Vol. 31 · January 2018
DOI: https://doi.org/10.7719/jpair.v31i1.566

Print ISSN 2012-3981
Online ISSN 2244-0445

On Generalized Solutions of Linear Congruence ax ≡ b (mod n) for Large Modulus n

POLEMER M. CUARTO
http://orcid.org/0000-0002-5507-3640
polemath@yahoo.com
Mindoro State College of Agriculture and Technology
Calapan City, Oriental Mindoro, Philippines

Originality: 99% • Grammar Check: 90 • Plagiarism: 1

ABSTRACT

Number Theory, a branch of Pure Mathematics, is crucial in cryptographic algorithms. Many cryptographic systems depend heavily on some topics of Number Theory. One of these topics is the linear congruence. In cryptography, the concept of linear congruence is used to directly underpin public key cryptosystems during the process of ciphering and deciphering codes. Thus, linear congruence plays a very important role in cryptography. This paper aims to develop an alternative method and generalized solutions for solving linear congruence ax ≡ b (mod n). This study utilized expository-developmental research method. As a result, the alternative method considered two cases: (1) when (a,n) = 1 and (2) when (a,n) > 1. The basic idea of the method is to convert the given congruence ax ≡ b (mod n) to ax = b + kn for some k, reduce modulus n by interchanging a and n, simplify the new congruence and perform the process recursively until obtaining a congruence that is trivial to solve. The advantage

of this method over the existing approaches is that it can solve congruence even for large modulus n with much more efficiency. Generalized solution of linear congruence $ax \equiv b \pmod{n}$ considering both cases was obtained in this study.

Keywords – Number Theory, cryptography, expository-developmental research, Philippines

INTRODUCTION

In the global information economy, personal data have become the fuel, driving much of current online activity (United Nations, 2016). Day-by-day, large amount of data are transmitted, stored and collected across the globe enabled by massive improvements in computing and communication power. Protecting these data and privacy rights online is a significant and increasingly urgent challenge for policymakers. Thus, the use of cryptography has become popular and vital.

Linear congruence plays a very important role in cryptographic system. It is widely used in the encryption and decryption of codes in public key cryptosystems like the Rivest Shamir Adlemann (RSA) system (Ashioba & Yoro, 2014; Gupta, Srivastava, & Singh, 2012). Because of this, numerous researchers and mathematics educators have been interested in studying and developing methods for solving linear congruence $ax \equiv b \pmod{n}$.

A standard method of solving linear congruence involves the use of multiplicative inverse of a modulo n (Ore, 1988; Burton, 1989). Using this method, multiplying the linear congruence $ax \equiv b \pmod{n}$ through by the factor a^{-1} gives $x = ba^{-1} \pmod{n}$. However, finding multiplicative inverse for large number is quite difficult, thus using this method will also take time in finding the congruence classes (Koddoura, 2006).

Another method used to solve linear congruence is an approach which translates the given congruence into Diophantine equation $ax + by = c$ to solve linear congruence and solve using Extended Euclidean Algorithm. However, according to Gold (1995), using Diophantine equations in finding congruence classes for $ax \equiv b \pmod{n}$ require at most $\log_2(b)$ iterations, or in the case $a<n$, $1+\log_2(a)$ iterations.

Remodulization method, a novel solution for linear congruence was introduced by (Gold & Tucker, 1995), which characterizes the conditions under which solutions exists and then determines the solution space. This novel method

relates the solutions space of $cx \equiv b \pmod n$ to the Euler function c rather than of b. This allows one to develop an alternative efficient approa ch to encryption and decryption of codes in public key cryptosystems. However, this method is not that efficient for large modulus n since characterizing the conditions under which solutions exists for large n is a cumbersome task.

An algebraic method for solving linear congruence was introduced in 2014. This method translates the linear congruence into a algebraic linear equation $x = b+nq$, where b is the residue, n is the modulus and q is any arbitrary integer. After translating into linear equation, the equation is then solved algebraically (Cuarto, 2014; Cuarto 2015).

Although there are existing approaches developed, finding solutions to congruence still remain pedagogically difficult especially on the part of the students. This is because the methods make use of complex algorithms. Thus, in this paper, the researcher aimed to develop an alternative method for solving congruence class $ax \equiv b \pmod n$ that does not use an exhaustive, gradual and incremental method which invites a definite risk of computation complexity.

