Algebraic Method For Solving System Of Linear Congruences

Polemer M. Cuarto

Published and reprinted with permission from the
Asia Pacific Journal of Education Arts and Sciences
(APJEAS) pp.34-37
Vol. 1 Num. 1P-ISSN 2350-7756
and E-ISSN 2350-8442
Lyceum of the Philippines, Batangas City

Abstract

The paper aimed to devise an alternative algorithm for solving system of linear congruences. This algorithm is an extension of the algebraic algorithm which is an alternative method for finding solutions in linear congruences. The basic idea of the technique is to convert the given linear congruences into linear equations and solve them algebraically. The advantage of this algorithm is the simplicity of its computations and its applicability to systems of linear congruences where the conditions of the Chinese Remainder Theorem that the moduli m1…mn should be pairwise coprime is not satisfied. Some illustrative examples are given to show validity of this method for solving system of linear congruences.

Keywords: Algebraic algorithm, system of linear congruences, Number Theory, Chinese Remainder Theorem, crypthography

1.0 Introduction

With the increasing quantity of digital information being stored and communicated via telephone lines, microwaves or satellites, organizations in both the public and commercial sector need to protect their transmitted information. Cryptography is the science of making communications unintelligible to all except authorized parties using the process of encryption and decryption. This process of ciphering and deciphering codes makes use of the concept of linear congruences. Thus, linear congruences and system of linear congruences play a very important role in cryptography.

Because of its great use in public key cryptosystems, 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.

In similar vein, several authors made various studies on the different aspects of congruences. Schanuel (2005) studied problems equivalent to one on simultaneous linear congruences to which one seeks solutions with the variables restricted to the values 0 and 1. The main tool is an extension of Chevalley's theorem on finite fields to congruences modulo prime powers. On the other hand, Sburlati (2003) analyzed some known formulas which concern counting the number of solutions of linear congruences and we find two important related numerical values which give an answer to interesting questions in Elementary Number Theory related to distributions of sums modulo in an integer.

In addition to this, several authors also devised algorithms in solving system of linear congruences. Most notably among these methods is the Chinese Remainder Theorem (CRT) which was discovered by ancient Chinese mathematician and was first written down in the Shushu Jiuzhang (Nine Chapters in the Mathematical Art) by Qin Jiushao in the thirteenth century. CRT is used when mi are pairwise relatively prime producing a unique solution modulo

The product of $m = m_1 m_2 \ldots m_n$. Alternatively, Piedra et al (2007) proposed a parallel congruence algorithm which makes use of Gaussian Elimination algorithm and mixed-radix conversion to solve system of linear congruences.

Although there are already several approaches developed, finding solutions to congruence still remain pedagogically difficult. There are situations in which these methods are inadequate or far less general which cannot solve all forms of congruences as in the case of Qin Jiushao's CRT which only applies if the moduli $m_1..m_n$ have GCD equal to one or are relatively prime. Moreover, some methods are general but makes use of complex algorithms.

This paper is an attempt to devise an algorithm for solving system of linear congruences that is applicable to all linear congruences and 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.

1.1 Objectives of the Study

The study aims to develop an algebraic

algorithm for solving system of linear congruences. Specifically, the study seeks to:

1. devise an extension of the algebraic algorithm to solve system of linear congruences; and
2. validate the developed algorithms through illustrative examples

1.2 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.

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.

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* $ak \equiv bk \pmod n$.

2.0 Methodology

The study is a development of an algebraic algorithm for solving system of linear congruences. 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.

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 study, experts in the field and colleagues in the academe were consulted to be able to present the topic more clearly.

3.0 Results and Discussions

The subsequent sections provide discussion and illustrative examples of the proposed algebraic algorithm for solving linear congruences and system of linear congruences.

3.1 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.

Step 2. 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 1

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.

Since the greatest common divisor of 16 and 22 is 2 which is a factor of 26, the linear congruence ***$16x \equiv 22 \pmod{26}$*** has solutions.

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

The linear congruence ***$16x \equiv 22 \pmod{26}$*** 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 va$x = \frac{11 + 13q}{8}$umber.

Given , 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).**

3.2 Algebraic Algorithm for Solving System of Linear Congruences

The algebraic algorithm for solving linear congruences is extended to another algorithm that makes use of similar technique to solve system of linear congruences. Aside from the simplicity of the computations, this algorithm is applicable for finding solutions to system of linear congruences where the conditions of the Chinese Remainder Theorem is not satisfied.

The extension of the algebraic algorithm is presented below.

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

Step 2. Convert the given linear congruences into linear equations using different variables (e.g. a and b)

Step 3. Combine equation 1 and equation 2 to form a single equation.

Step 4. Find an integer solution to the equation algebraically.

Step 5. Substitute the values of the variables to any of the equation. Name it k.

Step 6. Find the least common multiple of the given moduli. Name it n.

Step 7. Plug in the values of k and n to the congruence $x \equiv k \ (mod\ n)$ to get the general solutions of the system of linear congruences.

To show the validity of this algorithm, illustrative examples are provided in this section.

Illustrative Example 2

Case 1. When the moduli of the given system of linear congruences is pairwise coprime

Solve the system of linear congruences given below.

x ≡ 3 (mod 7) **x ≡ 5 (mod 8)**

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

x ≡ 3 (mod 7)

x ≡ 5 (mod 8)

Both the two given linear congruences is solvable since in the first congruence (1,7) =1, which a factor of 3 while in the second congruence (1, 8) = 1, which is a factor of 5.

