International Research Journal of
SCIENCE, TECHNOLOGY, EDUCATION, AND MANAGEMENT
P-ISSN: 2799-063X | E-ISSN: 2799-0648
ISO 9001:2015 Certified
Volume 3, No. 2 | June 2023

Some applications of linear congruence from number theory

Senad Orhani[1], Besim Çeko[2]
[1]*Faculty of Education, University of Prishtina "Hasan Prishtina", Prishtina, Kosovo*
[2]*Lower Secondary School, "Zef Lush Marku", Prizren, Kosovo*
senad.orhani@uni-pr.edu

ABSTRACT

In this research, two distinct areas of number theory and its use in computer science are combined. In this article, an investigation was conducted on the implementation of solutions to linear congruence problems. Linear congruence is a concept implying that two integers a and b are congruent modulo m (denoted as $ab\ (mod\ \equiv m)$), if the difference between them is exactly proportional to m. The study is important in the field of number theory and computer science which brings many benefits and efficient solutions to various problems. Therefore, the study investigates the application of linear congruence through illustrative examples, to apply number theory in finding the ISBN number, in converting decimal numbers to binary, octal, and hexadecimal, and its application in encoding and decoding messages from the field of cryptography. This section of the paper can make it easier for mathematicians to apply problems involving linear congruences, especially for those who need basic expertise in number theory. The findings of the study show that the compatibility of the book ISBN format can be checked through linear congruence. Additionally, these findings demonstrate your understanding of how to convert decimal values to binary, octal, and hexadecimal using linear congruence in a fairly comprehensive manner. Additionally, because the idea of a linear congruence system is employed in the encoding and decoding of codes for network security and other purposes, the findings of this study may be helpful to researchers working in the field of cryptography.

ARTICLE INFO

Received : May 19, 2023
Revised : May 22, 2023
Accepted : June 30, 2023

KEYWORDS

Computer science, Cryptography, ISBN, Linear congruence, Math, Number theory

Suggested Citation (APA Style 7th Edition):

Orhani, S. & Çeko, B. (2023). Some applications of linear congruence from number theory. *International Research Journal of Science, Technology, Education, and Management,* 3(2), 1-11. https://doi.org/10.5281/zenodo.8141702

INTRODUCTION

In abstract algebra, an equivalence relation on an algebraic structure (such as a set, ring, or vector space) is called a linear congruence relation (or simply congruence). This relation is consistent with the structure in the sense that algebraic operations carried out on equivalent elements will result in equivalent elements. There is a matching coefficient structure for each linear congruence relation, and its components are the relation's equivalence classes (or congruence classes). (Hungerford, 1974). A linear congruence is an equivalence relation on an algebraic object that is consistent with the algebraic structure, meaning that the operations are clearly described in the equivalence classes (Barendregt, 1990).

A linear congruence is an equivalence relation between two integers a and b, with respect to a given positive integer m. A is said to be congruent to b modulo m, denoted as a ≡ b (mod m), if the difference between them is exactly proportional to m, or equivalently, they have the same remainder of division by m (Rosen, 2008; Niven, Zuckerman, & Montgomery, 2019; Burton, 2011).

Linear congruence is an important concept in the field of number theory and discrete mathematics that has found wide applications in computer science. This concept involves a special relationship between two integers based on a certain modulus. The applications of linear congruence are numerous and extensive in the field of computer science. In cryptography, for example, linear congruence is used to create security algorithms, helping to develop security and cryptography protocols. Also, linear congruence plays an important role in generating random numbers, which are essential for computer simulations, statistical tests, and security protocols. In addition, linear congruence is also found in many aspects of discrete mathematics and number theory. It is used for solving systems of linear congruences of many variables, as well as in the analysis of mathematical structures and social networks. The understanding and application of linear congruence has brought great contributions to the field of mathematics, number theory and computer science. By paying attention to this concept, we can develop deep knowledge and benefit from efficient solutions to complex problems in these areas. However, this study focuses only on the application of linear congruence in finding the ISBN number, in the conversion of decimal numbers to binary, octal and hexadecimal, its application in encoding and decoding messages from the field of cryptography.

