Algebraic Algorithm for Solving Linear Congruences: Its Application To Cryptography

POLEMER M. CUARTO
polemath@yahoo.com
Mindoro State College of Agriculture and Technology
PHILIPPINES

Abstract - *This study is an integration of two different fields: Number Theory and Computer Science. In this paper, an algebraic algorithm as an alternative method for finding solutions to problems on linear congruences was developed. The basic idea of the technique is to convert the given linear congruence into linear equations and solve them algebraically. 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 validity of this method for solving linear congruences. An application of developed algorithm on solving linear congruences to cryptography using RSA cryptosystem was also presented in this paper.*

Keywords: linear congruences, Number Theory, cryptography, Computer Science, RSA

I. INTRODUCTION

The growth of the internet and electronic commerce has brought to the forefront the issue of privacy in electronic communication. Large volumes of personal and sensitive information are electronically transmitted and stored every day. With this, organizations in both the public and commercial sector need to protect this information when it is being transmitted. Cryptography, a field in Computer Science, is the science of making communications unintelligible to all except authorized parties using the process of encryption and decryption. Cryptography secures the information by protecting its confidentiality and can also protect information about the integrity and authenticity of data.

There are two different cryptography systems. One is the private key cryptography system in which the sender and the receiver agree on a secret key that is both used to encrypt decrypt the message. An example of this is the well-known Caesar's cipher, a shift cipher in which $f(p) = (p + k) \bmod 26$. The other cryptography system is called public key cryptosystem in which a public key is used to encrypt the message and a private key is used to decrypt the message. An example of this is the RSA, named after its inventors Rivest, Shamir and Adlemann in 1978. In RSA system, private key consists of two prime numbers p and q while a public key is a number n which is a product of p and q and another number e which is a number relatively prime to $(p-1)(q-1)$.

This process of ciphering and deciphering codes makes use of the concept of linear congruences. Thus, linear congruence plays a very important role in cryptography. Because of this, finding solutions to congruences has received remarkable attention in the past several decades. This problem has been studied intensively by numerous authors. There are several methods to solve congruences, specifically, system of linear congruences. In solving linear congruences, Gold et al (2005) made use of remodulization method as a vehicle to characterize the conditions under which the solutions exist and then determine the solution space. This approach relates the solution space of $cx \equiv a \bmod b$ to the Euler totient function for c which allows to develop an alternative approach to the problem of creating enciphering and deciphering keys in public key cryptosystems. Stein (2009) also presented in one of his books in Number Theory an approach which translate the given congruence into Diophantine equation $ax + by = c$ to solve linear congruences. Koshy (2007) also presented an algorithm making use of multiplicative inverses of a modulo m in solving linear congruences.

Although there are already several approaches developed, finding solutions to congruence still remain pedagogically difficult. This is because the methods make use of complex algorithms. Thus, this paper is an attempt to devise an algorithm for solving linear congruences that does not follow an exhaustive, gradual and incremental method which invites 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 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. Similarly, the result of this study can help those in the field of cryptography because the concept of system of linear congruences 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 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.

In the light of the foregoing perspectives, the researchers felt the need to conduct this study.

ISSN 2362 – 8022 | www.apjeas.apjmr.com

II. OBJECTIVES OF THE STUDY

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 linear congruences; to validate the developed algorithm through illustrative examples; to apply the developed algorithm in cryptography using the RSA cryptosystem.

Preliminaries

In order to effectively understand the concept of linear 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.

1.1 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.

1.2 **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.*

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

1.4 **Reflexive Property**. *If a is an integer then* $a \equiv a \pmod{n}$.

1.5 **Symmetric Property**. *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.

1.6 Transitive Property. *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.

1.7 **Simplification Property**. *If k divides a, b and n, then* $a \equiv b \pmod{n}$ *is congruent to* $a/k \equiv b/k \pmod{n/k}$.

1.8 **Cancellation Property**. *If gcd(k, n) = 1, then* $ak \equiv bk \pmod{n}$ *is congruent to* $a \equiv b \pmod{n}$.

1.9 **Addition Property**. *If* $a \equiv b \pmod{n}$, *then* $a + k \equiv b + k \pmod{n}$.

