Basic Theory of Congruences

A Dissertation for

MAT-651 Discipline Specific Dissertation

Credits: 16

Submitted in partial fulfilment of Masters Degree

M.Sc. in Mathematics

by

Miss. Chandani Rajbhargav Mistry

22P0410016

ABC ID : 884-952-308-287

201602898

Under the Supervisor of

Mr. Brandon Fernandes

School of Physical & Applied Sciences

Mathematics Discipline

GOA UNIVERSITY

APRIL 2024

Examined by:

Seal of the School

DECLARATION BY STUDENT

I hereby declare that the data presented in this Dissertation report entitled, "Basic Theory of Congruences" is based on the results of investigations carried out by me in the Mathematics Discipline at the School of Physical & Applied Sciences, Goa University under the Supervision of Mr. Brandon Fernandes and the same has not been submitted elsewhere for the award of a degree or diploma by me. Further, I understand that Goa University will not be responsible for the correctness of observations / experimental or other findings given the dissertation.

I hereby authorize the University authorities to upload this dissertation on the dissertation repository or anywhere else as the UGC regulations demand and make it available to any one as needed.

Signature:

Student Name: Chandani Rajbhargav Mistry

Seat no: 22P0410016

Date: 9|5|2024

Place: GOA UNIVERSITY

COMPLETION CERTIFICATE

This is to certify that the dissertation report "Basic Theory of Congruences" is a bonafide work carried out by Miss. Chandani Rajbhargav Mistry under my supervision in partial fulfilment of the requirements for the award of the degree of Master of Science in Mathematics in the Discipline Mathematics at the School of Physical & Applied Sciences , Goa University.

Signature :

Supervisor : Mr. Brandon Fernandes

Date: 10|05|2024

School of Physical and Applied Sciences
Goa University

School Stamp

Signature of HoD of the Dept

Date: 10|5|2024

Place: Goa University

PREFACE

This Project Report has been prepared in partial fulfilment of the requirement for the Subject: MAT - 651 Discipline Specific Dissertation of the programme M.Sc. in Mathematics in the academic year 2023-2024.

The topic assigned for the research report is: "Basic Theory of Congruences." This survey is divided into five chapters. Each chapter has its own relevance and importance. The chapters are divided and defined in a logical, systematic and scientific manner to cover every nook and corner of the topic.

FIRST CHAPTER :

The Introductory stage of this Project report is based on overview of Congruences and the history of number theory.

SECOND CHAPTER:

This chapter deals with the Concept of Congruences. In this topic we have discuss the Elementary Properties of Congruences, also have discussed topics like Complete Residue System and Reduced Residue System.

THIRD CHAPTER:

In this chapter we have introduce a type of congruence, that is, Linear Congruences. The main aim is to prove some basic result concerning this type of congruences, and, in particular, some theorems that are related to this topic, for example, Fermat's Theorem, Euler's Theorem and so on. We have also discussed one application here. .

FOURTH CHAPTER:

This chapter deal with another type of congruence that is, Identical Congruences. Our main focus is on topics like Order of Integers and Primitive roots which are often used in solving problems in congruences. .

FIFTH CHAPTER.

This chapters deals with one more type of congruence, that is, Quadratic Congruences. This topic includes the Quadratic Congruences and Quadratic Residues. .

ACKNOWLEDGEMENTS

First and foremost, I would like to express my gratitude to my Mentor, Mr. Brandon Fernandes, who was a continual source of inspiration. He pushed me to think imaginatively and urged me to do this homework without hesitation. His vast knowledge, extensive experience, and professional competence in Number Theory enabled me to successfully accomplish this project. This endeavour would not have been possible without his help and supervision.

Table of contents

Chapter 1

INTRODUCTION

The great German mathematician Gauss was the first to introduce the concept of congruence in number theory and to invent an appropriate symbol to denote it. With this tool Gauss was able to revolutionize the science of numbers.

Gauss (1777-1855) is considered by many as the greatest mathematician in history. His researches pervaded all the known branches of mathematics of his time, geometry, analysis, algebra, complex numbers, mechanics, electricity and magnetism, astronomy, and above all, theory of numbers in which he particularly took great delight.

Chapter 2

Congruences

2.1 Introduction

In this chapter we introduce the elementary concepts and elementary properties of congruences. The concept of congruence was proposed by K. F. Gauss about 1800. Congruences often arise in everyday life.
For instance, if the second of January is Sunday, then 9, 16, 23, 30 of the same month are all Sundays, since when they are divided by 7, the remainders are all 2.

Gauss introduced a remarkable notation which simplifies many problems concerning divisibility of integers. In so doing he created a new branch of number theory called the theory of congruences, the foundations of which are discussed in this chapter.

2.2 Concept of Congruences and its Elementary Properties

Definition 2.2.1. Let a and b be any two integers. If a positive integer m divides $a-b$, then we say a is **congruent** to b modulo m.
i.e.

$$a \equiv b \pmod{m} \tag{2.1}$$

Expression (2.1) is called the congruence, m is called the modulus of the congruence, and b is called a residue of $a \pmod{m}$.

Theorem 2.2.2. *Congruence relations satisfy the following properties of equivalence:*

Proof. : **Reflexive Law:** $a \equiv a \pmod{m}$

Symmetric Law: If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Transitive Law: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Addition Law: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.