Therefore, knowledge of the following definitions, theorems, and properties that will be employed later in the development of this subject is required in order to comprehend the idea of linear congruences.

Definition: Linear congruence or congruence of the first degree is called any congruence of the form:

$$ax \equiv b\ (mod\ m), \qquad \text{where} \qquad m \in N\ (m > 1) \quad and \quad a, b\ \in Z$$

The whole number x_0 proves or satisfies the linear congruence if:

$$ax_0 \equiv b\ (mod\ m)$$

For each $y \in Z$ we $ay \not\equiv b\ (mod\ m)$ say that the linear congruence has no solution.

Corollary: If $PMMP(a, m) = 1$ then the linear congruence $ax \equiv b\ (mod\ m)$ has only one solution.

Summary: Linear congruence $ax \equiv b\ mod\ m$ has a solution if and only if $PMMP(a, m)$ it divides b. How can we find these solutions?

Case 1: $g = (a, m) = 1$. Then the inversion $a\ mod\ m$ to get $x \equiv a^{-1}b\ mod\ m$. Using the algorithm we find $ax_0 + my_0 = 1$ with the Euclidean Algorithm, we have $ax_0 \equiv 1\ mod\ m$ where $x_0 = a^{-1}$, so $x \equiv x_0 b = a^{-1}b$ that solves the congruence $(ax \equiv a\ (x_0 b) \equiv (ax_0)\ b \equiv b\ mod\ m)$ (Bourke & Choueiry, 2006).

Conclusion: This is a single solution for $mod\ m$.

Case 2: $g = (a,m) > 1$. If $g \nmid b$, we have no choice. If $g \mid b$, we write $a = a'g,\ b = b'g,\ m = mg$ so that $ax \equiv b\ mod\ m \Rightarrow a'x = b'\ mod\ m'$ so that (a', m') now is 1. The only solution (found by Case 1) $x\ mod\ m'$ is completed by $ax \equiv b\ mod\ m$ so that we have a solution $mod\ m$. We know that every solution $\tilde{x}\ mod\ m$ must be congruent to $x\ mod\ m'$, so $\tilde{x}$ it must have the form $x + m'k$ for some values of k. Where k is from 0 to where $g - 1$ takes the value from $G\ mod\ m$: $x, x + m',\ x + 2m' \ldots x + (g-1)\ m'$ which g is fulfilled $a\tilde{x} \equiv b\ mod\ m$, because

$$\begin{aligned} a(x + km') &= ax + akm' \\ &= ax + a'g\ km' \\ &= ax + m\ (a'k) \\ &\equiv ax\ (mod\ m) \\ &\equiv b\ (mod\ m) \end{aligned}$$

Conclusion: This congruence is $g = (a,m)$ solution $mod\ m$ (Robert & Page, 2003).

Congruence System of Different Modulus Congruence

Given

$$\begin{aligned} x &\equiv a1\ (mod\ m_1) \\ x &\equiv a2\ (mod\ m_2) \\ &\vdots \\ x &\equiv ak\ (mod\ m_k) \end{aligned}$$

Theorem (Chinese Remainder Theorem). If the modules are in pairs (e.g.,$(\mathrm{m_i}, \mathrm{m_j}) = 1$ for i $\neq$ j), then the system has a unique solution $mod\ m_1, m_2 \ldots m_k$ (Conrad, 2004).