1.10 **Subtraction Property**. *If* $a \equiv b \pmod{n}$, *then* $a - k \equiv b - k \pmod{n}$

1.11 **Multiplication Property**. *If* $a \equiv b \pmod{n}$, *then* $ak \equiv bk \pmod{n}$.

III. MATERIALS AND METHODS

The study is a development of an algebraic algorithm for solving linear congruence. It is an developmental research in pure mathematics. The method goes through a series of trials and computations before arriving at the algorithm. The developed algorithm was subjected to validation by providing illustrative examples. An application of the developed algorithm in cryptography using the RSA system was also presented.

For a better understanding of the study, related concepts have been discussed in the preliminaries. These concepts are definition, theorems and properties related to linear congruences and system of linear congruences.

Several articles and related studies from general references, books, journals and internet sources have been reviewed and cited to establish a systematic and mathematical analysis of the topic. The presentation of every topic is systematic and illustrative in order for the students and general readers 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.

IV. RESULTS AND DISCUSSIONS

The subsequent sections provide discussion and illustrative examples of the proposed algebraic algorithm for solving linear congruences and an application of the algorithm in cryptography using the RSA system.

Algebraic Algorithm for Solving Linear Congruences

Linear congruences in the form $ax \equiv b \pmod{n}$ 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 any integer. From this, the idea of solving linear congruences algebraically emanated. The basic idea of the method is to express the given linear congruence to equation and solve it algebraically.

The algorithm for solving linear congruences is presented below.

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

Step2. Convert the given linear congruence into linear equation in terms of the unknown variable.

Step 3. Find the smallest positive integer solutions to the linear equation that will make the unknown variable a whole number.

Step 4. Evaluate the linear equation using the integer solution. The result will be the smallest positive integer that is a solution to the given linear congruence. The general solution is given by the congruence $x \equiv b \pmod{n}$ where b is the smallest positive integer solution and n is the given modulus.

To show the validity of this algorithm, an illustrative example is provided in this section.

Illustrative Example

Solve the linear congruence $16x \equiv 22 \pmod{26}$.

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 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.*

ISSN 2362 – 8022 | www.apjeas.apjmr.com

Since the greatest common divisor of 16 and 22 is 2 which is a factor of 26, the linear congruence ***16x ≡ 22(mod 26)*** has solutions.

Step 2. Convert the given linear congruence into linear equation in terms of the unknown variable.

The linear congruence ***16x ≡ 22(mod 26)*** when converted to linear equation in

is 16x = 22 + 26q. In terms of x, it will become $x = \frac{22+26q}{16}$ or in a more simplified form $x = \frac{11+13q}{8}$.

Step 3. Find the smallest positive integer solutions to the linear equation that will make the unknown variable a whole number.

Given $x = \frac{11+13q}{8}$, the smallest positive integer value of *q* that will make *x* a whole number is 1.

Step 4. Evaluate the linear equation using the integer solution. The result will be the smallest positive integer that is a solution to the given linear congruence. The general solution is given by the congruence $x \equiv b \ (mod\ n)$ where b is the smallest positive integer solution and *n* is the given modulus.

If q = 1, then evaluating $x = \frac{11+13q}{8}$ will be :

$$x = \frac{11+13(1)}{8}$$
$$x = \frac{11+13}{8}$$
$$x = \frac{24}{8}$$
$$x = 3$$

Thus, the solution to linear congruence ***16x ≡ 22(mod 26)*** is **3(mod 26).**

Application of the Developed Algebraic Algorithm for Solving Linear Congruences in Cryptography using the RSA System

In this section, the developed algorithm on linear congruence will be applied in some parts in the decryption and encryption of the message using the RSA system.

RSA (Rivest Shamir Adleman) system is a private key cryptosystem using prime numbers *p* and *q* as the private key and number *n* (product of *p* and *q*) and number *e* (number relatively prime to (p-1)(q-1)) as well as the ciphertext $C = M^e \ (mod\ n)$. This cryptosystem is used in this study for the following reasons:

1. The encryption function used in RSA is a trapdoor function. Trapdoor function is easy to compute in one direction but very difficult in reverse direction without additional knowledge.
2. Encryption direction is very easy because it only requires exponentiation and modulo operations.
3. Decryption without the private key is very hard because it requires prime factorization which adds to the security of the RSA.