Multiplication Law: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Exponential Law: If $a \equiv b \pmod{m}$ and $k \in N$ then $a^k \equiv b^k \pmod{m}$

Cancellation Law: If $a \equiv b \pmod{m}$ and $gcd(a,m) = 1$, then $ac \equiv bc \pmod{m} \Rightarrow c \equiv d \pmod{m}$. □

2.3 Complete Residue System

Definition 2.3.1. Let $a \equiv b \pmod{m}$. If $0 \leq b < m$ then b is called the **least residue** of a (mod m).

Definition 2.3.2. A set of m integers whose least residues (mod m) are $0, 1, 2, ..., m-1$ in some order is called **complete system** (mod m).

Example: 2.3.3. *The set of integers*

$$\{-5, 11, 59, -13, -57, 26, 49\}$$

is a complete system $\pmod{7}$ *because the set consist of 7 integers whose least residue* $\pmod{7}$ *are 2, 4, 3, 1, 6, 5, 0 which is a permutation of the numbers o, 1, 2, 3, 4, 5, 6.*

Theorem 2.3.4. *A set of integers is a complete system* $\pmod{m}$ *if and only if the set consist of m integers which are incongruent* $\pmod{m}$.

Proof. i. First suppose the set is a complete system $\pmod{m}$. Then by definition it has m integers whose least residues $\pmod{m}$ are $0, 1, \ldots, m-1$ in some order. Since this residues are incongruent $\pmod{m}$, it follows that the m integers of the set are all incongruent $\pmod{m}$. This proves the only if part of the theorem.

ii. Conversely, suppose that the set consist of m integers which are incongruent $\pmod{m}$. This implies that the least residues of the integers are: m in numbers, belongs to the set $\{0, 1, \ldots, m-1\}$ and are all different. It follows that the least residues of the m integers of the set are $\{0, 1, \ldots, m-1\}$ in some order.

Therefore the set is a complete system $\pmod{m}$. □

Theorem 2.3.5. *Any m integers in arithmetical progression with common difference relatively prime to m form a complete system* $\pmod{m}$.

Proof. Let the integers in A.P. be

$$a, a+t, \ldots, a+(m-1)t \tag{2.2}$$

such that $(t,m) = 1$. We shall prove that these m integers are incongruent $\pmod{m}$. Suppose these are not. This implies that

$$a+it \equiv a+jt \pmod{m} \tag{2.3}$$

for some i and j such that $i \neq j$.

It follows that $it \equiv jt \pmod{m}$ and since $(t,m) = 1, i \neq j \pmod{m}$, i and j are both less than m.

Therefore this is a contradiction, since $i \neq j$. Hence the integers (2.2) are incongruent $\pmod{m}$. □

The following theorem is very important and should be committed to memory.

Theorem 2.3.6. *Let a be any given integer and let C be any complete system of residues mod m.Then there exists in C a unique integer b corresponding to a, such that $a \equiv b$* $\pmod{m}$.

Proof. Let r be the least residue of $a \pmod{m}$ so that we have

$$a \equiv r \pmod{m}, \quad o \leq r < m. \tag{2.4}$$

Also the set of least residues of $C \pmod{m}$ is $S = \{0, 1, \ldots, m-1\}$. Hence r belongs to S. If then b is the unique member of C of which r is the least residue $\pmod{m}$ then obviously

$$r \equiv b \pmod{m} \tag{2.5}$$

(2.4) and (2.5) prove that $a \equiv b \pmod{m}$ and this proves the theorem. □

Example: 2.3.7. *The set*

$$(49, 20, 10, 17, -18, -27)$$

is a complete system $\pmod 6$. *Find the integer of the set which is congruent* $\pmod 6$ *to 491.*

Solution: The least residues of the numbers of the given set are $1, 2, 4, 5, 0, 3$ *respectively and the least residue of 491* $\pmod 6$ *is 5. Hence 17* $\pmod{16}$. *Therefore 17 is the required number.*

Theorem 2.3.8. *Every complete system* $\pmod m$ *has exactly* $\phi(m)$ *integers relatively prime to m.*

Proof. Let C be the complete system. Also let a be any integer of C and r its least residue modulo m. Then we know $(a, m) = 1$ if and only if $(r, m) = 1$. It follows that there are exactly as many integers prime to m in C as are integers prime to m among (the least residues of C) $0, 1, 2, ..., (m-1)$. But we know that there are exactly $\phi(m)$ integers prime to m. Hence C has exactly $phi(m)$ integers prime to m. □

Theorem 2.3.9. *Let* $\{a_1, \dots, a_m\}$ *be a complete system* $\pmod m$. *Let* $(k, m) = 1$. *Then* $\{ka_1, \dots, ka_m\}$ *is also a complete system* $\pmod m$.

Proof. Let $S = \{ka_1, \dots, ka_m\}$. Obviously there are m integers in S. Also these integers are all incongruent $\pmod m$. If this is not true let $ka_i = ka_j \pmod m$ for two different integers i and j. Then, since $(k, m) = 1$ we can cancel the factor k from the two sides of the congruence obtaining $a_i = a_j \pmod m$. But this contradicts the fact $\{a_1, \dots, a_m\}$ is a complete system $\pmod m$. Therefore the integers of S are incongruent $\pmod m$. It follows that S is a complete system $\pmod m$. □

Theorem 2.3.10. *Let*

1. $\{a_1,\ldots,a_{m_1}\}$ *be a complete system* $\pmod{m_1}$.

