mod 4). ■

The Euler Method

This is a method to solve a linear Diophantine equation $ax + by = c$ .It is equally a way of solving congruence $ax \equiv c(modb)$. The Euler method for solving $ax + by = c$ involves taking congruences, and also changing congruences to equations.

Procedure: Euler's method for solving linear congruences.

In solving a linear congruence $ax \equiv b\ (mod\ c)$.

i. Change congruence to an equation.: ax=b+cy
ii. Take the equation and change it to congruence modulo the smallest coefficient.
iii. Simplify and repeat as many as necessary, till you get the solution x≡ d mod c.

Example 2.3. Solve the Linear congruence 3x≡ 5(mod 7)

Solution: (i) converting to equation, we get 3x=5+7y, for y in Z.

(ii) Changing to congruence of smaller co-efficient, we obtain the following congruence $7y \equiv -5(mod\ 3)$

Then, (iii) simplifying the congruence in (ii), we have $y \equiv -2\ (mod\ 3)$. Then y= -2.and $x = \frac{5+7(-2)}{3} = -\frac{9}{3} = -3$. Thus, any solution x of the congruence 3x≡ 5(mod 7) is given by $x \equiv -3(\ mod\ 7)$

Remark 2.1. Recall $\mathbb{Z}_n^*$ denotes the set of invertible elements of the ring $\mathbb{Z}_n$[1]. The number of elements of $\mathbb{Z}_n^*$ is denoted by φ (n).

Definition 2.2. Euler's totient function φ (n) is defined for positive integer n as the number of elements of $\mathbb{Z}_n^*$. Equivalently, φ (n) is equal to the number of integers between 0 and n-1 that are relatively prime to n.

Example 2.4. φ (1) =1, φ (2) =1, φ (3) =2 and φ (4) =2.

Remark 2.2. we note that $\mathbb{Z}_m^*$ is a group with φ(m) elements. It follows that if gcd (x, m) =1, $\bar{x}$ is an element of $\mathbb{Z}_m^*$ and by Lagrange's theorem on finite groups,$\bar{x}^{\varphi(m)} = 1$ in $\mathbb{Z}_m$. Hence, we have $x^{\varphi(m)} \equiv 1(mod\ m)$ for each x, gcd (x, m) =1. As consequence, we get:

Theorem 2.5. (Fermat's Little Theorem): For every integer x and p, p prime, $x^p \equiv 1(mod\ p)$.

2.5. System of Linear Congruence

Here under, we discuss system of linear congruences in one variable.

Definition 2.3: Suppose $m_1, m_2 \dots \dots \dots m_n$ are natural numbers, $a_i, b_i, i = 1,2,3, \dots \dots \dots, n$ are integers. Then

$$\begin{cases} a_1 x \equiv b_1 (mod\ m_1\ ) \\ a_2 x \equiv b_2 (mod\ m_2\ ) \\ \quad\vdots \\ a_n x \equiv b_n (mod\ m_n\ ) \end{cases} \qquad (*)$$

, is called a system of linear congruences in on variable.

Definition 2.4: An integer x_0 is called a solution of the system (*) iff $a_i x_0 \equiv b_i (mod\ m_i\ )$, for every i=1, 2, …, n.

Remark 2.3. In view of the cancelation law, each congruence of the system in (*) is equivalent to x≡ $c_i\ (mod\ \frac{m_i}{d_i})$,

Where $d_i = gcd\ (a_i, m_i)$ and some appropriate integers c_i. Hence it suffices to develop a technique that solves the system

$$x \equiv c_i\ (mod\ \tfrac{m_i}{d_i})\ ,\ i=1, 2, \dots\dots\dots, n$$

for arbitrary but fixed integers $c_1, c_2, \dots \dots \dots, c_n$ and natural numbers$m_1, m_2 \dots \dots \dots m_n$.

Example2.5. solve the following system of congruences

$$\begin{cases} 2x \equiv 4(mod\ 9) \\ 3x \equiv 15(mod\ 12) \end{cases}$$

Solution: Since (2, 9) =1|4 and (3, 12) =3|15, it is clear that each of the congruences in the system has a solution. Evidently, $2x \equiv 4(mod\ 9)$ is equivalent to $x \equiv 2(mod\ 9)$ and $3x \equiv 15(mod\ 12)$ is equivalent to $x \equiv 1(mod\ 4)$. Hence, the complete solution of $2x \equiv 4(mod\ 9)$ is given by

$$S_1 = \{2 + 9n | n \in \mathbb{Z}\},$$

While that of $3x \equiv 15(mod\ 12)$ is given by

$$s_2 = \{1 + 4m | m \in \mathbb{Z}\}.$$

Therefore, $S_1 \cap S_2$ is the solution of the given system of congruences. Choosing n=-1 and m=-2, for instance, we notice that -7 is a solution of the system. It is easy to see that {x/ x≡-7(mod 36)} is the complete set of solutions

[1] Fix a positive integer n. The set Z_n is denote a ring of residue classes modulo n under addition and multiplication modulo n, and $\mathbb{Z}_n^*$ form a multiplicative group modulo n.

using the next theorem.