The only proof. We assume that there are two solutions $x \equiv y \equiv a_1\ mod\ m_1,\ x \equiv y \equiv a_2\ mod\ m_2$, etc. Then $m_1 \mid (x - y), m_2 \mid (x - y)$, etc. Where m is relatively simple in pairs, where their product $m_1 m_2 \ldots m_k$ is fully divisible by $x - y$, as well as $x \equiv y\ mod\ m_1 m_2 \ldots m_k$. So, the solution, if it exists, must be the only one $mod\ m_1 m_2 \ldots m_k$ ■

Proof of existence. We write the solution as a linear combination of a_i

$$A_1 a_1 + A_2 a_2 + \cdots + A_k a_k$$

After we have arranged it so that $mod\ a_i$ of all A_j for $j \neq i$ is $\equiv 0\ mod\ m$, and $A_i \equiv 1\ mod\ m_i$. Let it be

$$\begin{aligned} N_1 &= m_2 m_3 \ldots m_k \\ N_2 &= m_1 m_3 \ldots m_k \\ &\vdots \\ N_i &= m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k \end{aligned}$$

So, $(N_i, m_i) = 1$, since all $m$others are relatively simple too. Let m_i the inverse of the multiplication N_i be equal to $H_i\ mod\ m_i$, and let be $A_i = H_i N_i$. Where $A_i \equiv 0\ mod\ m_j$ for $j \neq i$ and $A_i \equiv 1\ mod\ m$. So now we have

$$\begin{aligned} a &= A_1 a_1 + A_2 a_2 + \cdots + A_k a_k \\ &= H_1 N_1 a_1 + H_2 N_2 a_2 + \cdots + H_k N_k a_k \end{aligned}$$

Then if we take $mod\ m_i$ from all terms except the term n will be canceled (since $m_i \mid N_j$ for $j \neq i$). So

$$a \equiv H_1 N_1 a_1 \ (mod\ m_i)$$
$$\equiv a_1 \ (mod\ m_i) \ \blacksquare$$

OBJECTIVES OF THE STUDY

The study aims to develop an investigation of some applications of linear congruence from number theory. Specifically, the study seeks to develop solutions of linear congruences through illustrative examples, to apply number theory in finding the ISBN number, in the conversion of decimal numbers to binary, octal, and hexadecimal, its application in encoding and encoding messages from the field of cryptography. To achieve this objective, the research will include: Investigating linear congruence theory; Focus on understanding the concept of linear congruence and its important properties, including equivalence relations and arithmetic operations related to linear congruence; Identifying applications of linear congruence in finding ISBN numbers; It will explore how linear congruence can be used to verify and locate ISBN numbers in the world of books and publications; Analyzing the use of linear congruence in converting numbers; It will examine how linear congruence can be used to convert numbers from base 10 to other bases used in computing, such as binary, octal and hexadecimal; Understanding the use of linear congruence in the field of cryptography; The role of linear congruence in information security and message encoding in the field of cryptography and computer security will be examined.

MATERIALS AND METHODS

The methodology of this study describes the steps and strategies followed to achieve the objectives of the study on applications of linear congruence. At first, a bibliographic analysis of the relevant literature was performed to meet the basic knowledge in number theory and computer science. After that, the main sources of data, including books, scientific articles and technical documents, that contributed to the deep understanding of this field were identified. The data collection process was accomplished through case studies, examining specific applications of linear congruence in various areas of computer science. Data analysis was performed using mathematical and computational methods to evaluate the efficiency and performance of linear congruence applications. Throughout this process, ethical aspects were respected in the processing and interpretation of data. This study includes a structured and detailed methodology to determine how applications of linear congruence can be used in computer science and to arrive at conclusive conclusions. Subsections provide discussions of an application of linear congruence to ISBNs, the number system, and the field of cryptography.

Applying linear congruence in ISBN (International Standard Book Number)

The main purpose of the ISBN (International Standard Book Number) system is to uniquely identify books and other published materials. ISBN is a unique identification code used to separate and identify books worldwide, providing an efficient way of identifying them for authors, publishers, booksellers and consumers. The importance of the ISBN system comes from the fact that it provides an internationally accepted standard for identifying books. With the help of an ISBN number, books can be uniquely identified on the world market. This helps in managing inventory, marketing and selling books efficiently. ISBN also allows bookstores and libraries to organize and catalogue books in an orderly manner. For authors and publishers, ISBN provides a way to promote and sell their books in the international market. An accurate and valid ISBN number can help increase the visibility and findability of the book online and in book distribution systems (NLK, 2023).