2. $\{b_1,\ldots,b_{m_2}\}$ *be a complete system* $\pmod{m_2}$.

3. $(m_1,m_2)=1$. *Then the set C defined by*

$$\{a_i m_2 + b_j m_1, \quad i=1,2,\ldots,m_1, \quad j=1,2,\ldots,m_2\}$$

is a complete system $\pmod{m_1,m_2}$

Proof. i can have m_1 different values and j can have m_2 different values independent of each other. Therefore the numbers in C is m_1m_2. Also the integers of C are incongruent $(\text{mod } m_1m_2.)$ This can be proved as below:

$$a_i m_2 + b_j m_1 \equiv a_k m_2 + b_l m_1 \pmod{m_1m_2}$$

for somr i,j,k and l.

Then in succession we obtain

$$a_i m_2 + b_j m_1 \equiv a_k m_2 + b_l m_1 \pmod{m_1},$$

$$a_i m_2 \equiv a_k m_2 \pmod{m_1},$$

$$a_i \equiv a_k \pmod{m_1}.$$

which is impossible unless $i = k$.

Similarly we can prove that $b_j \equiv b_l \pmod{m_2}$ which also is impossible unless $j = l$. It follows that C is a complete system $\pmod{m_1 m_2.}$ □

2.4 Reduced Residue System

Definition 2.4.1. A set of $\phi(m)$ integers whose least residues $\pmod{m}$ are $r_1, \dots, r_{\phi(m)}$ in some order is called a **reduced system of residues** $\pmod{m}$ or briefly a **reduced system** $\pmod{m}$.

Example: 2.4.2. *Show that the set*

$$\{22, -1, 43, 46, -19, 79, 113, 452\}$$

is a reduced system $\pmod{15}$.

***Solution**: The least residues* $\pmod{15}$ *of the integers of the set*

$$7, 14, 13, 1, 11, 4, 8, 2 \tag{2.6}$$

respectively. Alsonthe integers less than 15 and prime to it are

$$1, 2, 4, 7, 8, 11, 13, 14. \tag{2.7}$$

It is easily seen that (2.6) is a permutation of (2.7). Therefore the given set is a reduced system $\pmod{m}$.

Theorem 2.4.3. *A set R of integers is a reduced system $\pmod{m}$ if and only if R has integers which are incongruent $\pmod{m}$ and prime to m.*

Proof. (A) First suppose that R is a reduced system $\pmod{m}$. This implies that R has $\phi(m)$ integers, the least residues of which are $r_1, r_2, \ldots, r_{\phi(m)} \pmod{m}$, in some order. Now $r_1, r_2, \ldots, r_{\phi(m)}$ are prime to m and are incongruent It follows that the integers of r are also prime to m and are incongruent $\pmod{m}$. This proves the only if part of the theorem.

(B) Conversely, suppose R has $\phi(m)$ integers which are incongruent $\pmod{m}$ and prime to m. then consider the least residue of these integers $\pmod{m}$.

1. They are obviously $\phi(m)$ in numbers.
2. They belong to the set $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ because the integers of R being prime to m their least residues are also prime to m.
3. They are all different since the integers of R are incongruent $\pmod{m}$.

From (1),(2) and (3) it follows that the least residues of the $\phi(m)$ integers of R are $r_1, r_2, \ldots, r_{\phi(m)}$ in some order. So by definition R is a reduced system $\pmod{m}$. □

Theorem 2.4.4. *Let R be any reduced system of residues $\pmod{m}$ and let a be any given integer such that $(a,m) = 1$. Then there exists in R a unique integer, corresponding to a, say b such that $a \equiv b \pmod{m}$.*

Proof. Let r be the least residue of $a \pmod{m}$ so that we have

$$a \equiv r \pmod{m}, \quad 0 \leq r < m \tag{2.8}$$

and

$$(r,m) = (a,m) = 1. \tag{2.9}$$

But the set of least residues of R is $S = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ where $r_1, r_2, \ldots, r_{\phi(m)}$ are all positive integers less than m and prime to m. It follows from (2.8) and (2.9) that r belong to S. If then b is the unique member of R of which r is the least residue $\pmod{m}$ then obviously

$$r \equiv b \pmod{m}. \tag{2.10}$$

(2.8) and (2.10) imply that $a \pmod{m}$ which proves the theorem. □

Chapter 3

LINEAR CONGRUENCES

3.1 Introduction

Just we have equations and their solutions in algebra we have congruences and their solutions in number theory. For example, $6x \equiv 5 \pmod{7}$ where x is an unknown number(integer). Any value of x which satisfies the given congruence is called its solution. Thus if we put $x = 2$, we find that $6 \times 2 \equiv 5 \pmod{7}$ is true. Hence $x = 2$ is a solution. Further it is clear that all integers congruent to $2 \pmod{7}$ namely, $x = \ldots, -12, -5, 2, 9, 16\ldots$ also satisfies given congruence. Hence each of them is a solution of given congruence.

But all these congruent solutions are by convention considered as one and the same solution, and the solution is written $x \equiv 2 \pmod{7}$ which obviously includes all the integers. We could as well have written the solution as $x \equiv -5 \pmod{7}$ or $x \equiv 9 \pmod{7}$

and so on. But we choose to write it as $x \equiv 2 \pmod 7$ because 2 belongs to the set of least residues $\pmod 7$. This is the usual and standard practice.