2.6. **Properties of System of Linear Congruences**

Theorem2.6. The system of congruences

$$\begin{cases} x \equiv a(mod\ m) \\ x \equiv b(mod\ n) \end{cases}$$

has a solution iff $(m,n)|(a-b)$. Moreover, if x_0 is a solution of the system, any other solution is given by $x \equiv x_0(mod\ [m,n])$.

The integer x_0 is a solution of the system iff $x_0 = a + my$ and $a + my \equiv$b (mod n), for some integer y. This is equivalent to saying that y is a solution of the linear congruence mx ≡b-a (mod n).

In view of a theorem of solving linear congruences, this holds iff$(m,n)|(a-b)$. To prove the second part of the theorem, suppose x_0 and x are any two solutions of the system. Then $x \equiv a \equiv x_0(mod\ m)$ and $x \equiv b \equiv x_0(mod\ n)$. It follows that $x - x_0$ is a multiple of m and n, and hence $x \equiv x_0(mod\ [m,n])$.

Lemma 2.7. If $m_1, m_2\ \ldots\ldots\ldots m_n$ are natural numbers, a and are integers such that $a \equiv b\left(mod\ (m_1, m_j)\right)$, i=2, 3, …, n, then $a \equiv b\left(mod\ (m_1, [m_2\ \ldots m_n])\right)$.

Proof: Assume the hypothesis holds and let p be a prime such that p^θ divides $(m_1, [m_2\ \ldots m_n])$.Then $p^\theta | m_1$ and $p^\theta | [m_2\ \ldots m_n]$. It follows that for some i_0=2, 3, …, n $p^\theta | m_{i_0}$ and hence $p^\theta | (m_1, m_{i_0})$. Since$a \equiv b\left(mod\ (m_1, m_{i_0})\right)$, we conclude that p^θ is a factor of $a-b$. As p is an arbitrary prime and θ is any non-negative integer, we conclude that $a \equiv b\left(mod\ (m_1, [m_2\ \ldots m_n])\right)$.

Theorem 2.8. The system of linear congruences

$$\begin{cases} x \equiv a_1(mod\ m_1\ ) \\ x \equiv a_2(mod\ m_2\ ) \\ \quad\quad\vdots \\ x \equiv a_n(mod\ m_n\ ) \end{cases}$$

has a solution iff $(m_i, m_j)|(a_i - a_j)$ for every i and j=1, 2, …., n. Moreover, if x_0 is a solution of the system any other solution, x, is given by $x \equiv x_0(mod\ [m_1, m_2\ \ldots m_n])$.

Proof: Suppose the system has a solution. Then for each pair I and j, the system

$$\begin{cases} x \equiv a_i(mod\ m_i\ ) \\ x \equiv a_j(mod\ m_j\ ) \end{cases}$$

has a solution. In view of the above theorem, this true iff $(m_i, m_j)|(a_i - a_j)$ .This completes the proof of the forward implication.

To prove the converse of the theorem, we assume the result holds for any system consisting of $n-1$ linear congruences. Then the system

$x \equiv a_i(mod\ m_i\ )$ $, i = 1,2, \ldots\ldots, n-1,$ has a solution x_0. Now consider the system $\begin{cases} x \equiv x_0(mod\ [m_1, m_2\ \ldots m_{n-1}]\ ) \\ x \equiv a_n(mod\ m_n\ ) \end{cases}$ and claim that the system has a solution. This assertion equivalent to saying $([m_1, m_2\ \ldots m_{n-1}], m_n\ )$ is a factor of $x_0 - a_n$. We show that the latter holds. Indeed, since $x_0 \equiv a_i(mod\ m_i)$ for each i= 1, 2, ……., n-1, we notice that for each i= 1, 2, ……., n-1,

$$x_0 \equiv a_i\ (mod\ (m_i, m_n)).$$

Thus $(x_0 - a_i) + (a_i - a_n) \equiv 0(\text{mod}\ (m_i, m_n))$

yielding $x_0 \equiv a_n(\text{mod}\ (m_i, m_n))$, i=1, 2, ..., n-1. By the above lemma, it follows that

$x_0 \equiv a_n(\text{mod } ([m_1, m_2 \ldots m_{n-1}], m_n))$.

Consequently, the system of congruences

$$\begin{cases} x \equiv x_0(mod\ [m_1, m_2 \ldots m_{n-1}]) \\ x \equiv a_n(mod\ m_n) \end{cases}$$ has a solution. This solution is clearly a solution of the system $x \equiv a_i(mod\ m_i), i = 1,2, \ldots, n$.

Finally, if x and x_0 are solutions of the system, then

$x \equiv a_i \equiv x_0(mod\ m_i), i = 1,2, \ldots, n.$ Hence $x - x_0$ is a common multiple of $m_1, m_2 \ldots \ldots \ldots m_n$. it follows $x \equiv x_0(mod\ [m_1, m_2 \ldots m_n])$.

Next, we consider system of linear congruences with respect to moduli that are relatively prime in pairs. The result we state here is known as the Chinese remainder theorem, and is extremely useful in a number of contexts.

Corollary 2.9. (***Chinese Remainder Theorem***) suppose $m_1, m_2 \ldots \ldots \ldots m_n$ are natural numbers that are pair wise relatively prime and $a_1, a_2, \ldots, a_n$ are arbitrary integers. Then the system $x \equiv a_i(mod\ m_i), i = 1,2, \ldots, n$ has a solution. Moreover, if x and y are solution of the system then $x \equiv y(mod\ m_1 . m_2 \ldots m_n)$.