This study aimed to generalize solution of linear congruence $ax \equiv b \pmod n$. Specifically, the study sought to:

1. determine an alternative method for solving linear congruence $ax \equiv b \pmod n$ for large modulus n considering case when $(a,n) = 1$ and when $(a,n) > 1$;
2. validate the developed alternative method using formal proof and illustrative examples.

The results of this study are deemed important for Mathematics students, instructors, computer programmers as well as future researchers. Using the developed alternative method, Mathematics students especially the beginners who are taking up Number Theory can easily solve problems on linear congruence since it uses the concept of algebraic principles which every Mathematics student is familiar with. Utilizing the algorithm presented in this paper will help them realize that Mathematics can be made simpler because the method 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 congruence in Number Theory. Similarly, the result of this study can help those in the field of cryptography because the concept of linear congruence is used in ciphering and deciphering codes for network security and others. This algorithm could also give programmers insights in developing a program based on this technique that can automatically solve problems on linear congruence. This study would also provide input for

future researchers who will conduct studies on development of other Number Theory-based cryptosystem.

FRAMEWORK

This paper was built on the following definitions, theorems and properties which will be used further in the development of this paper. These were taken from several readings of the works of Adams (2010), Burger (2006), Stein (2008), Benjamin and Brown (2009), Rose (2010), Rosen (2011) and Wall (2010).

Definition 1. A **congruence** is a linear equation involving congruent relations. Let n be a fixed positive number. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b \pmod{n}$ if n divides the difference $a - b$; that is, provided *that* $a - b = kn$ for some integer k.

Congruences may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is similar to ordinary equality (=). Some of the basic properties of equality that carry over to congruences appear in the following theorem.

Definition 2. A **congruence class** $[a]_n$ is the set of all integers that have the same remainder as a when divided by n. If a linear congruence $ax \equiv b \pmod{n}$ has a particular solution, it has an infinite number of solutions. Thus, the complete congruence class solutions can be expressed as $[x_0]_n$ where x_0 is a particular solutions and n is the modulus.

Theorem 1. In modular arithmetic, if a and b are any integers and n is a positive integers, then the congruence $ax \equiv b \pmod{n}$ has a solution for x if and only if the greatest common divisor of a and n (denoted by gcd (a,n)) is a factor of b.

Theorem 2. The congruence $ax \equiv b \pmod{n}$, $n \neq 0$, with $\gcd(a,n) = d|b$, has d distinct solutions.

Theorem 3. If $a \equiv b \pmod{n}$ then $b = a + nq$ for some integer q, and conversely.

Theorem 4. For any integers a and b, and positive integer n, $a \equiv a \pmod{n}$.

Proof: $n|(a - a)$ since 0 is divisible by any integer. Therefore, $a \equiv a \pmod{n}$.

Theorem 5. For any integers a and b, and positive integer n, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Proof: If $a \equiv b \pmod{n}$ then $n|(b - a)$. Therefore, $n|(-1)(b - a)$ or $n|(a - b)$. Therefore, $b \equiv a \pmod{n}$.

Theorem 6. For any integers a and b, and positive integer n, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Proof: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $n|(b-a)$ and $n|(c-b)$. Using the linear combination theorem, $n|(b - a + c - b)$ or $n|(c - a)$. Thus, $a \equiv c \pmod{n}$.

Theorem 7. If $a \equiv b \pmod{n}$, then $b = a + nk$ for some integer k, and conversely.

Proof: If $a \equiv b \pmod{n}$ then by definition $n|(b - a)$. Therefore, $b - a = nk$ for some k. Thus $b = a + nk$. Conversely if $b = a + nk$, then $b-a = nk$ and so $n|(b-a)$ and hence $a \equiv b \pmod{n}$, then $b = a + nk$.

Theorem 8. If $a \equiv b \pmod{n}$ then a and b leave the same remainder when divided by n.

Proof: Suppose $a \equiv b \pmod{n}$. Then by Theorem 6, $b = a + nk$. If a leaves the remainder r when divided by n, we have $a = nk + r$ with $0 \leq r$.