Definition 3.1.1. The general form of the congruence of the first degree in one unknown or variable s is

$$ax \equiv b \pmod m \tag{3.1}$$

where m does not divide a. This is called a **linear congruence**. Any value of x which satisfies (3.1) is called a **solution** (or root) of the congruence. Suppose $x = h$ satisfies (3.1). Then $x = h$ is a solution of (3.1). Obviously all integers congruent to $h \pmod m$ also satisfy (3.1). Hence they are, by definition, all solutions of the congruence, but these congruent solutions are not considered as distinct or different solutions. They are considered to constitute a single solution which is written as

$$x \equiv r \pmod m \tag{3.2}$$

where r is the least residue of $h \pmod m$. Obviously (3.2) covers all integers congruent to $h \pmod m$.

Example: 3.1.2. *Solve the congruence*

$$6x \equiv 3 \pmod 9$$

All the distinct solutions of the given congruence lie in $S = \{0, 1, 2, \ldots, 8\}$. We shall then find out which of these numbers satisfy given congruence. Thus modulo 9 we have:

$6 \times 0 \equiv 0, \quad 6 \times 1 \equiv 6, \quad 6 \times 2 \equiv 3\,, \quad 6 \times 3 \equiv 0,$

$6 \times 4 \equiv 6, \quad 6 \times 5 \equiv 3, \quad 6 \times 6 \equiv 0, \quad 6 \times 7 \equiv 6, \quad 6 \times 8 \equiv 3.$

Therefore x =2, 5, 8 satisfy given congruence.

Hence we write the solution as $x \equiv 2,5,8 \pmod{9}$.

Theorem 3.1.3. *The congruence*

$$ax \equiv b \pmod{m}, \quad (a,m) = 1 \tag{3.3}$$

has only one solution.

Proof. We know that all the incongruent solutions of (3.3) lie in the complete system $S = \{0,1,2,...,m-1\}$. Therefore there are as many solutions of given congruence as there are integers in $S_1 = \{a \times 0, a \times 1, a \times 2, \ldots, a \times (m-1)\}$ which are congruent to b modulo m. Now S i a complete system $\pmod{m}$ and $(a,m) = 1$. Hence S_1 is also a complete system $\pmod{m}$. It follows that there exists one and only one integer say ax_0 in S_1 such that $ax_0 \equiv b \pmod{m}$. This implies that there is one and only one solution, namely, $x \equiv x_0 \pmod{m}$. □

The above theorem can be put in an alternative form which will be found to be often very useful.

Theorem 3.1.4. *Let $(a,m) = 1$, and let b be any given integer. Then there exists a unique integer say x_0 in $\{0,1,\ldots,m-1\}$ such that $ax_0 \equiv b \pmod{m}$*

Note: We shall now consider the solution of the linear congruence in its general form

$$ax \equiv b \pmod{m}$$

where m does not divide a. Then we shall prove that given congruence is not solvable if d does not divide b.

Theorem 3.1.5. *The congruence*

$$ax \equiv b \pmod{m}, \quad (a,m) = d \tag{3.4}$$

is solvable only if d divides b.

Proof. Let (3.4) be solvable. Then there exists an integer x_0 such that $ax_0 \equiv b \pmod{m}$. This implies

$$ax_0 - b = mq_0 \tag{3.5}$$

for some integer x_0. Now we know that d divides a and m. It immediately follows from (3.5) that d divides b. □

Definition 3.1.6. Two congruences are said to be **equivalent** if they are satisfied by the same values of the variables.

Consider the congruence

$$ax_0 \equiv b \pmod{m} \quad (a,m) = d \tag{3.6}$$

where d divides b. Dividing throughout by d we obtain the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{3.7}$$

where $(\frac{a}{d}, \frac{m}{d}) = 1$. We shall show that both the congruences are equivalent.

1. Let $x = x_0$ satisfy (3.6). This implies $ax_0 \equiv b \pmod{m}$. It follows that $\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. Hence $x = x_0$ satisfies (3.7).

2. Let $x = x_0$ satisfy (3.7).Then

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Multiply by d we get $ax_0 \equiv b \pmod{m}$. This proves that $x = x_0$ satisfy (3.6). Thus the same value of x satisfy (3.6) and (3.7). Therefore the two congruence are equivalent.

3.2 Application: Check digits and the ISBN system

Congruences are frequently used to provide an efficient way to detect errors in data transmission. Suppose that we have a sequence of nine-digit numbers that we need to enter into a computer. It is important that the data be entered correctly, but the quantity of numbers to be entered is large enough that we prefer not to double-check them. Instead, we add a tenth digit, called a "**check digit**," to each number that will detect some of our errors. If our nine-digit number is $x_1x_2...x_9$ we define the tenth digit x_{10} to be the number that satisfies

$$x_{10} \equiv (x_1 + x_2 + \cdots + x_9) \pmod{10}$$

We ask the computer to alert us any time we enter a ten-digit number that does not satisfy the above congruence. Notice that if we take a ten-digit number $x_1x_2...x_{10}$ that satisfies the congruence and replace exactly one digit with a different digit, then the resulting number no longer satisfies the congruence. Thus, our tenth digit detects an error when we have typed exactly one digit incorrectly. Obviously, this will not catch all of our errors, but we only needed to enter one extra digit rather than retype all nine digits.