Proof: since for every distinct i and j,$(m_i, m_j) = 1$, and hence $[m_1, m_2 \ldots m_n] = m_1 . m_2 \ldots m_n$ the corollary is immediate from theorem proved above.

Remark 2.4. The proof in theorem 10 does not only give a necessary and sufficient condition for existence of solutions for the system but also an algorithm that could be used to find a solution. Indeed, if we are given a system of congruences

$$x \equiv a_i(mod\ m_i), i = 1,2, \ldots, n,$$

then we first obtain a solution x_0 to $x \equiv a_i(mod\ m_i), i = 1,2$, and solve the system

$$\begin{cases} x \equiv x_0(mod\ [m_1, m_2]) \\ x \equiv x_0(mod\ m_3) \end{cases}$$

Obtaining a solution x_1 of the last system, we again solve

$$\begin{cases} x \equiv x_1(mod\ [m_1, m_2, m_3]) \\ x \equiv a_4(mod\ m_4) \end{cases}$$

In this manner we obtain a specific solution to the system and use the theorem to find the complete solution of the system.

Example 2.6. Find the complete solution of the system of congruences

$$\begin{cases} x \equiv 3(mod\ 2) \\ x \equiv 4(mod\ 3) \\ x \equiv 2(mod\ 5) \\ x \equiv 5(mod\ 7) \end{cases}$$

Solution: Clearly the system has a solution. First consider the system $\begin{cases} x \equiv 3(mod\ 2 \\ x \equiv 4(mod\ 3) \end{cases}$

x_0 is a solution of the system iff $x_0 = 3 + 2t = 4 + 3q$ for some integers t and q. From the Diophantine equation $3 + 2t = 4 + 3q$, we get t=2 and q= 1 to be particular solution. Thus $x_0 = 7\ is\ a\ solution\ of\ the\ system. since\ [2,3]$=6, any solution of the system is given by $x \equiv 7(mod\ 6)$

Next we consider the subsystem $\begin{cases} x \equiv 7(mod\ 6) \\ x \equiv 2(mod\ 5) \end{cases}$

Using similar argument, we obtain -23 as a specific solution of the subsystem and the complete solution is given

by

$$x \equiv -23(mod\ 30).$$

We obtain -2543 as a specific solution of the subsystem and the complete solution is given by
$x \equiv -2543(mod\ 210)$

Since $-2543 \equiv 187(mod\ 210)$, the complete solution of the system is given by $x \equiv 187(mod\ 210)$

2.7. Properties of the Euler's Totient function

Theorem 2.10. The Euler's totient function, φ, is multiplicative.
Example 2.7. consider m=56. Then, it is evident that $\varphi\ (56) = \varphi\ (7).\varphi\ (8) = 6 \times 4 = 24$, where 7 and 8 are relatively prime. But, though $56 = 4 \times 14$, $\varphi\ (56) \neq \varphi\ (4).\varphi\ (14) = 12$ because 4 and 14 are not relatively prime.
Theorem2.11. If p is prime and n is natural number, then φ $(p^n) = p^{n-1}(p-1)$.In particular, φ $(p) = p - 1$.

Corollary 2.12. If $p_1, p_2, \ldots\ldots, p_n$ are distinct prime factors of the natural number m, then φ(m) =m $\prod_{i=1}^{n}(1 - \frac{1}{p_i})$.

Theorem 2.13. (**Euler- Fermat's Theorem**): If m is positive integer and (a, m) =1, then $a^{\alpha(m)} \equiv 1\ (mod\ m)$.
Note that Euler- Fermat's Theorem is the general case of Fermat's little Theorem.

2.8. Properties Higher Order Congruences

What has been developed in the previous section of this chapter can also be used to solve higher order congruence f(x) $\equiv 0(mod\ m)$. This is usually done by reducing the congruence to one of lower degree.

Theorem 2.14. (*Factor Theorem*) b is a solution of the congruence $f(x) \equiv 0(mod\ m)$ iff $f(x) \equiv (x-b)g(x)(mod\ m)$ for some polynomial $g(x)$ with integer coefficients and $deg\ g < deg\ f$.

Corollary 2.15. If p is a prime, f is a polynomial of degree n and $b_1, b_2, \ldots, b_t$ are incongruent solutions of $f(x) \equiv 0(mod\ p)$, then there exists an integer coefficient polynomial $g_t(x)$ of degree $n - t$ such that

$$f(x) \equiv (x-b_1)(x-b_2)\ldots(x-b_t)g_t(x)(mod\ p).$$

Lemma 2.16. If f(x) $= \sum_{k=0}^{n} a_k x^k$, then $f(a+b) = f(a) + bf'(a) + b^2q$ for some integer q and $f'(x) = \sum_{k=0}^{n} ka_k x^{k-1}$.

Theorem 2.17. Assume the p is a prime number and $\propto \geq 2$. x_0 is a solution of $f(x) \equiv 0(mod\ p^\alpha)$ iff $x_0 = b + cp^{\alpha-1}$ with b a solution of f(x)≡0(mod $p^{\alpha-1}$) and c is a solution of $\frac{f(b)}{p^{\alpha-1}} + yf'(b) \equiv 0(mod\ p)$.

