American Journal of Educational Research, 2018, Vol. 6, No. 2, 149-151
Available online at http://pubs.sciepub.com/education/6/2/10
©Science and Education Publishing
DOI:10.12691/education-6-2-10

Linear Congruence $ax \equiv b \pmod{n}$ Solver

Polemer M. Cuarto*

Mindoro State College of Agriculture and Technology – Calapan City Campus, Masipit, Calapan City, Oriental Mindoro, Philippines
*Corresponding author: polemath@yahoo.com

Abstract Although there are existing methods for solving linear congruence ax ≡ b (mod n), finding solutions still remain difficult especially when the modulus n is large. Thus, this paper aimed to develop a linear congruence solver that will provide step by step solutions even for large modulus n. The linear congruence solver was based on alternative numerical method devised by the researcher and was developed using Microsoft Visual Studio C# programming language. The system was tested using ISO 9126 standard questionnaire for software quality characteristics such as functionality, reliability, and usability. The result of the evaluation shows that the developed linear congruence solver is highly functional, highly reliable and highly usable. The use of linear congruence solver as an instructional aid for instructors and students is highly recommended.

Keywords: *mathematics, number theory, linear congruence ax ≡ b (mod n), developmental research method, ISO 9126 software quality characteristics*

Cite This Article: Polemer M. Cuarto, "Linear Congruence *ax* ≡ *b* (mod n) Solver." *American Journal of Educational Research*, vol. 6, no. 2 (2018): 149-151. doi: 10.12691/education-6-2-10.

1. Introduction

In today's modern age, information security is a major challenge in the field of internet and network application. With the development and advancement of the internet and electronic commerce, large volumes of personal and sensitive information are being electronically transferred and stored everyday. Thus, the security and privacy in electronic communication and the need to protect these information when they are being transmitted become an important issue to consider. Using the process of encryption and decryption, cryptography makes communications indecipherable to all except authorized parties [1]. Cryptography is widely used tool which secures the information by protecting its confidentiality as well as the integrity and authenticity of data from the attack of intruders [2,3]. With cryptography, electronic data transmitted in correspondence, online shopping, financial transactions such as online banking or even in social media account passwords are secured from unauthorized users in data communication [4].

There are two broad categories of cryptography systems. One is a symmetric-key systems that use a single key used by both sender and recipient, and the other is public-key systems that uses a public key which can be widely known and a private key which is being used only by the receiver of messages [5]. An example of the symmetric-key system is Caesar's cipher, a shift cipher in which f(p) = (p + k) mod 26 [6]. RSA®, named after its inventors Rivest, Shamir and Adlemann in 1978 is an example of public key cryptosystem. 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) [7].

Linear congruence play 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 [6,7].

Because of this, numerous researchers and mathematics educators have been interested in studying and developing methods for solving linear congruence ax ≡ b (mod n). A standard method of solving linear congruence involves the use of multiplicative inverse of *a* modulo *n*. Another is an approach which translates the given congruence into Diophantine equation ax + by = c to solve linear congruence and solved using Extended Euclidean Algorithm [8,9]. Remodulization method, a novel solution for linear congruence which characterizes the conditions under which solutions exists and then determines the solution space [10]. 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 [11,12].

Although there are existing approaches developed, finding solutions to congruence still remain difficult especially on the part of the students. This is because the methods make use of complex algorithms. Many computer programmers have also developed linear congruence calculators that provides congruence class solutions but failed to show the step by step procedures for solving such problems. Thus, this paper aimed to devise a computer program that solves ax ≡ b (mod n) in a step by step fashion based on an alternative method that solves complex linear congruence problems.

2. Objectives of the Study

This study aims to develop a linear congruence solver using C# programming language and evaluate the developed system using the ISO 9126 standard questionnaire for software quality characteristics such as functionality, reliability, and usability.

3. Methodology

3.1. Project Development

C# (C Sharp) is an object-oriented programming (OOP) language from Microsoft that combines the computing power of C++ and the programming ease of the Visual Basic. C# provides an advanced code editor, convenient user interface designers, integrated debugger, and many other tools to make it easier to develop applications based on the C# language and the .NET Framework. With these features, C# was chosen as the programming language in developing linear congruence $ax \equiv b \pmod{n}$ solver. The system was coded and constantly improved using various types of testing methods to completely attain the desired goals.

3.2. User Interface

User interface include graphical user interface (GUI) which is a human-computer interface that uses windows, icons and menus which can be manipulated by a mouse. It is the most important part of an application and it is certainly the most visible. To the user, the interface is the application they probably are not aware of the code that is executed behind the scene.

The interface of the developed linear congruence solver contains three textboxes for inputting the value of a, b and n. It has three buttons: print, solve and clear buttons. Solve button is used for solving the given linear congruence $ax \equiv b \pmod{n}$ inputted in the textboxes. Once the solve button is clicked, a step-by-step solution will appear if the given congruence is solvable. If it is not solvable, a label will appear that it has no solution and the reason why it is not solvable. A warning will also appear if the solve button is clicked without the complete values for a, b and n. The print button is used to preview and print the solutions of the given congruence. On the other hand, the clear button is used to delete previous data.