Theorem 9. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

Proof: Using Theorem 6, $b = a + nk_1$ and $d = c + nk_2$. Then adding equalities, we get $b + d = a + c + nk_1 + nk_2 = a + c + n(k_1 + k_2)$. This shows that $a + c \equiv b + d \pmod{n}$ by Theorem 6.

Theorem 10. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Proof: Using Theorem 6, $b = a + nk_1$ and $d = c + nk2$. By multiplying, we get $bd = (a + nk_1)(c + nk_2) = ac + nak_2 + nck_1 + n_2k_1k_2$. Thus, $bd = ac + n(ak_2 + ck_1 + nk_1k_2)$, and so $ac \equiv bd \pmod{n}$, by Theorem 6.

Theorem 11. If $a \equiv b \pmod{n}$, and c is a positive integer, then, $ca \equiv cb \pmod{cn}$.

Proof: Since $n|(b - a)$, we have $cn|c(b - a)$ or $cn|(cb - ca)$.

These definitions and theorems were used in establishing a formal mathematical proof of the alternative method for solving linear congruence specifically for large modulus n.

METHODOLOGY

The study is expository research in nature, thus, the resources found in the library and electronic resources was used in the conduct of the study. Expository research is a research that gives detailed solutions and exposes it using set of words that is understandable to the readers (Roxas & Reyes, 2013). This study will focus on the development of an alternative method for solving congruence classes for $ax \equiv b \pmod{n}$. The method was subjected through a series of trials and computations before arriving at generalized solutions. This was validated through a formal proof and illustrative examples.

For a better understanding of the study, related concepts were discussed in the preliminaries. These concepts are definition, theorems and properties related to linear congruence.

Several articles and related studies from general references, books, journals and internet sources were reviewed and cited to establish a systematic and mathematical analysis of the topic. The presentation of every topic are systematic and illustrative in order for the students and general readers to comprehend easily what is being discussed. For the purpose of clarifying concepts in the research study, experts in the field and colleagues in the academe were consulted to be able to present the topic more clearly and understandable

RESULTS AND DISCUSSION

The subsequent sections are systematically structured as follows: first, the steps of the developed alternative method for solving linear congruence $ax \equiv b \ (mod\ n)$ as well as its proof were presented, then some illustrative examples in cases when a and n have greatest common divisor equal to 1 and when a and n have greatest common divisor greater than 1 were also provided. A shorter version of the solutions using the alternative method is also given after each illustrative example to simplify the computations. Discussion on the development of linear congruence solver is also presented in the succeeding section.

Alternative Method for Solving Linear Congruence $ax \equiv b \ (mod\ n)$

Linear congruence in the form $ax \equiv b \ (mod\ n)$ can be expressed to a linear equation in the form $x = b + nq$, where b is a residue, n is the modulus and q is an arbitrary integer. From this, the idea of solving linear congruence $ax \equiv b \ (mod\ n)$ algebraically emanated. The basic idea of the method is to express the given congruence to linear equation and reduce the modulus recursively until arriving at a congruence that is trivial to solve.

Existing methods work well when the modulus n is not large. However, for large n, the methods become useless as the solution becomes more exhaustive. The advantage of the alternative method is that it can solve linear congruence $ax \equiv b \ (mod\ n)$ even for large n. The alternative method considered two cases: case 1: when $(a,n) = 1$ and case 2: when $(a,n) > 1$. The steps in solving linear congruence $ax \equiv b \ (mod\ n)$ using the developed alternative method is as follows:

CASE 1: When (a,n) = 1

Step 1. Check the solvability of the given linear congruence.

Step 2. Convert the given linear congruence $ax \equiv b \pmod{n}$ into linear equation $ax = b + nk$.

Step 3. Reduce the modulus n by interchanging a and n algebraically. Simplify and solve the new congruence $nk \equiv -b \pmod{a}$. Perform this step recursively until obtaining a congruence that is trivial to solve.

Step 4. Substitute the values of a, b, n and k to the equation $x_0 = \frac{b+nk}{a}$ to solve the given congruence.

CASE 2: When (a,n) > 1

Step 1. Check the solvability of the given linear congruence.

Step 2. Convert the given linear congruence $ax \equiv b \pmod{n}$ into linear equation $ax = b + nk$.