Example 2.8. Find the solution of the congruence

$$f(x) = x^3 - x^2 + 7x + 1 \equiv 0(mod\ 200).$$

Solution: Since$200 = 2^3.5^2$, solving the congruence $f(x) \equiv 0(mod\ 200)$

Is equivalent to solving the system, $\begin{cases} f(x) \equiv 0(mod\ 8) \\ f(x) \equiv 0(mod\ 25) \end{cases}$

First, we solve each sub-congruence. Since 1 is the only solution of $(x) \equiv 0(mod\ 2)$, a solution of $f(x) \equiv 0(mod\ 4)$ is of the form 1+2c where c is the solution of $\frac{f(1)}{2} + yf'(1) \equiv 0(mod\ 2)$

But, f(1)=8 and f'(1)=8. Hence, 0 and 1 are possible choices for c. Thus 1+2c=1 or 3 are solutions of $f(x) \equiv 0(mod\ 4)$.

Case 1. Suppose we chooses b=1 as a solution of f(x) ≡0 (mod 4). Then we set $x_0 = 1 + 4c$, where c is a solution of the congruence.

$$\frac{f(1)}{4} + yf'(1) \equiv 0(mod\ 2)$$

We notice that c=0 and 1are also possible choices for c. Hence x_0=1, 1+$2^2 = 5$ are solutions of $f(x) \equiv 0(mod\ 8)$.

Case 2. Suppose we chooses b=3 as a solution of f(x) ≡0 (mod 4). Then

$x_0 = 3 + 4c$, with c is a solution of the congruence $\frac{f(3)}{4} + yf'(3) \equiv 0(mod\ 2)$, is a solution of $f(x) \equiv 0(mod\ 8)$.But $f(3) = 40\ and\ f'(3) = 28$. Thus, again, c=0 or1 are possible solutions of $f(x) \equiv 0(mod\ 8)$.

We conclude that 1, 3, 5, and 7 are solutions of $f(x) \equiv 0(mod\ 8)$ in a complete least residue system (mod 8). Of course, these could have been obtained by direct substitution.

With regard to the congruence $f(x) \equiv 0(mod\ 25)$,we first solve $f(x) \equiv 0(mod\ 5)$. by substitution, 3 is the only solution in the complete least residue system (mod 5). Then $x_0 = 3 + 5c$ is the solution of $f(x) \equiv 0(mod\ 25)$ where c is the solution of the congruence $\frac{f(3)}{5} + yf'(3) \equiv 0(mod\ 5)$,. But $f(3) = 40\ and\ f'(3) = 28$. Hence, c is the solution of 28y +8≡0 (mod 5). We notice that c=4 is the solution of the linear congruence in the complete least of residue system (mod 5). Hence, 23 is the only solution of $f(x)$ ≡0(mod 25) in the complete least residue system (mod 25). Finally, we solve each of the following system of congruences

$$\begin{cases} x \equiv 1(mod\ 8) \\ x \equiv 23(mod\ 25) \end{cases} \quad \begin{cases} x \equiv 3(mod\ 8) \\ x \equiv 23(mod\ 25) \end{cases} \quad \begin{cases} x \equiv 5(mod\ 8) \\ x \equiv 23(mod\ 25) \end{cases} \quad \begin{cases} x \equiv 7(mod\ 8) \\ x \equiv 23(mod\ 25) \end{cases}$$

Since (8, 25) =1, each system has a solution and we find that 73, 123, 173, and 23 are the respective solutions of the system in the complete least residue system (mod 200).

If the degree of the polynomial is larger than the modulus, we require the following theorem.

Theorem 2.18. If p is a prime and $deg\ f = n \geq p$, then there exists a polynomial $r(x)$ with degree less than p such that x_0 is the solution of $f(x) \equiv 0(mod\ p)$ if and only if it is a solution of $r(x) \equiv 0(mod\ p)$.

Proof: By long division method, let f(x)= $(x^p - x)q(x) + r(x)$ with $deg\ r \leq p - 1$ and r(x)=0. By Fermat's little theorem, for every$x = 0,1,2, \ldots \ldots, p - 1$, $x^p \equiv x(mod\ p)$.Hence, x_0 is a solution of $f(x) \equiv 0(mod\ p)$ iff it is a solution of $r(x) \equiv 0(mod\ p)$. This completes the proof.

Example 2.9. Solve the congruence $x^9 + 2x^6 - x^5 - x^2 + 4x \equiv 0(mod\ 25)$.

Solution: we first solve the congruence f(x) =$x^9 + 2x^6 - x^5 - x^2 + 4x \equiv 0(mod\ 5)$.

Since $x^5 \equiv x(mod\ 5)$, solving $f(x) \equiv 0(mod\ 5)$ is equivalent to solving

$$x + 2x^2 - x - x^2 + 4x \equiv 0(mod\ 5)$$

$$x^2 + 4x \equiv 0(mod\ 5)$$

Hence, 0 and 1 are the solution of $f(x) \equiv 0(mod\ 5)$. Using b=0, $x_0 = 5c$ is a solution of $f(x) \equiv 0(mod 25)$ where c is a solution of $\frac{f(0)}{5} + yf'(0) \equiv 0(mod\ 5)$. But f (0) =0 and f' (0) =4. Hence c =0 is a solution of {0,1,2, 3, 4}. Hence 0 is a solution of the congruence $f(x) \equiv 0(mod 25)$.