The **ISBN (International Standard Book Number)** scheme employs a slightly more sophisticated check digit. The ISBN of a book is a 10-digit number grouped into four blocks of numbers. For example, the ISBN for the fourth edition of *The Mathematica Book* [34] is 0-521-64314-7. The first block is determined by the country of publication. For books published in the U.S., U.K., Australia, New Zealand, or Canada, this number is 0. The second block indicates the publisher. Any book that has a 521 as its second block is published by Cambridge University Press. The third block of the ISBN identifies the title and edition of the book. The final block is the check digit. If $x_1x_2,...,29$ are the first nine digits of an ISBN, then the check digit is the number x_{10} satisfying

$$x_{10} \equiv \sum_{i=1}^{9} ix_i \pmod{11}.$$

In the case $x_{10} = 10$, the character X is used as the tenth digit.) Let's perform this calculation for the check digit of *The Mathematica Book.*

$$1 \cdot 0 + 2 \cdot 5 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 6 + 6 \cdot 4 + 7 \cdot 3 + 8 \cdot 1 + 9 \cdot 4 \equiv 7 \pmod{11}$$

The check digit of an ISBN detects not only errors in which one digit has been incorrectly entered, but also errors in which two digits have been inter- changed. Certainly, these would be very typical kinds of errors if the numbers are entered by hand. Let's see what happens when we make errors of these two types. First, consider the number 0-521-64714-7 obtained from the ISBN of *The Mathematica Book* by changing the seventh digit from a 3 to 7.

$$1 \cdot 0 + 2 \cdot 5 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 6 + 6 \cdot 4 + 7 \cdot 7 + 8 \cdot 1 + 9 \cdot 4 \equiv 2 \pmod{11}$$

The check digit formula produces a 2 instead of 7. If we swap the third and fourth digits (in the original ISBN) we obtain the number 0-512-64314-7.

$$1 \cdot 0 + 2 \cdot 5 + 3 \cdot 1 + 4 \cdot 2 + 5 \cdot 6 + 6 \cdot 4 + 7 \cdot 3 + 8 \cdot 1 + 9 \cdot 4 \equiv 8 \pmod{11}$$

Again, the congruence defining the check digit produces a number other than 7. This will always happen for these types of errors.

Proposition 3.2.1. *If $x_1x_2 \ldots x_{10}$ is a valid ISBN and the number $x'_1x'_2 \ldots x'_{10}$ is obtained from that number by either altering exactly one digit interchanging two unequal digits, then*

$$x'_{10} \not\equiv \sum_{i=1}^{9} ix'_i \pmod{11}$$

Proof. In a valid ISBN,

$$\sum_{i=1}^{10} ix_i \equiv 0(mod 11).$$

We will prove that

$$\sum_{i=1}^{10} ix'_i \not\equiv 0(mod 11).$$

Suppose that we have an error of the first type; say, $x_j \neq x'_j$ for some j. Then
$\sum_{i=1}^{10} ix'_i \equiv \sum_{i=1}^{10} ix_i - jx_j + jx'_j \pmod{11} \equiv j(x'_j - x_j) \pmod{11}$
Since $j(x'_j - x_j)$ is not divisible by 11, we have proved that the required congruence fails.
Now suppose that we have an error of second type, i.e.,$x'_j = x_k$ and $x'_k = x_j$ for some $k \neq j$ and $x_j \neq x_k$. Then

$\sum_{i=1}^{10} ix'_i \equiv (\sum_{i=1}^{10} ix_i) + jx_k - jx_j + kx_j - kx_k \pmod{11} \equiv (k-j)(x_j - x_k) \pmod{11}$.
Then integers $k - j$ and $x_J - x_k$ are non-zero and have absolute less value than 10.
In particular, neither is divisible by 11, and so their product id not divisible by 11. □

In this section we shall be concerned with properties of positive integers only. We first prove the following theorem.

Theorem 3.2.2. *Let p be a prime. Then* $\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r'}$ $0 < t < p$, *is divisible by* p.

Proof. $p(p-1)\cdots(p-r+1)$ is the product of r consecutive integers, hence divisible by $r!$. But $r!$ is relatively prime to p. It follows that $r!$ divides $(p-1)(p-2)\cdots(p-r+1)$. This implies

$$\frac{p(p-1)(p-2)\cdots(p-r+1)}{r!}$$

is a multiple of p. □

Theorem 3.2.3. *If p is a prime then* $(a+b)^p \equiv a^p + b^p (mod\ p)$.

Proof. $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p +$ terms divisible by p. By previous theorem it follows that $(a+b)^p \equiv a^p + b^p (mod\ p)$. □

By successive application of the last theorem we can prove the following theorem.

Theorem 3.2.4. $(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p (mod\ p)$.

Proof.

$$\begin{aligned}(a_1+a_2+\cdots+a_n)^p &\equiv a_1^p+(a_2+a_3+\cdots+a_n)^p(mod\ p)\\ &\equiv a_1^p+a_2^p+(a_3+a_4+\cdots+a_n)^p(modp).\\ &.\\ &.\\ &\equiv a_1^p+a_2^p+\cdots+a_n^p(mod\ p)\end{aligned}$$

□

3.3 Fermat's Theorem

This last theorem enables us to prove one of the most famous and beautiful results in the whole field of number theory. This is known as *Fermat's Theorem.* This discovery of Fermat was found (1640) among his notes written in the margin of a book by Bachet on number theory. It was Fermat's practice not to disclose the proof of the theorems he discovered. So, the theorem remained without proof for a long time, nearly a century, till the great Euler broke the ice and gave two proofs of the same. He was also able to generalize the theorem in terms of a new function $\phi(n)$ discovered by himself.