Since 1970, books have been given an ISBN made up of four parts: the first block identifies the country (or, more precisely, the language of the country), the second block details the publishing house, the third block details the book within this house, and the final digit serves as a check digit by calculating as follows: The check digit is an

integer, and we multiply the ISBN digits by 1, 2, 3,..., 10, starting from the left. where the number 10 appears in this way:

$$1 \cdot a_1 + 2 \cdot a_2 + 3 \cdot a_3 + 4 \cdot a_4 + 5 \cdot a_5 + 6 \cdot a_6 + 7 \cdot a_7 + 8 \cdot a_8 + 9 \cdot a_9 = a_{10} \text{ (mod 11)}$$

Example: Check the ISBN number 0-13-184-868-2 that it is correct.

$$1 \cdot 0 + 2 \cdot 1 + 3 \cdot 3 + 4 \cdot 1 + 5 \cdot 8 + 6 \cdot 4 + 7 \cdot 8 + 8 \cdot 6 + 9 \cdot 8 = 255 \equiv 2 \text{ (mod 11)}$$

From the solution of the task, we notice that the last digit is 2, and we find that the ISBN number is correct (Bradley, 1954; Hill, 1986).

So, the ISBN is an example of an application of an area of mathematics called coding theory. The code used for ISBN-10 is an error detection code. This means it can detect if a common mistake, such as a wrong digit or two digits being swapped, has been made in handling the number. Let's know briefly about the validity and how to find ISBN check digits, which is very essential in various fields.

Applying linear congruence to converting decimal numbers to binary, octal, and hexadecimal

The process of converting numbers to binary, octal and hexadecimal is important in computer science and programming. These numbering systems make use of different bases to represent numerical values. It can be challenging to mentally convert lengthy decimal values to binary, octal, and hexadecimal systems. While the decimal numbering system permits each digit in a number to have a value of one of ten (0–9), hexadecimal numbers can have 16 (0–F), octal numbers can only have eight (0–7), and binary numbers can only have two (0–1) digits (Henry-Stocker, 2022).

To convert whole decimal numbers into binary ones with base 2, the decimal number must be divided by 2, so $(mod\ 2)$ their remainders represent the binary number reading from bottom to top.

Also, analogously, the whole decimal number is converted into the octal one, that is, with base 8 using $(mod\ 8)$.

The same applies to the conversion of whole decimal numbers to hexadecimal, i.e. base 16 using $(mod\ 16)$, where the digits after 9 are replaced by $10 = A, 11 = B, 12 = C,\ 13 = D, 14 = E, and\ 15 = F$.

$$n = bq_0 + a_0, \quad 0 \le a_0 \le b$$

Example: To convert the decimal number $(12345)_{10}$ into an octal number, so $(mod\ 8)$.

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

The required number is $(\mathbf{30071})_{\mathbf{8}}$.

The number system is an essential part of computer technology that enables computers to perform all functions in just a few seconds. The three commonly used number systems, i.e., binary, octal, and hexadecimal play important roles in various applications and fields of computer and digital technology. Therefore, converting

numbers in these systems is very important. Our study showed that this conversion was efficient through the application of linear congruence for solving these problems.