Using b=1, $x_0 = 1 + 5c$ is the solution of $f(x) \equiv 0(mod 25)$ where c is a solution of $\frac{f(1)}{5} + yf'(1) \equiv 0(mod\ 5)$. But f (1) =5 and f' (1) =18. Therefore, c=3 is the solution of the linear congruence 1+3y≡ $0(mod\ 5)$. It follows that 1+3(5) =16 is the solution of $f(x) \equiv 0(mod 25)$. Hence, o and 16 are the solutions of $f(x) \equiv 0(mod 25)$.

3. Main Result

In this section, we develop a modified algorithm for solving system of linear congruences without actually know that whether the system has solution or not, and we also use it in solving higher order congruences and their corresponding systems.

Proposition 3.1. Algorithm (Intelligent Inspection Type-I)

(1) Let $\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \vdots \\ x \equiv a_n (mod\ m_n) \end{cases}$ be a given system of linear congruences, where $a_{1,}, a_{2,\ldots} a_n$ are integers, and $m_{1,}, m_{2,\ldots} m_n$ are positive integers with $m_1 < m_2 < \cdots < m_n$. Let N=LCM ($m_{1,}, m_{2,\ldots} m_n$).

Step-1: Find the N

Step-2: Starting with the initial solution of $x \equiv a_n (mod\ m_n)$,

Step-3: Obtain all consecutive solutions of the underlying linear congruence up to the largest, which is less than N.

Step-4. Test whether each of the solutions of the congruence satisfy the remaining n-1 linear congruences in the system, or not. If we find one, that is the particular common solution of the system. Then we stop. Otherwise, we continue the same manner until we get the required solution, which is less than N.

Note 3.1: if such a solution does not exist, it is possible to conclude that the system has no solution.

Example 3.1. Solve the following system

$\begin{cases} 2x \equiv 3 (mod\ 5) \\ 3x \equiv 6 (mod\ 7) \end{cases}$

Solution: Using cancellation law, the above system is reduced to the system

$\begin{cases} x \equiv 4 (mod\ 5) \\ x \equiv 2 (mod\ 7) \end{cases}$

In using the above algorithm, the largest modulus is 7 and LCM (5, 7) =35. Then we find and test the solutions of the congruence $x \equiv 2 (mod\ 7)$ starting with the initial one, that is,$x_0 = 2$. Clearly, 2 is not solution of the other congruence. Then consider the next solution.

Any solution x is given by $x \equiv 2 (mod\ 7)$. In view division algorithm, it is given by x=2+7t, where t=0, 1, 2, 3, 4 so that x is less than 35.

Table 2: Solution of System of Two Linear Congruences with One Variable

t	*x=2+7t*	*Is x solution of* $x \equiv 4 (mod\ 5)$*?*	*Remark*
0	2	No	9 is the solution of the system
1	9	Yes	
2	16	No	
3	23	No	
4	30	No	

Thus, the solution of $x \equiv 2 (mod\ 7)$ which is also satisfies $x \equiv 4 (mod\ 5)$, is 9. Then any other solution x of the system is given by $x \equiv 9 (mod\ 35)$.

Example 3.2. Solve the following system $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$ [2]

Solution: We notice that the largest modulus in the system is 7 and LCM $(3, 5, 7) = 105$. According to the algorithm, we start solving the congruence $x \equiv 2(mod\ 7)$. In view of division algorithm, $x \equiv 2(mod\ 7)$ is written as $x = 2 + 7t$, where t= 0, 1, 2, 3, …, 14.

Table 3: Solution of System of Three Linear Congruences with One Variable

t	*x=2+7t*	*Is x solution of*	*Is x solution of*	*Remark*
0	2	Yes	No	Not solution of the System
1	9	No	No	Not solution of the System
2	16	No	No	Not solution of the System
3	23	Yes	Yes	Solution of the System
4	30	No	No	Not solution of the System
5	37	No	No	Not solution of the System
6	44	Yes	No	Not solution of the System
7	51	No	No	Not solution of the System
8	58	No	Yes	Not solution of the System
9	65	Yes	No	Not solution of the System
10	72	No	No	Not solution of the System
11	79	No	No	Not solution of the System
12	86	Yes	No	Not solution of the System
13	93	No	Yes	Not solution of the System
14	100	No	No	Not solution of the System

(*) <105= LCM $(3, 5, 7)$[3]

From the above analysis using the algorithm, the particular solution of the system is 23, and any solution x of the system is given by $x \equiv 23(mod\ 105)$.

Proposition 3.2. Algorithm (Intelligent Inspection type-II)

Step-1: Find the immediate (initial) solution of the linear congruence $x \equiv a_n(mod\ m_n)$, clearly the solution is a_n.

Step-2: Test whether a_n is the solution at least one of the remaining n-1 linear congruences in the system, or not.

[2] 'Sun Zi Suanjing (Problem 26' Volume 3) reads: "There are certain things whose number is unknown. A number is repeatedly divided by 3, the remainder is 2; divided by 5, the remainder is 3; and by 7, the remainder is 2. What will the number be?"', it was the first problem that led to the development of Chinese Remainder theorem as cited by SHEN KANGSHENG.