Step 3. Reduce the modulus n by interchanging a and n algebraically. Simplify and solve the new congruence $nk \equiv -b \pmod{a}$. Perform this step recursively until obtaining a congruence that is trivial to solve.

Step 4. Substitute the values of a, b, n and k to the equation $x_0 = \frac{b+nk}{a}$ to solve the given congruence. If x_0 is a particular solution to the $ax \equiv b \pmod{n}$, then the complete congruence class solution is given by:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d} \text{ where } d = (a,n).$$

Proof of the Alternative Method for Solving Linear Congruence $ax \equiv b \pmod{n}$

This section provides validity of the developed alternative method for solving linear congruence $ax \equiv b \pmod{n}$ by showing the theorems as well as its proof.

Step 1. Check the solvability of the given linear congruence.

Theorem 1. In modular arithmetic, if a and b are any integers and n is a positive integer, then the congruence $ax \equiv b \pmod{n}$ has a solution for x if and only if d (the greatest common divisor of a and n) is a factor of b.

Proof: *Let b be an integer and d is (a,n). By theorem 3, $ax = b + ny$ for some integer y. By Subtraction Property of Equality, $ax - ny = b$ which is a linear Diophantine equation. If d divides b, then the Diophantine equation has solution, so the congruence has solutions.*

Step 2. Convert the given linear congruence ax ≡ b (mod n) into linear equation ax = b + nk for some integer k.

Theorem 3. If a ≡ b (mod n), then b = a + nk for some integer k, and conversely.

Proof*: If a ≡ b mod n then by definition n|(b – a). Therefore, b – a = nk for some k. Thus b = a + nk. Conversely if b = a + nk, then b–a = nk and so n|(b–a) and hence a ≡ b mod n then b = a + nk.*

Step 3. Reduce the modulus *n* by interchanging *a* and *n* algebraically. Simplify and solve the new congruence nk ≡ -b (mod a). Perform this step recursively until obtaining a congruence that is trivial to solve.

Proposition 1. Let a, b, n and x be positive integers, then ax ≡ b (mod n) is congruent to nk ≡ -b (mod a) for some integer k.

Proof*. If ax ≡ b (mod n), then by Theorem 3, ax = b + nk for some integer k. Thus, ax - b = nk, by Subtraction Property of Equality and nk = ax – b, by Symmetric Property of Equality. By Theorem 3, nk ≡ -b (mod a).*

Step 5. Substitute the values of a, b, n and k to the equation **x = (b + nk)/a** to solve the given congruence.

Proposition 2. Let a, b, n and k be positive integers, then the solution to x ≡ b (mod n) is given by x = (b + nk)/a.

Proof. *By Theorem 3,* ax ≡ b (mod n) is congruent to ax = b + nk for some integer k. By Division Property of Equality, x = (b + nk)/a.

CASE 1: When (a,n) = 1
Illustrative Example 1

Solve the linear congruence 11x ≡ 42(mod 101).

Step 1. Check the solvability of the given linear congruence.

To check the solvability of the given congruence, we use Theorem 1 which is previously stated in the preliminaries**.**

In modular arithmetic, if a and b are any integers and n is a positive integer, then the congruence ax ≡ b (mod n) has a solution for x if and only if d (the greatest common divisor of a and n) is a factor of b. If d|b, then, it has d mutually incongruent solutions modulo n.

Since the greatest common divisor of 11 and 101 is 1, which is a factor of 42, the linear congruence ***11x ≡ 42(mod 101)*** has a unique solution.

Note: In case when a and n are relatively prime, the given congruence always has a unique solution since 1 divides any value of b. Thus, there is no need to check solvability condition.

Step 2. Convert the given linear congruence ax ≡ b (mod n) into linear equation ax = b + nk.

The linear congruence ***11x ≡ 42(mod 101)*** when converted to linear equation is given as : 11x = 42 + 101k.

Step 3. Reduce the modulus *n* by interchanging *a* and *n* algebraically.

11x = 42 + 101k
11x – 42 = 101k
101k = -42 + 11x
101k = -42 (mod 11)

Step 4. Simplify and solve the new congruence nk ≡-b (mod a). Perform step 3 and 4 recursively until obtaining a congruence that is trivial to solve.