Theorem 3.3.1. *Let p be a prime,* $(a,p)=1$. *Then* $a^{p-1}-1$ *is divisible by* p.

Proof. we have $(x_1+x_2+\cdots+x_n)^p \equiv x_1^p+x_2^p+\cdots+x_a^p \pmod{p}$.
Letting $x_1=x_2=\cdots=x_a=1$ we obtain

$$a^p \equiv a(modp).$$

But $(a, p) = 1$. Therefore we can cancel the common factor a from the two sides of the congruence. So we get $a^{p-1} \equiv 1 \pmod{p}$ which implies $a^{p-1} - 1 \equiv 0 \pmod{p}$. The theorem is therefore proved.

There are many ways in which Fermat's Theorem can be proved. However, the proof given above is probably the simplest. □

Euler generalized Fermat's theorem in terms of the ϕ function. He proved that $a^{\phi(m)} \equiv 1 \pmod{m}$ if $(a,m) = 1$. We shall prove this result in the next section after establishing the property of primes.

Theorem 3.3.2. *If p is a prime and* $(a, p) = 1$ *then*

$$a^{\phi(p^b)} \equiv 1(mod\ p^b).$$

Proof. By Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$. Raising both sides of this congruence to the power p^{b-1} we obtain

$$\begin{aligned}(a^{p-1})^{p^{b-1}} &\equiv 1(mod\ p^{1+b-1})\\ &\equiv 1(mod\ p^b)\end{aligned}$$

But

$$\begin{aligned}(a^{p-1})^{p^{b-1}} &= a^{p^{b-1}}(p-1)\\ &= a^{p^b - p^{b-1}}\\ &= a^{p^b - p^{b-1}}\\ &= a^{\phi(p^b)}.\end{aligned}$$

It follows that $a^{\phi(r^b)} \equiv 1 \pmod{p^b}$. □

3.4 Euler's Theorem

Theorem 3.4.1. *Let* $(a,m) = 1$. *Then* $a^{\phi(m)} \equiv 1 \pmod{m}$..

Proof. If $m = 1, \phi(m) = 1$ and the theorem is true. Suppose now $m \neq 1$. Let $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the canonical decomposition of m. Then obviously $\phi(p_1^{a_1})$ divides $\phi(m)$.

(Recall that $\phi(m)$ is multiplicative). Now

$$a^{\phi(p^{a_1})} \equiv 1(mod\ p_1^{a_1}).$$

Raising both sides of this congruence to the power $\frac{\phi(m)}{\phi(p_1^{\sigma_1})}$ we obtain

$$a^{\phi(m)} \equiv 1(mod\ p_1^{a_1})$$

Similarly we can prove

$$a^{\phi(m)} \equiv 1(mod\ p_2^{a_2})$$

$$.$$

$$.$$

$$a^{\phi(m)} \equiv 1(mod\ p_k^{a_k})$$

It follows that

$$\begin{aligned} a^{\phi(m)} &\equiv 1(mod[p_1^{a_1}, p_2^{a_2}, ..., p_k^{a_k}]) \\ &\equiv 1 \pmod{m}. \end{aligned}$$

□

Note that the above theorem is known as **Fermat-Euler Theorem**. Fermat's Theorem is very useful in calculating the residues of numbers whose exponents are large.

Example: 3.4.2. *Find the remainder when* 72^{1001} *is divided by 31.*
$72 \equiv 10 \pmod{31}$. *Hence* $72^{1001} \equiv 10^{1001} \pmod{31}$. *Now* $(10,31) = 1$ *and* 31 *is a prime. It follows that*

$$10^{30} \equiv 1 \pmod{31}$$

. *Raising both sides to the power* 33 *we obtain*

$$10^{990} \equiv 1 \quad (\text{mod } 31.)$$

Also

$$10^2 \equiv 7 \pmod{31}.$$

$$10^4 \equiv -13 \pmod{31}.$$

$$10^8 \equiv 14 \pmod{31}.$$

Therefore

$$\begin{aligned} 72^{1001} &\equiv 10^{1001} \pmod{31} \\ &\equiv 10^{990} \times 10^{8} \times 10^{2} \times 10 \pmod{31} \\ &\equiv 1 \times 14 \times 7 \times 10 \pmod{31} \\ &\equiv 5 \times 10 \pmod{31} \\ &\equiv 19 \pmod{31}. \end{aligned}$$

Hence the required remainder is 19.

Example: 3.4.3. *Find the least residue of* $7^{973} \pmod{72}$.

Solution *:* $(7,72) = 1$. *Hence* $7^{\phi(72)} \equiv 1 \pmod{72}$*, that is,*

$$7^{24} \equiv 1 \pmod{72}$$

Consequently

$$7^{960} \equiv 1 \pmod{72}..$$

Again we have

$$\begin{aligned} 7^2 &\equiv -23 \pmod{72}. \\ 7^4 &\equiv 25 \pmod{72}. \\ 7^8 &\equiv -23 \pmod{72}. \end{aligned}$$

Hence

$$\begin{aligned}
7^{973} &= 7^{960} \times 7^{8} \times 7^{4} \times 7 \\
&\equiv 1 \times (-23) \times 25 \times 7 \pmod{72} \\
&\equiv (-23) \times 31 \pmod{72} \\
&\equiv 7 \pmod{72}.
\end{aligned}$$

Chapter 4

IDENTICAL CONGRUENCES

4.1 Introduction

In algebra we use the equality symbol in two different senses. For example consider the following

$$x^2 + 12 = 7x \tag{4.1}$$

$$x^2 - 7x + 12 = (x - 3)(x - 4) \tag{4.2}$$

(4.1) is called **an equation**. It is an equality between two numbers. This happens only when $x = 3$ or $x = 4$

When $x = 3$ the equality is between 21 and 21 and

when $x = 4$, between 28 and 28.