[3] The inequality (*) refers to the fact that the values of x in the second column are the consecutive solutions of $x \equiv 2(mod\ 7)$ which are $LCM\ (3, 5, 7) = 105$. Note that they are not all the solutions of the system considered.

Step-3: if a_n is the solution of $x \equiv a_{n-1}(mod\ m_{n-1})$, we find the LCM$(m_{n-1}, m_n)$ and the successive positive solution $a_n + t.\text{LCM}(m_{n-1}, m_n)$ modulo LCM(m_{n-1}, m_n) where $t = 0, 1, \ldots$ such that $a_n + t.\text{LCM}(m_{n-1}, m_n)$ is less than LCM(m_{n-2}, m_{n-1}, m_n) , followed by application of Step-2 on the linear congruence with modulus m_{n-2}.

Step-4. Continuing the same manner, we get a particular common solution x_0 of the given system (1). Moreover, any solution x of the system is given by $x \equiv a_n + t.\text{LCM}(m_2, \ldots, m_n)(mod\ N)$.

Remark 3.1. If such a solution does not exist, it is possible to conclude that the system has no solution.

The next example is already solved under section 2.5., in example #. here we solve it again for the purpose of making comparison between the former and the new algorithm developed in this paper. Thus, making use of the later algorithm we find the solution much more (significantly) quicker than the former one in which iterative grouping, conversion to system of linear equation and application of Euclid's algorithm is required.

Example 3.3. Find the complete solution of the system of congruences

$$\begin{cases} x \equiv 3(mod\ 2) \\ x \equiv 4(mod\ 3) \\ x \equiv 2(mod\ 5) \\ x \equiv 5(mod\ 7) \end{cases}$$

Solution: We start with the linear congruence $x \equiv 5(mod\ 7)$. Clearly, the immediate solution is 5. According to the above algorithm, the next solution, which satisfies the second[4] congruence is of the form $5 + 7t, t = 0, 1, 2, 3, 4 < 5$ Thus, this solution is 12 =5+7(1). Again, we find the next solution in a similar manner, where the solution has the form 12+t. LCM (7,5) = 12+35t with $t = 0, 1, 2 < 3$. Then the solution is 82 in modulo 105, because which satisfies the third congruence. The final solution which is the particular solution of the given system of the form 82+105t, with $t = 0, 1 < 2$. Thus, the solution is 187 in modulo $210 = LCM(2, 3, 5, 7)$.

4. Application to solving Higher Oder congruences and system of Higher Oder congruences

In this section we use the above algorithm in solving Higher Order congruences and their corresponding systems. We examine the algorithm by giving the following couple of illustrative examples.

4.1. Solving Higher order congruences

Example 4.1. Solve the following

$$f(x) = 9x^{17} + 3x^{10} + 3x^9 - 2x^2 + 2 \equiv 0(mod\ 15). \text{ ..... (1)}$$

Solution: using theorem 2.1(iii), and definition of congruence, we obtain the following system

$$\begin{cases} 9x^{17} + 3x^{10} + 3x^9 - 2x^2 + 2 \equiv 0(mod\ 5) \\ 9x^{17} + 3x^{10} + 3x^9 - 2x^2 + 2 \equiv 0(mod\ 3) \end{cases} \text{ ..... (2)}$$

Now, using theorem 2.18, we find the solutions of each one of the sub-congruences solving them separately. It is found that the particular incongruent solutions (mod5) of $9x^{17} + 3x^{10} + 3x^9 - 2x^2 + 2 \equiv 0(mod\ 5)$ are 1 and 2. Moreover, any solution x of this sub-congruence is given by:

$x \equiv 1(mod\ 5)$ or
$x \equiv 2(mod\ 5)$..... **(3)**

Similarly, by the same theorem used above, we possibly found the particular incongruent solutions (mod 3) of $9x^{17} + 3x^{10} + 3x^9 - 2x^2 + 2 \equiv 0(mod\ 3)$ are 1 and 2. Moreover, any solution x of this sub-congruence is given by:

$x \equiv 1(mod\ 3)$ or
$x \equiv 2(mod\ 3)$..... **(4)**

Now, we form the following four systems of linear congruences using the linear congruences in (3) and (4), and we obtain the solutions of these systems applying the new algorithm developed.

(i) $\begin{cases} x \equiv 1(mod\ 5) \\ x \equiv 1(mod\ 3) \end{cases}$ **(ii)** $\begin{cases} x \equiv 1(mod\ 5) \\ x \equiv 2(mod\ 3) \end{cases}$ **(iii)** $\begin{cases} x \equiv 2(mod\ 5) \\ x \equiv 1(mod\ 3) \end{cases}$ **(iv)** $\begin{cases} x \equiv 2(mod\ 5) \\ x \equiv 2(mod\ 3) \end{cases}$

[4] By the second solution we mean the solution which satisfies the linear congruence with lesser modulus (i.e. in this case, $x \equiv 2(mod\ 5)$.