101k = -42 (mod 11)
2k = 2 (mod 11)

Since this congruence can be easily solved now, there is no need to repeat step 3 and 4 process.

k = 1(mod 11)

Step 5. Substitute the values of a, b, n and k to the equation **x = (b + nk)/a** to solve the given congruence.

x = (b + nk)/a
x = [42 + 101(1)] / 11
x = (42 + 101) / 11
x = 143 / 11
x = 13

Thus, the congruence class solution of ***11x ≡ 42(mod 101)*** is $[13]_{101}$.

A shorter version of the solution of ***11x ≡ 42(mod 101)*** is given below:

11x ≡ 42(mod 101)

11x = 42 + 101k	Converting to linear equation
101k = -42 (mod 11)	Interchanging *a* and *n*

$2k = 2 \pmod{11}$	Simplifying the congruence
$k = 1 \pmod{11}$	Solving the congruence in terms of k
$x = (b + nk)/a$	
$x = [42 + 101(1)] / 11$	Substituting values to the general solution
$x = 13$	Simplifying the equation
$x = [13]_{101}$	The congruence class solution of
$11x \equiv 42 \pmod{101}$.	

Illustrative Example 2
Solve the linear congruence $35x \equiv 67 \pmod{509}$.

Step 1. Check the solvability of the given linear congruence.

Since a and n are relatively prime, the given congruence always has a unique solution since 1 divides any value of b. Thus, there is no need to check solvability condition.

Step 2. Convert the given linear congruence $ax \equiv b \pmod{n}$ into linear equation $ax = b + nk$

The linear congruence ***$35x \equiv 67 \pmod{509}$*** when converted to linear equation is given as: $35x = 67 + 509k$.

Step 3. Reduce the modulus *n* by interchanging *a* and *n* algebraically.

$35x = 67 + 509k$
$35x - 67 = 509k$
$509k = -67 + 35x$
$509k = -67 \pmod{35}$

Step 4. Simplify and solve the new congruence $nk = -b \pmod{a}$. Perform step 3 and 4 recursively until obtaining a congruence that is trivial to solve.

$509k = -67 \pmod{35}$
$19k = 3 \pmod{35}$

Since this congruence is still complex, there is a need to repeat step 3 and 4 process.

$19k = 3 \pmod{35}$
$19k = 3 + 35k_1$
$19k - 3 = 35k_1$
$35q_1 = -3 + 19q$

$35k_1 = -3 \pmod{19}$
$16k_1 = 16 \pmod{19}$
$k_1 = 1 \pmod{19}$
$19k = 3 + 35k_1$
$19k = 3 + 35(1)$
$19k = 3 + 35$
$19k = 38$
$k = 2$

Step 5. Substitute the values of a, b, n and k to the equation **x = (b + nk)/a** to solve the given congruence.

x = (b + nk)/a
$x = [67 + 509(2)] / 35$
$x = (67 + 1018) / 35$
$x = 1085 / 35$
$x = 31$

Thus, the congruence class solution of $\boldsymbol{35x \equiv 67 (mod\ 509)}$ is $[31]_{509}$.
A shorter version of the solution of $\boldsymbol{35x \equiv 67 (mod\ 509)}$ is given below:

$35x \equiv 67 (mod\ 509)$

$35x = 67 + 509k$	Converting to linear equation
$509k = -67 \pmod{35}$	Interchanging *a* and *n*
$19k = 3 \pmod{35}$	Simplifying the congruence
$19k = 3 + 35k_1$	Converting to linear equation
$35k_1 = -3 \pmod{19}$	Interchanging *a* and *n*
$16k_1 = 16 \pmod{19}$	Simplifying the congruence
$k_1 = 1 \pmod{19}$	
$19k = 3 + 35q_1$	Solving the congruence in terms of k
$k = 2$	
x = (b + nk)/a	
$x = [67 + 509(2)] / 35$	Substituting values to the general solution
$x = 31$	Simplifying the equation

$x = [31]_{509}$ The solution of **$35x \equiv 67 (mod\ 509)$.**

CASE 2: When (a,n) >1

Illustrative Example 1

Solve the linear congruence 14x ≡ 35(mod 301).

Step 1. Check the solvability of the given linear congruence.