Applying linear congruence in cryptography

Information security is the art and science of cryptography. It covers strategies and tactics intended to safeguard information and communications against unwanted access and outside intervention. The importance of cryptography in the digital society is emphasized, providing security and reliability in communications and data storage. It ensures protection of personal privacy, prevents identity theft, and protects critical and important information from external threats (Schneier, 1996; Ferguson, Schneier, & Kohno, 2010). On the other hand, the Chinese Remainder Theorem, also called the Chinese Restitution Theorem, is a theorem in number theory that provides a method for solving linear congruence problems. The theorem is based on the principle of number division through the common remainder of a group of numbers. The Chinese Remainder Theorem is important in computer science and security theory, especially in the field of cryptography, where the use of linear congruences and their solutions is used to develop encryption and decryption algorithms (Rosen, 2008; Niven, Zuckerman, & Montgomery, 2019).

The purpose of cryptography is that the adversary cannot see or receive the data (message) sent to the recipient. And this is done by encrypting the message sent where the receiver of the message using the key decrypts the message. We have two types of configurations: private key (synchronous) and public key (asynchronous) (Richards, 2021).

One type of message encryption is Caesar's key, which was used to send messages to the generals ($mod\ 3$), where each letter shifted by 3.

Example: Decrypt the message using Cesar's algorithm from the alphabet of the Albanian language:

LZHSHDLSHHJZH

The decrypted message ($mod\ 36$) is: $f(p) = (p+1)\ \boldsymbol{mod}\ 36$

MATEMATIKA

Note: Assuming that we have $m_1, m_2, \ldots m_k$ which are relatively simple, the rest of the Chinese Theorem states that each choice of $a_1\ mod\ m_1,\ a_2\ mod\ m_2,$ etc. creates in particular $x(a_1, a_2, \ldots a_k)\ mod\ m_1 m_2 \ldots m_k$. The number of choices we have is $m_1 m_2 \ldots m_k$,

Which agrees with the whole number $mod\ m_1 m_2 \ldots m_k$.

Note: Now we notice that $x(a_1, a_2, \ldots a_k, m_1, \ldots m_k)$ is prime factor of $m_1 m_2 \ldots m_k$ only if $(a_i, m_i) = 1$.

If x is a prime factor in $\prod m_i$ then it is a relatively prime factor for each of them, since $x \equiv a_i\ mod\ m_i$ where we will have $(a_i, m_i) = 1$.

Conversely, if $(a_i, m_i) = 1$. for all i, since $x \equiv a_i\ \ mod\ m_i$, this implies that $(x_i, m_i) = 1$. for all i, so, $(x, \prod m_i) = 1$.

For example, $x \equiv 2\ (mod\ 3)$

The numbers that are divisible by 3 and have a remainder of 2 are: … 2, 5, 8, 11, 14, . . .
Thus $(2,3)=1 \quad (5,3)=1 \quad (8,3)=1 \quad (11,3)=1 \quad (14,3)=1$
And their production $2\cdot 5=10 \quad (3,10)=1$

$$2\cdot 5\cdot 8=80 \quad (3,80)=1$$
$$2\cdot 5\cdot 8\cdot 11=880 \quad (3,880)=1$$

What is the number x as a prime factor in $\prod m_i$?
(By definition this is $\emptyset(m_1 m_2 \ldots m_k)$)

$$\underset{\emptyset(m_1)}{\left(\overset{\#of\ solutions\ a_1}{\longleftrightarrow}\right)}\underset{\emptyset(m_1)}{\left(\overset{\#of\ solutions\ a_2}{\longleftrightarrow}\right)}$$

with one a_i prime factor of m_i. This gives the conclusion that if m_i is a prime factor in pairs, $\emptyset(\prod m_i)=\prod \emptyset(m_i)$

We can use this to understand $\emptyset(n)$ for every n, with m_i factors in pairs

$$n=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$$
$$m_1=p_1^{e_1}, \quad m_2=p_2^{e_2}\ \ldots\ \quad m_k=p_k^{e_k}$$
$$\emptyset(n)=\emptyset\left(p_1^{e_1}\right)\emptyset\left(p_2^{e_2}\right)\ldots\ \emptyset\left(p_k^{e_k}\right)$$