In each of the systems (i) to (iv), We start with the linear congruence with the modulus 5. According to the above algorithm, the next solution, which satisfies the second[5] congruences is of the form $1+5t, t=0,1,2<3$,and $2+5t, t=0,1,2<3$.Thus, As it can easily be seen, the systems (i) and (iv) take on the solutions 1 and 2 ,that is, where t=0 in both cases. Whereas, in the case of systems (ii) and (iii) the solutions are found, respectively, when t=2 and t=1.Thus, the solutions are 11 and 7. Therefore, the incongruent solutions modulo 15 of the HOC (1), are 1, 2, 7, and 11. Any solution x of the Higher order congruence is given by:

$x \equiv 1(mod\ 15)$ or
$x \equiv 2(mod\ 15)$ or
$x \equiv 7(mod\ 15)$ or
$x \equiv 11(mod\ 15)$.

4.2. Solving system of Higher Order Congruences

Example 4.2. Solve the following

$$\begin{cases} x^2+5x+4 \equiv 0(mod 21) \\ x^2+5x \equiv 0(mod\ 46) \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Solution: As we have done in above examples, we first reduce the given system into systems of sub-systems of sub- congruences of each of the congruences of the original system, as follows

$$\begin{cases} \begin{cases} x^2+5x+4 \equiv 0(mod 3) \\ x^2+5x+4 \equiv 0(mod 7) \end{cases} \\ \begin{cases} x^2+5x \equiv 0(mod\ 2) \\ x^2+5x \equiv 0(mod\ 23) \end{cases} \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Solving each sub-system in (2), separately; again, by solving each quadratic congruence in the sub-systems using factor theorem and theorem 2.18, we obtain, consecutively, the following solutions:

$x \equiv 1(mod\ 3)$ or $x \equiv 2(mod\ 3)$

$x \equiv 2(mod\ 7)$ or $x \equiv 6(mod\ 7)$ ..... (3)

$x \equiv 0(mod\ 2)$ or $x \equiv 1(mod\ 2)$

$x \equiv 0(mod\ 23)$ or $x \equiv 18(mod\ 23)$ ..... (4)

Using linear congruences in (3) and (4), separately, we form the following pair of four systems and we find their solutions using the new algorithm as follows:

(i) $\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 2(mod\ 7) \end{cases}$ **(ii)** $\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 6(mod\ 7) \end{cases}$ **(iii)** $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 2(mod\ 7) \end{cases}$ **(iv)** $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 6(mod\ 7) \end{cases}$ and

As to the algorithm, we start with the initial solutions of the linear congruences with larger moduli

Table 4: Solution of System of Two linear Congruences in solving SHOC

t	x=2+7t	Is x solution of $\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 2(mod\ 7) \end{cases}$	Is x solution of $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 2(mod\ 7) \end{cases}$	x=6+7t	Is x solution of $\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 6(mod\ 7) \end{cases}$	Is x solution of $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 6(mod\ 7) \end{cases}$
0	2	No	Yes	6	No	No
1	9	No	No	13	Yes	No
2	16	Yes	No	20	No	Yes

[5] By the second solution we mean the solution which satisfies the linear congruence with lesser modulus (i.e. in this case, $x \equiv 2(mod\ 5)$.

In table 4 above, using the algorithm, the incongruent solutions (mod 21) of the sub-system are 2, 13, 16, and 20. any solution x of the sub-system is given by:

$x \equiv 2(mod\ 21)$,

$x \equiv 13(mod\ 21)$,

$x \equiv 16(mod\ 21)$ or

$x \equiv 20(mod\ 21)$ …………………………………………………..… (5)

Similarly, we solve the following systems

(v) $\begin{cases} x \equiv 0(mod\ 2) \\ x \equiv 0(mod\ 23) \end{cases}$ **(vi)** $\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 18\ (mod\ 23) \end{cases}$ **(vii)** $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 0\ (mod\ 23) \end{cases}$ **(viii)** $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 18\ (mod\ 23) \end{cases}$

Table 5 :Solution of System of Two Linear Congruences in solving SHOC

t	x=23t	Is x solution of $\begin{cases} x \equiv 0(mod\ 2) \\ x \equiv 0(mod\ 23) \end{cases}$	Is x solution of $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 0(mod\ 23) \end{cases}$	x=18+23t	Is x solution of $\begin{cases} x \equiv 0(mod\ 2) \\ x \equiv 18(mod\ 23) \end{cases}$	Is x solution of $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 18(mod\ 23) \end{cases}$
0	0	Yes	No	18	Yes	No
1	23	No	Yes	41	No	Yes

In table 5 above, using the algorithm, the incongruent solutions (mod 46) of the sub-system are 0, 23, 18, and 41. any solution x of the sub-system is given by:

$x \equiv 0(mod\ 46)$,

$x \equiv 23(mod\ 46)$,

$x \equiv 18(mod\ 46)$ or

$x \equiv 41(mod\ 46)$ …………………………………………………..… (6)

Now, using linear congruences in (5) and (6), we form the following sixteen systems and we find their solutions using the new algorithm as follows:

$\begin{cases} x \equiv 2(mod\ 21) \\ x \equiv 0(mod\ 46) \end{cases}$, $\begin{cases} x \equiv 2\ (mod\ 21) \\ x \equiv 18\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 2\ (mod\ 21) \\ x \equiv 23\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 2\ (mod\ 21) \\ x \equiv 41\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 13(mod\ 21) \\ x \equiv 0(mod\ 46) \end{cases}$,
$\begin{cases} x \equiv 13\ (mod\ 21) \\ x \equiv 18\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 13(mod\ 21) \\ x \equiv 23\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 13(mod\ 21) \\ x \equiv 41\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 16(mod\ 21) \\ x \equiv 0(mod\ 46) \end{cases}$, $\begin{cases} x \equiv 16\ (mod\ 21) \\ x \equiv 18\ (mod\ 46) \end{cases}$,
$\begin{cases} x \equiv 16(mod\ 21) \\ x \equiv 23\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 16(mod\ 21) \\ x \equiv 41\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 20(mod\ 21) \\ x \equiv 0(mod\ 46) \end{cases}$, $\begin{cases} x \equiv 20\ (mod\ 21) \\ x \equiv 18\ (mod\ 46) \end{cases}$, $\begin{cases} x \equiv 20(mod\ 21) \\ x \equiv 23\ (mod\ 46) \end{cases}$,
$\begin{cases} x \equiv 20(mod\ 21) \\ x \equiv 41\ (mod\ 46) \end{cases}$

Table 6: The complete set of integers modulo LCM (21, 46) =966

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
46t	0	46	92	138	184	230	276	322	368	414	460	506	552	598	644	690	736	782	828	874	920
18+ 46t	18	64	110	156	202	248	294	340	386	432	478	524	570	616	662	708	754	800	846	892	938
23+ 46t	23	69	115	161	207	253	299	345	391	437	483	529	575	621	667	713	759	805	851	897	943
41+ 46t	41	87	133	179	225	271	317	363	409	455	501	547	593	639	685	731	777	823	869	915	961

The table 6 contains four groups of integers from which we obtain the incongruent solutions (mod 966) of the system (1) using the algorithm.

In each of the systems, we start with the linear congruence with the modulus 46. According to the underlying algorithm, the solutions of all the systems, which satisfies the first linear congruences are of the form $0 + 46t$, $18 + 46t, 23 + 46t,$ and $41 + 46t, t = 0, 1, 2, \ldots, 20 < 21$ so that all the sixteen solutions are less than LCM(21, 46). Thus, the incongruent solutions modulo LCM (21, 46) of the SHOC (1), are 23, 41, 184, 202,230,317,391, 478,506, 667, 685, 713, 800, 874 and 961. Any solution x of the System Higher order congruences (1) is congruent to one of the incongruent solutions modulo 966.

5. Conclusion

Aside from the known methods and techniques for solving SLC, HOC of composite moduli and SHOC, this algorithm provides another way arriving at a particular solution of the underlying congruence equations, that minimize the difficulties and the amount of time required in seeking solution significantly. Thus, we introduced this algorithm (intelligent inspection) which is easier as compared to Euclid's Algorithm and Euler's Method for solving linear congruences, it supports tools, mentioned in theorem 2.17. and 2. 18, for solving HOC and their systems. With the simplicity of this algorithm, those who are beginners in leaning system of linear congruences and their higher degree partners, may found this method more preferable those already published in books and journals. Moreover, this algorithm can be used as basis for developing computer program that can solve system of linear congruences with much more efficiency, and application of the algorithm in the class room, specifically in number theory classes is highly recommended in order to facilitate the teaching learning of the concepts of SLC, HOC and SHOC more effectively. Finally, we suggest for interested scholars in the area, that they would strive for developing generalized version of the algorithm, and investigation of further applications of this algorithm and related ones.

6. References

Burton, D. M. (2011). *Elementary Number Theory* (7th ed ed.). New York, 1221 Avenue of the AmericasNY 10020.: Published by McGraw-Hill.

Eugel Verdal. (2006). Solutions of Some Classes of Congruences. *The Teaching of Mathematics, 9*(1), 41-44.

G. H. Hardy, a. E. (1979). *An Introduction to the Theory of Numbers, .* Oxford : Oxford University Press.

Gold N.E, T. C. (2002). From system comprehension to program comprehension,. *26th Annual International Computer Software and Applications Conference* (pp. 26-29). Oxford,England: Los Almitos,CA: IEEE , pp 427-432.

John Frederic Chionglo. (2016). How I solved The linear Congruence 25x=15(mod 29)? doi:10.13140/RCR 2.2.1476856324

Jones G.A, J. J. (1998). Congruences,. In J. J. Jones G.A, *Elementary Number Theory* (p. Springer Undergraduate Mathematics Series). London: Springer.

Niven, S. Z. (1991.). *An Introduction to the Theory of Numbers, , .* New York.

Polemer M. Cuarto. (2014). Algebraic Algorithm for solving linear Congruences: its application to Cryptography. *APJEAS, 1*(1), 34-37. Retrieved from www.apjeas.apimr.com

Rosen, K. H. (1984). *Elementary number theory and its applications.* Read ing, , Massachusetts,: Addison-Wesley Publishing Company.

Smarandache, F. (2007). An Algorithm For Solving Linear gongruences and System of Linear Congruences. doi:10.2139/ssm.2725483.

William Stein. (2009). *Elementary number theory: Primes, Congruences and Secrets,* . (S. A. Ribert, Ed.) New York, , NY 10013, 233 Spring Street, , USA: Springer Science and Business Media, LLC. doi:10.1007/978-0-387-85