To check the solvability of the given congruence, we use Theorem 1 which is previously stated in the preliminaries**.**

In modular arithmetic, if a and b are any integers and n is a positive integer, then the congruence ax ≡ b (mod n) has a solution for x if and only if d (the greatest common divisor of a and n) is a factor of b. If d|b, then, it has d mutually incongruent solutions modulo n.

To find the greatest common divisor of *a* and *n*, use the Euclidean Algorithm.

GCD of 14 and 301

301 = 14*21 + 7

14 = 7*2 + 0

(14,301) = 7

Since the greatest common divisor of 14 and 301 is 7, which is a factor of 35, the linear congruence ***14x ≡ 35(mod 301)*** has exactly 7 congruence class solutions modulo *n*.

Step 2. Convert the given linear congruence ax ≡ b (mod n) into linear equation ax = b + nk.

The linear congruence ***14x ≡ 35(mod 301)*** when converted to linear equation is given as: 14x = 35 + 301k.

Step 3. Reduce the modulus *n* by interchanging *a* and *n* algebraically.

14x = 35 + 301k

14x – 35 = 301k

301k = -35 + 14x

301k = -35 (mod 14)

Step 4. Simplify and solve the new congruence nk =-b (mod a). Perform step 3 and 4 recursively until obtaining a congruence that is trivial to solve.

301k = -35 (mod 14)

7k = 7 (mod 2)

Since this congruence can be easily solved now, there is no need to repeat step 3 and 4 process.

k = 1(mod 2)

Step 5. Substitute the values of a, b, n and k to the equation **x = (b + nk)/a** to solve the given congruence.

x = (b + nk)/a

x = [35 + 301(1)] / 14

x = (35 + 301) / 14

x = 336 / 11

x = 24

One congruence class solution of $14x \equiv 35 \pmod{301}$ is $[24]_{101}$.

If x is a solution, then a complete congruence class solution is:

x, x + n/d, x + 2n/d, . . ., x + (d-1)n/d where d = (a, n).

Therefore, the complete congruence class solution to $14x \equiv 35 \pmod{301}$ is $[24]_{301}$, $[67]_{301}$, $[110]_{301}$, $[153]_{301}$, $[196]_{301}$, $[239]_{301}$, and $[282]_{301}$.

A shorter version of the solution of $14x \equiv 35 \pmod{301}$ is presented below:

(14, 301) = 7	Finding the gcd
7 is a factor of 35	Checking solvability
14x = 35 + 301k	Converting to linear equation
301k = -35 (mod 14)	Interchanging *a* and *n*
7k = 7 (mod 2)	Simplifying the congruence
k = 1 (mod 2)	Solving the congruence in terms of k
x = (b + nk)/a	
x = [35 + 301(1)] / 14	Substituting values to the general solution
x = 24	Simplifying the equation
x = $[24]_{301}$	The congruence class solution of **$14x \equiv 35 \pmod{301}$.**

The complete set of congruence class solutions are: $[24]_{301}$, $[67]_{301}$, $[110]_{301}$, $[153]_{301}$, $[196]_{301}$, $[239]_{301}$, and $[282]_{301}$.

Illustrative Example 2

Solve the linear congruence $48x \equiv 36(mod\ 138)$.

Step 1. Check the solvability of the given linear congruence.

To check the solvability of the given congruence, we use Theorem 1 which is previously stated in the preliminaries**.**

In modular arithmetic, if a and b are any integers and n is a positive integer, then the congruence $ax \equiv b\ (mod\ n)$ has a solution for x if and only if d (the greatest common divisor of a and n) is a factor of b. If d|b, then, it has d mutually incongruent solutions modulo n.

To find the greatest common divisor of *a* and *n*, use the Euclidean Algorithm.

GCD of 48 and 138

138 = 48*2 + 42

48 = 42*1 + 6

42 = 6*7 + 0

(48, 138) = 6

Since the greatest common divisor of 48 and 138 is 6, which is a factor of 36, the linear congruence $\boldsymbol{48x \equiv 36(mod\ 138)}$ has exactly 6 congruence class solutions modulo *n*.

Step 2. Convert the given linear congruence $ax \equiv b\ (mod\ n)$ into linear equation ax = b + nk.

The linear congruence $\boldsymbol{48x \equiv 36(mod\ 138)}$ when converted to linear equation is given as: 48x = 36 + 138k.