On the other hand (4.2) is called **an identity**. Here the equality is between two algebraic expressions. The coefficient of each term on the left side of the equality symbol is equal to the coefficient of the term of the same degree on the right side. The equality therefore holds good for all values of x. In like manner, in number theory the congruence symbol is used in two different senses. When we say, for example, that $x^2+2x \equiv 1 \pmod 7$ *it is an ordinary congruence, that is, a congruence between two numbers.* The congruence holds good only when $x \equiv 1,4 \pmod 7$. When $x=1$ the congruence is between 3 and 10 and when $x=4$, it is between 24 and 10 modulo 7. On the other hand consider

$$6x^2+7x+9 \equiv x^2+2x+4(mod 5).$$

This is called an *identical congruence*. Here the congruence is between two algebraic expressions. The coefficient of each term on the left side of the congruence symbol is congruent $\pmod 5$ to the coefficient of the term of the same degree on the right side. Thus

$$6x^2 \equiv x^2, \quad 7x \equiv 2x, \quad 9 \equiv 4 \pmod 5.$$

Therefore the congruence holds good for all values of x. It is usual to write the same congruence symbol for the two types of congruence.

Definition 4.1.1. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

be two integral polynomials of degree n. If $a_i \equiv b_i \pmod{m}$ for $i = 0, 1, ..., n$ then $f(x)$ is said to be **identically congruent** to $g(x)$ modulo m and we write this as $f(x) \equiv g(x) \pmod{m}$ identically.

Throughout this section we assume hence forward that

i. $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

ii. n is less than the modulus in the congruence $f(x) \equiv 0 \pmod{p}$.

Theorem 4.1.2. *If b is a solution of*

$$f(x) \equiv 0 \pmod{m} \tag{4.3}$$

then

$$f(x) \equiv (x-b)h(x) \pmod{m}$$

identically where $h(x)$ *is a polynomial of degree* $(n-1)$.

Proof. We have $f(b) \equiv 0 \pmod{m}$. Hence

$$\begin{aligned} f(x) &\equiv f(x) - f(b) \pmod{m} \\ &\equiv a_n(x^n - b^n) + a_{n-1}(x^{n-1} - b^{n-1}) + \cdots + a_1(x-b) \pmod{m} \\ &\equiv (x-b)h(x) \pmod{m} \end{aligned}$$

where $h(x)$ is a polynomial of degree $n-1$. □

The following theorem is the converse of the last.

Theorem 4.1.3. *If $(x-b)$ divides $f(x) \pmod{m}$ then b is a solution of $f(x) \equiv 0 \pmod{m}$.*

Proof. Since $(x-b)$ divides $f(x)$ modulo m it follows that

$$f(x) \equiv (x-b)h(x) \pmod{m}$$

where $h(x)$ is some polynomial. Therefore

$$f(b) \equiv (b-b)h(b) \pmod{m} \equiv 0 \pmod{m}.$$

This proves the theorem. □

Theorem 4.1.4. *Every congruence*

$$f(x) \equiv 0 \pmod{p} \tag{4.4}$$

of degree $n < p$ can have at most n incongruent solutions unless $f(x)$ is identically congruent to zero $\pmod{p}$.

Proof. If possible let (4.4) have $n+1$ incongruent solutions say $b_1, ..., b_{n+1}$. Then considering the first n solutions and we have

$$f(x) \equiv a_n(x-b_1)(x-b_2)\cdots(x-b_n) \pmod{p} \tag{4.5}$$

identically. But since b_{n+1} is a solution of (4.4),

$$f(b_{n+1}) \equiv 0(mod p).$$

Hence

$$a_n(b_{n+1}-b_1)(b_{n+1}-b_2)\cdots(b_{n+1}-b_n) \equiv 0 \pmod{p}. \tag{4.6}$$

But p does not divide $(b_{n+1}-b_1),(b_{n+1}-b_2),(b_{n+1}-b_n)$. Hence p divides a_n. So $a_n \equiv 0 \pmod{p}$. The theorem at once (4.5) above. □

Theorem 4.1.5. *Every congruence $f(x) \equiv 0 \pmod{p}$ of degree $n < p$ can have at most n incongruent solutions $f(x) \equiv 0 \pmod{p}$ identically.*

Proof. We consider that the given congruence is not identical. Then obviously the theorem holds good when $n = 1$. Let us then assume that the theorem is true when $n = S$. Consider the congruence

$$f(x) \equiv 0 \pmod{p}$$

where $f(x)$ is of degree $S+1$. Let C be one of its solutions. Then

$$f(x) \equiv (x-C)h(x) \pmod{p}$$

where $h(x)$ is of degree S. But we know that $x-C \equiv 0 \pmod{p}$ has only one solution and by our assumption $h(x) \equiv 0(modp)$ has at most S solutions. It follows that at most $S+1$ solutions. Thus the theorem is proved to be true when $n = S+1$.
The required result is established by induction. □