How to find $\emptyset(p^e)$

$$\emptyset(p^e)=\{x \mid 1\ \le x\le p^e\ dhe\ (x,p)=1\ dhe\ k\ddot{e}shtu\ (x,p^e)=1\}$$
$$=\ p^e-p^{e-1}$$
$$=p^e-p^e\cdot p^{-1}$$
$$=p^e\left(1-\frac{1}{p}\right)$$

And, so:

$$\emptyset(n)=p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\ldots p_k^{e_k-1}(p_k-1)$$
$$=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ \left(1-\frac{1}{p_k}\right)$$
$$=n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

For example, $(2,3)=1$ and so $(2,3^2)=1, \quad (2,3^3)=1, \quad (2,3^4)=1$

These examples significantly advance computer science, particularly computer security, by demonstrating the fundamental significance of linear congruences in cryptography. This prepares the way for a simpler method of encrypting and decrypting the codes used in the RSA cryptosystem (Cuarto, 2014). These examples can also serve as the foundation for creating a computer program that solves linear congruences significantly more quickly. In addition, the application is highly recommended to facilitate learning and teaching the concept of linear congruence more effectively.

This study aims to further explore the applications of linear congruences in computer security and to develop a practical computer program that implements these concepts. Based on a strong theoretical foundation of linear congruences, the software will enable users to use and implement these security techniques in a consistent and efficient manner.

RESULTS AND DISCUSSION

Example:

$$\boldsymbol{17x \equiv 3\ (mod\ 29)}$$
$$17v \equiv 1\ (mod\ 29)$$
$$17v = 1 - 29w$$
$$17v + 29w = 1$$
$$\boldsymbol{x \equiv 3v\ (mod\ 29)}$$

$29 = 1 \cdot 17 + 12$
$17 = 1 \cdot 12 + 5$
$12 = 2 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$12 = 29 - 17$
$5 = 17 - 12$
$2 = 12 - 2 \cdot 2$
$1 = 5 - 2 \cdot 2$
$1 = 5 - 2 \cdot 2$
$1 = 5 - 2 \cdot (12 - 2 \cdot 5)$
$1 = 5 - 2 \cdot 12 + 4 \cdot 5$
$1 = 5 \cdot 5 - 2 \cdot 12$
$1 = 5 \cdot (17 - 12) - 2 \cdot 12$
$1 = 5 \cdot 17 - 5 \cdot 12 - 2 \cdot 12$
$1 = 5 \cdot 17 - 7 \cdot 12$
$1 = 5 \cdot 17 - 7 \cdot (29 - 17)$
$1 = 5 \cdot 17 - 7 \cdot 29 + 7 \cdot 17$
$1 = 12 \cdot 17 - 7 \cdot 29$
$\boldsymbol{17 \cdot 12 + 29 \cdot (-7) = 1} \quad \Rightarrow \quad \boldsymbol{17v + 29w = 1}$

Where $v = 12$ and $w = -7$

$17 \cdot 12 \equiv 1\ (mod\ 29)$

So 12 is the inverse of multiplication for 17 $(mod 29)$.

$$17x \equiv 3\ (mod\ 29)$$
$$12 \cdot 17x \equiv 12 \cdot 3\ (mod\ 29)$$
$$x = 36\ (mod\ 29)$$
$$\boldsymbol{x = 7}$$

Example:

$$35x \equiv 14\ (mod\ 28)$$

$GCD(35, 28) = 7$. To solve, it must first be satisfied by 7 winning $5x \equiv 2\ mod\ 4$. The solution of $x \equiv 2\ mod\ 4$ is $x = 2$, which will satisfy the congruence $m' = \frac{28}{7} = 4 \Rightarrow$ of all solutions $mod\ 28 \equiv 2, 6, 10, 14, 18, 22, 26$.

