APPLICATIONS OF CONGRUENCE IN VARIOUS FIELDS

Rushadije RAMANI HALILI[1], Azir JUSUFI[1], Merita BAJRAMI[1], Vesa HAZARI[1]

[1]*Department of Mathematics, Faculty of Natural Sciences and Mathematics*
** Corresponding author e-mail: rushadije.ramani@unite.edu.mk*

Abstract

Congruence theory is one of the fundamental topics in number theory and has important applications in various scientific and practical fields. This paper presents several applications of congruences, including check digits, identification numbers, ISBN systems, and modular designs. Special attention is devoted to the use of modular arithmetic in error detection and verification processes. In addition, we illustrate how congruences can be applied in the construction of geometric and artistic modular patterns. The presented examples demonstrate the relevance of congruence theory in mathematics, computer science, coding theory, and everyday life.

Keywords: Congruence,modular arithmetic,check digits, coding theory, identification numbers, ISBN,modul designs

Introduction

One of the most important concepts in number theory, the congruence relation, was introduced and developed by the German mathematician Karl Friedrich Gauss in 1801 in his work " Disquistiones Arithmeticae". Gauss focused on the reminder obtained when one natural number is divided by another natural number. $[1, 6, 12]$
The congruence made it possible to more easily formulate the results obtained in the theory of divisibility, so that unnecessary calculations are not carried over. The congruence relation shares many properties with the equality relation, so it is no coincidence that the congruence symbol
" $\equiv$ " , which introduced Gauss, similar to the equal sign " $=$ ". $[2, 7]$
Definitions 1. If **a** and **b** are integres, we say that **a** is congruent to **b** modulo **m** if $m \mid (a - b)$. If **a** is congruent to **b** modulo **m**, we write $a \equiv b \ (mod\ m\ )$. If $m \nmid (a - b)$, we write $a \not\equiv b \ (mod\ m\ )$ and say that **a** and **b** are incongruent modulo **m**. $[1, 7]$
In this research we will focus on the application of congruence and based on this research we will see that it is an integral part of everyday life. One of the most famous application of cngruence is clock aithmetic. The time on the clock is shifted using congruence of modulo 12. For example if it is 10 o'clock for 4 hours pass, it will be 14, but since the clock is divided into 12 equal parts,we have:

$$10 + 4 = 14 \equiv 2 \ (mod\ 12\ )$$

Also, numbers are all around us,driver's license numbers, books, products, and we will show that these numbers also use congruences as a form of protection and verification. We will see that beautiful designs can be created using congruence. Congruence is also used in scheduling and grouping systems in sports competitions.
Congruences have many applications in discrete mathematics, computer science, and many other disciplines. The three main applications are: using congruences to assign memory locations for computer files, generating pseudorandom numbers and checking digits. $[3, 6]$
Modular arithmetic can also be used to produce checksums of various types such as code numbers used to identify retail products, numbers used to identify books, airline ticket numbers etc.

Check Digits[1]

Coding theory is a branch of mathematics that deals with the analysis of codes that are transmitted through channels and the detection and correction of errors that may arise. In this part, we will show how congruences can help in finding and correcting errors in sent messages. [8, 9]

Identification numbers

Many institutions (such as banks, book publishers, post offices etc) and companies use identification numbers to mark their products, documents, accounts, people and many other entities. Identification numbers contain coded information about the thing they stand for and can typically be numeric (consisting of digits) or alphanumeric (constisting of numbers and letters of the English alphabet). The two pieces of information they carry are essential, the length of the identification number (total number of digits or letters) and the position of each digit or letter. An identification number of length n is denoted by $d_1d_2\ldots d_n$, where d_1 is the first digit or letter of the number, d_2 is the second digit or letter, and d_n which is the last digit or letter.

Every day, identification numbers are sent by phone, scanned or entered into computers, transmitted over the internet or sent by mail. During transmission, errors may occur, meaning one or more digits may be replaced. [9]

It is essential that the identification numbers are transmitted correctly. For example, if the product's barcode is scanned incorrectly in the store, it is possible that the customer will be charged a price of 100 dollars for a product that costs 15 dollars.

The most common transmission errors that occur are a single digit error (one digit in the identification number changes its value) and the error of replacing two consecutive digits.

In order to prevent this, it was necessary to develop a method that would recognize such errors, that is, that would recognize when the identification number is wrong. This method is a check digit method that depends mostly on the scalar product of two vectors and the modules.

The verification digit is usually an additional digit that servers to verify the received identification number. It can be anywhere in the identification number, but most often it is the last digit of the number.