Using an encryption (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n -1). Large numbers can be broken up into number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the e^{th} power modulo n. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power modulo n.

Illustrative Example

A. Encryption of Message

Encrypt the message "PASSWORD" using RSA with n = 85 and e = 3.

1. Represent the message as an integer. P=16 A=01 S=19 S=19 W=23 O=15 R=18 D=04
2. Group sequence into block of two digits. M = 16 01 19 19 23 15 18 04
3. Encrypt each block as $C = M^3 \ (mod\ 85)$

For the first block $16^3 \ (mod\ 85) = 16$; for the second block $01^3 \ (mod\ 91) = 01$; for the third block $19^3 \ (mod\ 91) = 59$; for the fourth block $19^3 \ (mod\ 91) = 59$; for the fifth block $23^3 \ (mod\ 85) = 12$; for the sixth block $15^3 \ (mod\ 91) = 60$; for the seventh block $18^3 \ (mod\ 91) = 52$; for the eight block $04^3 \ (mod\ 91) = 64$;

Ciphertext : 1601595912605264

B. Decryption of Message

Decrypt the ciphertext 1601595912605264 for the RSA cipher using p = 5, q = 17 and e = 3.

1. Compute d, the inverse of e modulo (p-1)(q-1). (p-1)(q-1) = 4 (16) = 64. Thus, we will have $3d \equiv 1 (mod\ 64)$
2. Use the algebraic algorithm to solve the linear congruence $3d \equiv 1 (mod\ 64)$

$3d = 1 + 64q \quad d = (1 + 64q)/3$

1 is the smallest integer q that will make number d whole number. Thus, by substituting

q = 2, d will be equal to 43.

3. To decrypt the ciphertext message, raise it to d modulo n.

$16^{43} \ mod\ 85 = 16$; $01^{43} \ mod\ 85 = 01$; $59^{43} \ mod\ 85 = 19$; $59^{43} \ mod\ 85 = 19$;

$12^{43} \ mod\ 85 = 23$; $60^{43} \ mod\ 85 = 15$; $52^{43} \ mod\ 85 = 18$; $64^{43} \ mod\ 85 = 04$

Decrypted message : 1601191923151804

Thus the message is PASSWORD.

CONCLUSIONS AND DIRECTIONS FOR FUTURE USE

Aside from the known methods and techniques of solving linear congruences and, the algebraic algorithm provides another way of finding solutions to congruences. With the simplicity of the computational process of the algebraic algorithm, those who are just starting to learn linear congruences may found this method more preferable than those already published in books and journal.

With the key role of congruences in cryptography, this algorithm provides a great contribution in computer science, specifically in computer security as this paves way to an easier

ISSN 2362 – 8022 | www.apjeas.apjmr.com

way to encrypt and decrypt codes used in RSA cryptosystem. Likewise, this algorithm can be used as basis for developing a computer program that can solve linear congruences with much more efficiency. Moreover, application of the developed algorithm in the classroom level specifically in Number Theory classes is highly recommended in order to facilitate the teaching and learning of the concept of linear congruence more effectively.

REFERENCES

Adams, D.G.(2010). *Distinct Solutions of Linear Congruences.* Acta Arithmetica Vol. 141 No. 2. pp. 103-152

Burger, E. B. (2006). *Small Solutions of Linear Congruence over Number of Fields.* Rocky Mountain Journal of Mathematics Vol. 26 No. 3.pp 875-888

Frieze, A. et al. (2006). *Reconstructing Truncated Integer Variables Satisfying Linear Congruences.* SIAM Journal on Computing. Vol. 17 No. 2. pp 262-280

Koshy, T. (2007). Elementary Number Theory with Applications. 2nd Ed. Elsevier Publishing Inc. pp. 211-245

Lindahl, L. A. (2003). Number Theory. Retrieved from http://www2.math.uu.se/~ lal/kompendier/Talteori.pdf. Accessed on August 14, 2013

Stein, W. (2009). Elementary Number Theory : Primes, Congruences and Secrets. 1st Ed. Springer Publication. pp 21-44

Sburlati, G. (2003). *Counting the Number of Solutions of Linear Congruences.* Rocky Mountain Journal of Mathematics Vol. 33 No. 4.pp 1487-1497

ISSN 2362 – 8022 | www.apjeas.apjmr.com