Step 3. Reduce the modulus *n* by interchanging *a* and *n* algebraically.

48x = 36 + 138k

48x – 36 = 138k

138k = -36 + 48x

138k = -36 (mod 48)

Step 4. Simplify and solve the new congruence nk =-b (mod a). Perform step 3 and 4 recursively until obtaining a congruence that is trivial to solve.

138k = -36 (mod 48)

42k = 12 (mod 8)

$7k = 2 \pmod 8$
$7k = 2 + 8k_1$
$8k_1 = -2 \pmod 7$
$k_1 = 5 \pmod 7$
$7k = 2 + 8k_1$
$7k = 2 + 8(5)$
$7k = 2 + 40$
$7k = 42$
$q = 6$

Step 5. Substitute the values of a, b, n and k to the equation **x = (b + nk)/a** to solve the given congruence.

x = (b + nk)/a
$x = [36 + 138(6)] / 48$
$x = (36 + 828) / 48$
$x = 864 / 48$
$x = 18$

One congruence class solution of $\boldsymbol{48x \equiv 36 (mod\ 138)}$ is $[18]_{138}$.

If x is a solution, then a complete congruence class solution is:

x, x + n/d, x + 2n/d, . . ., x + (d-1)n/d where d = (a, n).

Therefore, the complete congruence class solutions to $\boldsymbol{48x \equiv 36 (mod\ 138)}$ are $[18]_{138}$, $[41]_{138}$, $[64]_{138}$, $[87]_{138}$, $[110]_{138}$, and $[133]_{138}$.

A shorter version of the solution of $\boldsymbol{48x \equiv 36\ (mod\ 138)}$ is presented below:

(48, 138) = 6	Finding the gcd
6 is a factor of 36	Checking solvability
48x = 36 + 138k	Converting to linear equation
138k = -36 (mod 48)	Interchanging *a* and *n*
42k = 12 (mod 8)	Simplifying the congruence
7k = 2 (mod 8)	
k = 6 (mod 8)	Solving the congruence in terms of k
x = (b + nk)/a	
x = [36 + 138(6)] / 48	Substituting values to the general solution
x = 18	Simplifying the equation
$x = [18]_{138}$	The congruence class solution of
$48x \equiv 36 (mod\ 138)$.	

The complete set of congruence class solutions are: $[18]_{138}$, $[41]_{138}$, $[64]_{138}$, $[87]_{138}$, $[110]_{138}$, and $[133]_{138.}$

CONCLUSIONS

An easier alternative method for solving linear congruence $ax \equiv b \pmod{n}$ considering two cases: (1) when (a,n) = 1 and (2) when (a,n) > 1 was developed. The basic idea of the method is to convert the given congruence $ax \equiv b \pmod{n}$ to $ax = b + kn$ for some k, reduce modulus n by interchanging a and n, simplify the new congruence and perform the process recursively until obtaining a congruence that is trivial to solve. The advantage of this method over the existing approaches is that it can solve congruence even for large modulus n with much more efficiency. Generalized solution of linear congruence $ax \equiv b \pmod{n}$ considering both cases was obtained in this study.

Future researchers can also conduct study on the development of easier alternative methods for solving other types of congruences such as linear congruence ax + by $\equiv$ c (mod n), system of linear congruences, quadratic congruence and other non-linear congruences.

This research was used as a mathematical basis for developing a computer program that automatically solves linear congruence problems in a step by step fashion which is currently being used in teaching and learning the concept of linear congruence in Number Theory classes.

LITERATURE CITED

Adams, D.G. (2010). Distinct solutions of linear congruences. *Acta Arithmetica*, 141(2), 103-152. Retrieved from http://rmrj.usjr.edu.ph/index.php/RMRJ/article/view/13

Ashioba, N. C., & Yoro, R. E. (2014). RSA Cryptosystem using Object-Oriented Modeling Technique. *International Journal of Information and Communication Technology Research*, 4(2), 57–61. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=Ashioba%2C+N.+C.%2C+%26+Yoro%2C+R.+E.+%282014%29.+RSA+Cryptosystem+using+Object-Oriented+Modeling+Technique&btnG=