Definition 2: The scalar product of vectors $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ and $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ is defined by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i$$ [2]

ISBN (International Standard Book Number)

ISBN (International Standard Book Number) is a unique code assigned to book publications for their international identification. This code is used for printed books, eBooks, audiobooks, and some similar materials such as maps.

[1] Elementary Number Theory and its Applications, fifth edition, Kenneth H. Rosen

The ISBN system (International Standard Book Number) was designed and introduced in the United Kingdom in 1968 by J. Whitaker & Sons, and a year later the company R.R. Bowker introduced the ISBN system in the United States. [10]
ISBN is an important tool for the book industry, facilitating the registration and sharing of book information at a global level. It enables the transmission and computerized storage of book data.
Since 2007, the 13-digit ISBN has been in use, divided into five parts:
The first part is the prefix element, usually 978.
The second part identifies the country or language area in which the book is published.
The third part identifies the publisher of the book.
The fourth part is the unique number of the book within the publishing house.
The fifth part is the check digit (1 digit), calculated based on the previous digits, and it is used to verify the correctness of the code.

Figure 1. Example of an ISBN-13 code for a book publication.

The ISBN shown above belongs to the book "Methods of Numerical Analysis (Numerical Algorithms)" by Fatmir Hoxha. Based on our analysis, let us examine whether the components are correct by explaining what each number represents:
978 – this is the prefix element, indicating that the book follows the international ISBN format.
9928 – this number identifies the country where the book is published; this code shows that the book is published in Albania.
4091 – this code identifies the specific publisher of the book.
7 – this represents the specific title of the book within that publisher.
1 – this is the check digit, used to verify whether the ISBN is correct.
Thus, 1 is the digit obtained using congruence, specifically modulo 10.
Let us verify that the check digit of this ISBN is 1:

$$d \equiv -(x_1, x_2, \ldots, x_{12}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \ (mod\ 10)$$
$$\equiv -(9, 7, 8, 9, 9, 2, 8, 4, 0, 9, 1, 7) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \ (mod\ 10)$$
$$\equiv -(9 + 21 + 8 + 27 + 9 + 6 + 8 + 12 + 0 + 27 + 1 + 21) \ (mod\ 10)$$
$$\equiv -149 \ (mod\ 10) \equiv 1 \ (mod\ 10).$$

Thus, our analysis is correct.

Modular designs

Congruences can be used to create different designs. In this chapter, we will show how to create a star with m vertices, the design of residues (m,n) and the design obtained using tables of multiplication and addition of the smallest residues modulo m (quilt designs). [4]

1. A star with m points

In order to construct a star with m vertices on a circle of arbitrary radius, we mark m equidistant points and mark them with 0 to m-1 modulo m. We choose the smallest remainder i modulo m for which i and m are relatively prime, (i,m)=1. Connect each point x with point x+1 modulo m, more precisely connect 1 with 1+i (mod m) and continue like this until all points are connected and color the resulting star.
Example, let's construct a star with 13 points and choose the remainder 5, (13,5)=1.

Table 1. Values of "d≡x+5" ("mod13") used in the construction of the 13-point star.

x	$d \equiv x + i \ (mod\ 13)$	d
0	0+5	5
1	1+5	6
2	2+5	7
3	3+5	8
4	4+5	9
5	5+5	10
6	6+5	11
7	7+5	12
8	8+5	0
9	9+5	1
10	10+5	2
11	11+5	3
12	12+5	4

Connect 0 with 5, 1 with 6, 2 with 7… and 12 with 4. In this way, we got a star with 13 points shown in below

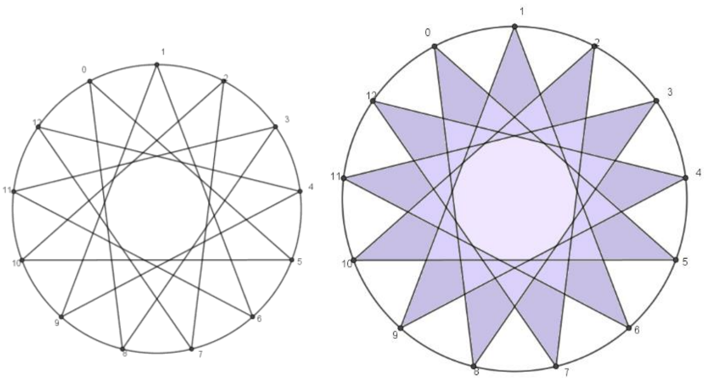

Figure 2. Construction of the 13-point modular star and its colored design.