Step 2. Convert the given linear congruences into linear equations using different variables (e.g. a and b)

x ≡ 3 (mod 7) x = 3 + 7a

x ≡ 5 (mod 8) x = 5 + 8b

Step 3. Combine equation 1 and equation 2 to form a single equation.

Since both the right sides of the equation is equal to *x*, by Transitive Property of Equality, 3 + 7a = 5 + 8b. Simplifying further, it will become 7a = 2 + 8b. Expressing in terms of a, the equation will be $a = \frac{2 + 8b}{7}$.

Step 4. Find an integer solution to the equation algebraically.

An integer solution to $a = \frac{2 + 8b}{7}$ is b = 5 and a = 6.

Step 5. Substitute the values of the variables to

any of the equation. Name it k.

x = 3 + 7a	x = 5 + 8b
x = 3 + 7(6)	x = 5 + 8(5)
x = 3 + 4	x = 5 + 40
x = 45	x = 45

Therefore, k = 45.

Step 6. Find the least common multiple of the given moduli. Name it n.

The least common multiple of the given moduli 7 and 8 is equal to 56. Therefore, n= 56.

Step 7. Plug in the values of k and n to the congruence $x \equiv k \ (mod\ n)$ to get the general solutions of the system of linear congruences.

Therefore, the solution to the system of linear congruences **x ≡ 3 (mod 7)** and **x ≡ 5 (mod 8)** is x ≡ 45 (mod 56).

Illustrative Example 3

Case 2. When the moduli of the given system of linear congruences is not pairwise coprime

Solve the system of linear congruences given below.

x ≡ 4 (mod 10)

x ≡ 6 (mod 12)

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

x ≡ 4 (mod 10)

x ≡ 6 (mod 12)

Both the two given linear congruences are solvable since in the first congruence (1,10) =1, which is a factor of 4 while in the second congruence (1, 12) = 1, which is a factor of 6.

Step 2. Convert the given linear congruences into linear equations using different variables (e.g. a and b)

x ≡ 4 (mod 10)	x = 4 + 10a
x ≡ 6 (mod 12)	x = 6 + 12b

Step 3. Combine equation 1 and equation 2 to form a single equation.

Since both the right sides of the equation is equal to *x*, by Transitive Property of Equality, 4 + 10a = 6 + 12b. Simplifying further, it will become 10a = 2 + 12b. Expressing in terms of a, the equation will be $a = \frac{2 + 12b}{10}$.

Step 4. Find an integer solution to the equation algebraically.

An integer solution to $a = \frac{2 + 12b}{10}$ is b = 4 and a = 5.

Step 5. Substitute the values of the variables to any of the equation. Name it k.

x = 4 + 10a	x = 6 + 12b
x = 4 + 10(5)	x = 6 + 12(4)
x = 4 + 50	x = 6 + 48
x = 54	x = 54

Therefore, k = 54.

Step 6. Find the least common multiple of the given moduli. Name it n.

The least common multiple of the given moduli 10 and 12 is equal to 60. Therefore, n= 60.

Step 7. Plug in the values of k and n to the congruence $x \equiv k \ (mod\ n)$ to get the general solutions of the system of linear congruences.

Therefore, the solution to the system of linear congruences **x ≡ 4 (mod 10)** and **x ≡ 6 (mod 12)** is x ≡ 54 (mod 60).

4.0 Conclusions and directions for future use

Aside from the known methods and techniques of solving linear congruences and system of linear congruences, the algebraic algorithm provides another way of finding solutions to congruences. Its applicability is far more general than the Chinese Remainder Theorem since this algorithm can solve system of linear congruences whether the given

moduli are pairwise relatively prime or not. 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 public key cryptosystem, this algorithm provides a great contribution in computer science, specifically, in the field of cryptography as this pave way to an easier way to encrypt and decrypt codes used in public key cryptosystem. Furthermore, this algorithm can be used as basis for developing a computer program that can solve linear congruences and system of linear congruences with much more efficiency.

5.0 References

Adams, D.G.(2010). *Distinct Solutions of Linear Congruences*. Acta Arithmetica Vol. 141 (2), 103-152

Burger, E. B. (2006). *Small Solutions of Linear Congruence over Number of Fields*. Rocky Mountain Journal of Mathematics Vol. 26 (3), 875-888

Congruences [Online]. (2013). Natick, MA : MathWorks. Retrieved http://www.mathworks.com/help/symbolic/ mupad.ug/congruences.html.

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

Gold, J.F., Tucker, D. H. (1995). *A novel solution of linear congruences*. Salt Lake City, UT.

Koshy, T. (2007). *Elementary Number Theory with Applications*. (2nd Ed.) Cambridege, MA : Academic Press.

Lindahl, L. A. (2002). Lectures on Number Theory [Online]. Sweden : Uppsala University Retrieved http://www2.math.uu.se/~astrombe/talteori2016/lindahl2002.pdf

Linear Congruences [Online]. (2013). Retrieved from http://www.math.cornell.edu/~csheridan//Math1350Schedule_files/LinearCongruences.pdf.

Linear Congruences [Online]. (2013). Dekalb, IL: Northern Illinois University. Retrived http://www.math.niu.edu/~richard/Math420/lin_cong.pdf.

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

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

System of Linear Congruences 2013. Ohio : Xavier University Computer Science. Retrieved from http://www.cs.xu.edu/math / math302/08f/06_CRT.pdf.

Weisstein, E. W. (2013). *Linear congruence equation*. [Online] Retrieved http://mathworld.wolfram.com LinearCongruenceEquation.html.