Benjamin, A. T. & Brown, E. (2009) Biscuits of Number Theory. *The Mathematical Association of America, Inc.* Retrieved from *https://scholar.google.com.ph/*

scholar?hl=en&as_sdt=0%2C5&q=Benjamin%2C+A.+T.+%26+Brown%2C+E.+%282009%29+Biscuits+of+Number+Theory.+&btnG=

Burger, E. B. (2006). Small solutions of linear congruence over number of fields. *Rocky Mountain Journal of Mathematics*, 26(3), 875-888. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=Burger%2C+E.+B.+%282006%29.+Small+solutions+of+linear+congruence+over+number+of+fields.&btnG=

Burton, D. M. (2011). *Elementary Number Theory 7th Edition*. McGraw Hill International Companies Inc. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=+Elementary+Number+Theory+&btnG=#d=gs_cit&p=&u=%2Fscholar%3Fq%3Dinfo%3AV5FxvbCTsa4J%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den

Cuarto, P. (2014). Algebraic algorithm for solving linear congruences: its application to cryptography. *Asia Pacific Journal of Education, Arts and Sciences* 1(1), 34-37. Retrieved from http://oaji.net/articles/2015/1710-1440015925.pdf

Cuarto, P. (2015). Algebraic method for solving system of linear congruences. *Recoletos Multidisciplinary Research Journal* 3(1), 93-100. Retrieved from http://rmrj.usjr.edu.ph/index.php/RMRJ/article/view/13

Gold, J. F., & Tucker, D. H. (1995). *A novel solution of linear congruence*s. In NCUR IX (Vol. 2, pp. 708–712). Retrieved from http://www.sciepub.com/reference/233027

Gupta,D.K., Srivastava, S.K., Singh, V. (2012). New concept of symmetric encryption algorithm a hybrid approach of caesar cipher and columnar transposition in multi stages. *Journal of Global Research in Computer Science,* 3(1), 60–66. Retrieved from http://www.jgrcs.info/index.php/jgrcs/article/view/295

Kaddoura, I. H. (2006). A new formula to find the solutions of the linear diophantine equations. *Lebanese Science Journal*, 7(1), 137–139. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=Kaddoura%2C+I.+H.+%282006%29.+A+new+formula+to+find+the+solutio

ns+of+the+linear+diophantine+equations&btnG=

Ore, O. (1988). *Number Theory and Its History*. Dover Publications, Inc., New York. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=Ore%2C+O.+%281988%29.+Number+Theory+and+Its+History&btnG=

Rose, H. E. (2010). A Course on Number Theory 2nd Ed. *Oxford Science Publications.* Retrieved from *https://www.amazon.com/Course-Number-Theory-Science-Publications/dp/0198523769*

Rosen, K. H. (2011). Elementary Number Theory Sixth Edition. *Pearson Education Inc. Retrieved from https://www.bookdepository.com/Elementary-Number-Theory-Kenneth-H-Rosen/9780321500311*

Roxas, S. & Reyes, F. (2013). On the determination of happy numbers, *University of Batangas Graduate School Journal,* 3(1), 98-116.

Stein, W. (2008). *Elementary number theory: primes, congruences, and secrets: a computational approach*. Springer Science & Business Media. *Retrieved from https://www.google.com/books?hl=en&lr=&id=5hYd0yX4mrMC&oi=fnd&pg=PP9&dq=Stein,+W.+(2009).+Elementary+number+theory:+primes,+congruences+and+secrets&ots=gFwav9HeUZ&sig=a-dGWuEhyQf88WZR3eRqH5zgjttE*

United Nations (2016). *Data protection regulations and international data flows: implications for trade and development*. United Nations Publication: Switzerland.
Retrieved from https://www.tralac.org/images/docs/9500/data-protection-regulations-and-international-data-flows-implications-for-trade-and-development-unctad-april-2016.pdf

Wall, E. (2010*). Elementary number theory* 7th Ed. McGraw Hill International Companies Inc. Retrieved from https://scholar.google.com.ph/scholar?hl=en&as_sdt=0%2C5&q=Wall%2C+E.+%282010%29.+Elementary+number+theory+&btnG=#d=gs_cit&p=&u=%2Fscholar%3Fq%3Dinfo%3Agwx_U2EZYzEJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den