Example:

$$x \equiv 2\ (mod\ 3), \quad N_1 = 5 \cdot 7 = 35 \equiv 2\ (mod\ 3), \quad H_1 = 2$$
$$x \equiv 3\ (mod\ 5), \quad N_2 = 3 \cdot 7 = 21 \equiv 1\ (mod\ 5), \quad H_2 = 1$$
$$x \equiv 5\ (mod\ 7), \quad N_3 = 3 \cdot 5 = 15 \equiv 1\ (mod\ 7), \quad H_3 = 1$$

$$x = H_1N_1a_1 + H_2N_2a_2 + H_3N_3a_3 \quad (mod\ m_1m_2m_3)$$
$$= 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 5\ (mod\ 105)$$
$$= 278\ (mod\ 105)$$
$$\equiv 68\ (mod\ 105)$$

Numerical calculations for Algorithms

To do the arithmetic calculation modulo N (for some given numbers). Steps to writing N, which is approximately the number of digits $N = c \log N$ for a $c$onstant number.

The additive property is stepped $\log N$/ time

Multiplication (multiplicative property) is $(\log N)^2$ steps/time in the simplest way

Karatsuba multiplication: This algorithm for multiplication is quicker and takes less time for $(\log N)^{\log 3/\log 2}$

The plugin can be further enhanced $\log N\ poly(\log\log n)$ using the fast transform mode.

Exponential form is to calculate $a^b\ mod\ N$, with a not greater than N and b also less than N. The most obvious way would be to repeat the multiplication for $N(\log N)^2$, but better write b in binary as:

$$b = b_r b_{r-1} \ldots b_0$$
$$= 2^r b_r + 2^{r-1} b_{r-1} + \ldots + b_0$$

After the calculation, $a^{2^0}, a^{2^1}, \ldots a^{2^k}\ mod\ N$ the repetition is obtained ($(\log N)^2$ for each). And it is taken

$$\left(a^{2^0}\right)^{b_0}\left(a^{2^1}\right)^{b_1}\left(a^{2^2}\right)^{b_2} \ldots \left(a^{2^r}\right)^{b_r}$$

for a total of

$$\log b\ (\log N)^2 \sim (\log N)^3$$

Example: Show that the amount $\log_3 2 + \log_3 2^2 + \log_3 2^3 + \cdots + \log_3 2^n$ is fully divisible by $n+1$, $(n \in N)$

$$(\log_3 2 + \log_3 2^2 + \log_3 2^3 + \cdots + \log_3 2^n) \equiv x\ (\ mod\ \ (n+1))$$
$$(1\log_3 2 + 2\log_3 2 + 3\log_3 2 + \cdots + n\log_3 2) \equiv x$$
$$(1 + 2 + 3 + \cdots + n\ )\log_3 2 \equiv x$$
$$\frac{n \cdot (n+1)}{2}\log_3 2 \equiv x$$
$$\tfrac{1}{2} \cdot n\ (\boldsymbol{n+1})\log_3 2 \equiv x \text{ where } (mod\ \ (\boldsymbol{n+1}))$$
$$x = 0$$

Example: 4^{62}, if you divide by 7, what will be the remainder?

$4^{62} \equiv x \quad (mod\ 7) \quad x =?$

$$\begin{aligned}
4^1 &\equiv 4 \pmod 7, \quad 4 = 7\cdot 0 + 4 \equiv 4 \pmod 7 \quad H_1 = 4\\
4^2 &\equiv 2 \pmod 7, \quad 16 = 7\cdot 2 + 2 \equiv 2 \pmod 7 \quad H_2 = 2\\
4^3 &\equiv 1 \pmod 7, \quad 64 = 7\cdot 9 + 1 \equiv 1 \pmod 7 \quad H_3 = 1\\
4^4 &\equiv 4 \pmod 7, \quad 256 = 7\cdot 36 + 4 \equiv 4 \pmod 7 \quad H_1 = 4\\
4^5 &\equiv 4 \pmod 7, \quad 1024 = 7\cdot 146 + 2 \equiv 2 \pmod 7 \quad H_2 = 2\\
&\vdots\\
62 &= 3\cdot 23 + 2 \quad \Rightarrow x = 2
\end{aligned}$$

4^{62} if divided by 7 the remainder will be 2

Example: If today is Tuesday in 200 days what day will it be?