3.3. Operation and Testing

After the development, a test case was conducted. The researcher presented the system to a panel for preliminary evaluation. Some computational errors were found out during the technical presentation. Series of trials and improvement were done to correct the errors and improve the functionality of the system.

3.4. System Evaluation

The linear congruence solver was evaluated using the ISO 9126 standard questionnaire [13] in terms of functionality, reliability and usability. The evaluators were 5 IT experts, 10 Mathematics faculty and 25 Mathematics students. Five-point Likert scale was used to evaluate the system: 4.50-5.00 – Very Effective; 3.50-4.49 – Effective; 2.50-3.49 – Moderately Effective; 1.50-2.49 – Slightly Ineffective and 1.00-1.49 – Ineffective. Result of the evaluation was tabulated and treated statistically using SPSS software.

4. Results and Discussion

4.1. Evaluation of the Linear Congruence Solver

To test the effectiveness of the solver, an evaluation of its functionality, reliability and usability was conducted. This was evaluated by a panel of IT experts, Mathematics faculty and students.

4.2. Functionality

Table 1 presents the results of the evaluation of the functionality of the system. As shown, the system was rated “very effective” by the IT experts (5.00), Mathematics faculty (5.00) and Mathematics students (5.00).

This implies that the system functions according to its specified purpose and produces accurate solutions to the linear congruence problems being encoded in the system. The evaluators believes that the system is very functional and can serve its purpose as a supplemental instructional material in teaching linear congruences.

4.3. Reliability

Table 2 shows the results of the evaluation of the reliability of the system. As presented in the table, the linear congruence solver was rated “effective” by the IT experts (4.30), Mathematics faculty (4.33) and Mathematics students (4.27).

This implies that the system has the ability to maintain the service and can manage and recover from factors that may affect its failure. Although the system can be operational even in the event of minor system, further improvement on the system may be considered to solve the problems encountered and provide reliable and efficient results.

Table 1. Level of Functionality of the Solver

Items	IT Experts		Math Faculty		Math Students	
	WM	VI	WM	VI	WM	VI
1. The system functions appropriately.	5.00	VE	5.00	VE	5.00	VE
2. The system produces accurate results and functions without errors or problems	5.00	VE	5.00	VE	5.00	VE
Overall Mean	5.00	VE	5.00	VE	5.00	VE

Table 2. Level of Reliability of the Solver

Items	IT Experts		Math Faculty		Math Students	
	WM	VI	WM	VI	WM	VI
1. The system functions for a long time without crashes or service interruptions.	4.40	E	4.20	E	4.30	E
2. The software can manage and/or recover from component or environmental failure.	4.00	E	4.20	E	4.00	E
3. The system can be revived and become fully operational even in the event of failure.	4.50	VE	4.60	VE	4.50	VE
Overall Mean	4.30	E	4.33	E	4.27	E

Table 3. Level of Usability of the Solver

Items	IT Experts		Math Faculty		Math Students	
	WM	VI	WM	VI	WM	VI
1. The function of the system is easily understood.	5.00	VE	5.00	VE	5.00	VE
2. The system is user-friendly.	4.80	VE	5.00	VE	4.80	VE
3. The system is easy to operate	4.80	VE	5.00	VE	4.80	VE
Overall Mean	4.87	VE	5.00	VE	4.87	VE

4.4. Usability

As shown in Table 3, in terms of usability, the system was rated by IT experts (4.87) as very effective, by Mathematics faculty (5.00) as very effective and by Mathematics students (4.80) as very effective. This means that the system is user-friendly, easy to operate and does not require learning effort for different type of users.

5. Conclusions and Recommendations

A linear congruence solver of ax ≡ b (mod n) showing step-by-step solutions was successfully developed using the C# programming language. The system met its objective of providing accurate and reliable congruence classes solutions for linear congruence problems. The overall results of the evaluation of the system passed software quality characteristics of functionality, reliability and usability. It is highly recommended that the linear congruence solver be integrated in teaching Number Theory as a supplemental instructional material.

References

[1] Krithika, K. (2014). A review on asymmetric cryptography – RSA and Elgamal algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 5(2), 98-105.

[2] Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, 2(2), 17-32.

[3] Sheth, R. K. (2015). Analysis of cryptography techniques. *International Journal of Research in Advanced Engineering*, 1(2), 1-6.

[4] Goyal, S. (2012). A survey on the applications of cryptography. *International Journal of Science and Technology*, 1(3), 137-140.

[5] Arya, P. K., Aswal, M. S., & Kumar, V. (2015). Comparative study of asymmetric key cryptographic algorithms. *International Journal of Computer Science & Communication Networks*, 5(1), 17-21.

[6] 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.

[7] 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.

[8] Ore, O. (1988). *Number Theory and Its History*. Dover Publications, Inc., New York.

[9] Burton, D. M. (2011). *Elementary Number Theory Seventh Edition*. McGraw Hill International Companies Inc.

[10] Gold, J. F., & Tucker, D. H. (1995). A novel solution of linear congruences. In NCUR IX (Vol. 2), pp. 708-712.

[11] 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.

[12] Cuarto, P. (2015). Algebraic method for solving system of linear congruences. *Recoletos Multidisciplinary Research Journal*, 3(1), 93-100.

[13] ISO 9126 Software Quality Characteristics. Retrieved from http://www.sqa.net/iso9126.html.