Now we will create the design of (59,57), by connecting the corresponding numbers we get:

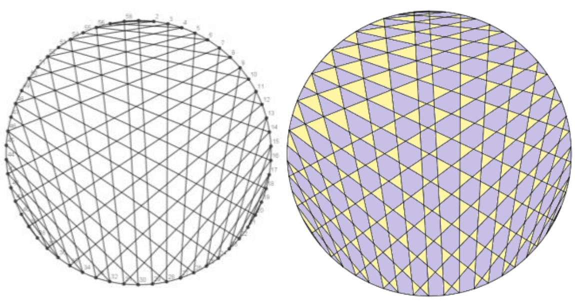

Figure 3. Residue design m (59,57) and its colored version.

Let's make a design with the addition table of modulo 8. We formulate the table:

Table 2. Addition table of the smallest residues modulo 8.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

We create designs for each issue

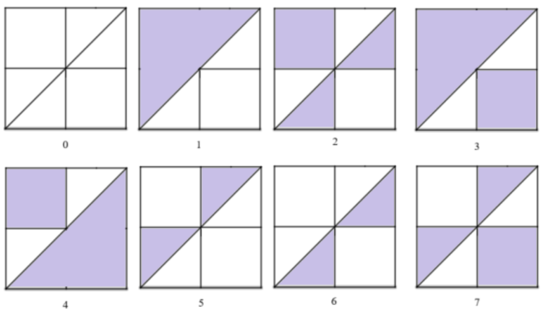

Figure 4. Basic modular patterns corresponding to the residues modulo 8.

By combining these designs according to the table, we obtain this design:

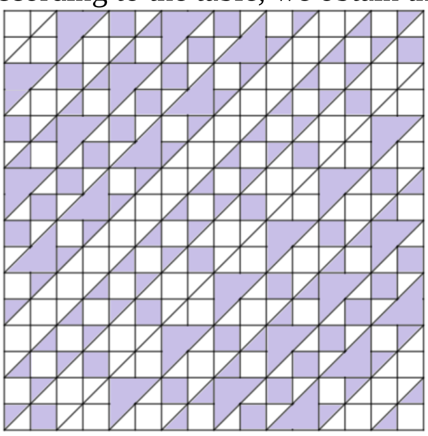

Figure 5. Modular quilt design obtained from the addition table modulo 8.

From this design we can also get other designs by rotating it in different directions and joining them. We get the design:

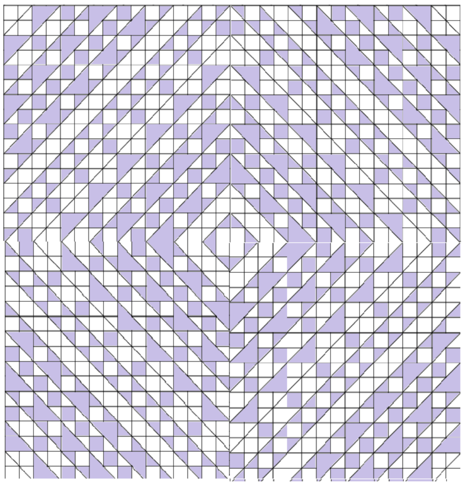

Figure 6. Rotated modular quilt design obtained from the modulo 8 addition patterns.

Conclusion

One of the oldest branches of mathematics is number theory and congruence theory.
Congruence as a simple idea finds wide application and sometimes we are not aware of its application in daily life. By looking at the clock or remembering the day of the week we apply congruence. Also, even before we knew its definition, we used it in elementary school to determine when one number was divided by another number.
As technology developed and the number of products and services increased, it was necessary to find a simple and easy way to track them, and they began to be marked with numbers. Identification numbers contain coded information about products, people, documents and other things.
Since they are encrypted, it is important that errors are detected when they are sent, scanned or entered into a computer. Of course it wouldn't matter to us if, for example, the EAN-13 barcode is scanned incorrectly and a higher product price is charged than it is.
Mail delivery in the United States is made easier and faster. The check digit method also has its drawbacks, because sometimes errors cannot be detected, but most of the time errors are detected.
In art, congruences can be applied to create beautiful modular designs, in sport fields to determine the day of the week for any date of any year.
These are some examples of that are presented in the paper, because congruence can also be applied in music, chemistry, cryptography and others. [13]

References

[1] Elementary Number Theory and its Applications, fifth edition, Kenneth H. Rosen
[2] Elementary Number Theory and Applications, 2-nd Edition, Thomas Koshy
[3] Discrete Mathematics, third edition, Schaum's
[4] Mathematics and Modulo Art, Tom Cooper, Tony Watson
[5] A Concrete Introduction to Higher Algebra, third edition, Lindsay N. Childs