$200 \equiv x \pmod 7$

$200 = 7\cdot 28 + \mathbf{4}$

Table 1. Calculation of the day for the example

MONDAY	WEDNESDAY	TUESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
6	0	1	2	3	4	5

CONCLUSION AND RECOMMENDATION

In this article, we have tried to describe some of the applications of number theory, namely linear congruence. We have also made an effort to establish links and linkages between these methodologies and theoretical frameworks, as well as to pinpoint knowledge gaps that may be filled by the theories in order to address different issues. Therefore, in this short paper, we have shown some powerful extensions and applications of linear congruence. We discussed here the applications of linear congruence in ISBN, in the conversion of decimal numbers to binary, octal, and hexadecimal, as well as its application in the field of cryptography.

The findings of the study show that the compatibility of the book ISBN format can be checked through linear congruence. Also, these results show in a very holistic way that you understand how using linear congruence the conversion of decimal numbers to binary, octal, and hexadecimal can be done. Additionally, because the idea of a linear congruence system is employed in the encoding and decoding of codes for network security and other purposes, the findings of this study may be helpful to researchers working in the field of cryptography.

The problems solved in this study are very motivating and intriguing applications have been found in several fields of mathematics and computer science, and there is a promise for more applications/implications in these or other directions.

DECLARATION OF CONFLICTING INTERESTS

The authors declare that there is no potential conflict of interest about the research conducted, in the authorship and/or publication of this article.

FUNDING

The authors received no financial support for the authorship, research, or publication of this article.

REFERENCES

Barendregt, H. (1990). Functional Programming and Lambda Calculus". In Jan van Leeuwen (ed.). Formal Models and Semantics. *Handbook of Theoretical Computer Science*, 321–364.

Bourke, C.M., & Choueiry, B. Y. (2006). Number Theory: Applications. *Computer Science & Engineering*, 1-10.

Bradley, P. (1954). Book numbering: The importance of the ISBN. *The Indexer, 18*(1), 25–26.

Burton, D. M. (2011). Elementary Number Theory. *McGraw-Hill Education*.

Conrad, K. (2004). The Chinise Remainder Theorem. *UConn math department.*

Cuarto, P.M. (2014). Algebraic Algorithm for Solving Linear Congruences: Its Application To Cryptography. *Asia Pacific Journal of Education, Arts and Sciences, 1*(1), 34-37.

Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. *John Wiley & Sons.*

Henry-Stocker, S. (2022). Converting numbers on Linux among decimal, hexadecimal, octal, and binary. *Network World:* https://www.networkworld.com/article/3681079/converting-numbers-on-linux-among-decimal-hexadecimal-octal-and-binary.html

Hill, R. (1986). First Course in Coding Theory. *Oxford, England: Oxford University Press.*

Hungerford, T. W. (1974). Algebra. *Springer-Verlag, 27*.

Niven, I., Zuckerman, H.S. & Montgomery, H.L. (2019). An Introduction to the Theory of Numbers. *John Wiley & Sons.*

NLK. (2023). International Standard Identifiers (ISBN/ISSN/ISNI). *National Library of Korea:* https://www.nl.go.kr/EN/contents/EN40800000000.do

Richards, K. (2021). Cryptography. *Tech Target:* https://www.techtarget.com/searchsecurity/definition/cryptography

Robert, L. & Page, I. (2003). Number Theory, Elementary. *Encyclopedia of Physical Science and Technology (Third Edition).*

Rosen, K.H. (2008). Discrete Mathematics and Its Applications. *McGraw-Hill Education.*

Schneier, B. (1996). Applied Cryptography. *John Wiley & Sons.*