We know that $x^{p-1} - 1 \equiv 0(modp)$ has exactly $(p-1)$ solutions. Here the number of solutions is equal to the degree of the congruences. It is curious that this property is possessed by all divisors of $p-1$ as the following theorem will show:

Theorem 4.1.6. *Let d be a divisor of* $(p-1)$. *Then the congruence* $x^d \equiv 0(modp)$ *has exactly d solutions.*

Proof. d divides $(p-1)$, hence (x^d-1) divides $(x^{p-1}-1)$.
This implies

$$x^{p-1}-1=(x^4-1)h(x) \tag{4.7}$$

where $h(z)$ is a polynomial of degree $(p-1-d)$. We write identity (4.7) as an identical congruence $x^{p-1}-1 \equiv (x^d-1)h(x)modp)$.
Now, we know that $x^{p-1}-1 \equiv 0(modp)$ has exactly $p-1$ solutions, and $h(x) \equiv 0 \pmod p$ at most $p-1-d$ solutions. It follows that

$$x^d-1 \equiv 0 \pmod p \tag{4.8}$$

has at least $p-1-(p-1-d)=d$ solutions. But (4.8) cannot obviously have more than d solutions. Therefore it has exactly d solutions. □

4.2 Order of Integers

We begin the study of this topic with a simple theorem.

Theorem 4.2.1. *The congruence*

$$a^x \equiv 1 \pmod m \tag{4.9}$$

is solvable if and only if $(a,m)=1$

Proof.

1. Let $(a,m)=1$. Then by Fermat-Euler theorem we have $a^{\phi}(m)\equiv 1 \pmod m$. Thus there is at least one solution of (4.9) namely $x=\phi(m)$.
2. Let (4.9) be solvable. Then $a^{x_0}\equiv 1 \pmod m$ for some integer x_0. It follows that $(a^{x_0},m)=(1,m)=1$. This implies $(a,m)=1$.

□

Since the congruence $a^x\equiv 1 \pmod m$, $(a,m)=1$ has at least one solution $x=\phi(m)$ it follows that it has a positive solution. This may be $\phi(m)$ or some other smaller integer. This smallest solution is of special interest to us and is called *the exponent to which a belongs* $\pmod m$. This name was suggested by Gauss who was the first to study its properties. As the name is rather inconvenient to use we will have a simpler expression.

Definition 4.2.2. The smallest positive value of x which satisfies

$$a^x\equiv 1 \pmod m$$

is called the order of $a(modm)$. This number is usually denoted by the symbol d.

Obviously the order of 1 modulo any integer m is 1 because

$$1^1\equiv 11 \pmod m.$$

Hence we shall generally assume that $a>1$ in the following discussion. The statement that the order of $a(modm)$ is d implies

$$(a,m)=1$$

$$a^d \equiv 1 \pmod{m}$$

$$a^h \pmod{m}, 0 < h < d$$

Example: 4.2.3. *Find the order of* 3 *modulo* 16.

Solution: $3^2 \equiv 9$, $3^3 \equiv 11$ $3^4 \equiv 1$ *modulo* 16. *So the smallest exponent which satisfies* $3^x \equiv 1 \pmod 16$ *is* 4. *Therefore the order of* $3 \pmod{16}$ *is* 4.

Example: 4.2.4. *Find the orders* $\pmod{9}$ *of all positive integers less then prime to it.*

Solution*: The positive integers less than* 9 *and prime to it are* $1,3,4,5,7$ *and* 8. *Then we have* $l^1 \equiv 1 \pmod{7}$.

$$\begin{aligned}2^2 \equiv 4,\ 2^3 \equiv 8\ 2^4 \equiv 7\ 2^5 \equiv 5,\ 2^6 \equiv 1 &\pmod{9}\\ 4^2 \equiv 7,\ 4^3 \equiv 1 &\pmod{9}\\ 5^2 \equiv 7,\ 5^3 \equiv 8\ 5^5 \equiv 2,\ 5^6 \equiv 1 &\pmod{9}\\ 7^2 \equiv 4,\ 7^3 \equiv 1 &\pmod{9}\\ 8^2 \equiv 1 &\pmod{9}\end{aligned}$$

Hence the orders of $1,2,4.5,7,8 \pmod{9}$ *are* $1,6,3,6,3,2$*, respectively.*

Note that $\phi(9) = 6$ *So the orders of* 2 *and* 5 $\pmod{9}$ *are* $\phi(9)$. *Such numbers whose orders* $\pmod{m}$ *are* $\phi(m)$ *are called* ***primitive roots of m****. Thus the primitive roots of* 9 *are* 2 *and* 5.

Theorem 4.2.5. *If* $b \equiv a \pmod{m}$*, then* b *has the same order* $\pmod{m}$ *as* a.

Proof. Let the order of $a \pmod{m}$ be d. Then $a^d \equiv 1 \pmod{m}$, $(a,m) = 1$ $a^h \not\equiv 1 \pmod{m}$, $0 < h < d$. Now $b \equiv a \pmod{m}$. Hence $(b,m) = (a,m) = 1$, $b^d \equiv$

$a^d \equiv \pmod{m}$, $b^h \equiv a^h \not\equiv 1 \pmod{m}$ for $0 < h < d$. This implies that the order $b \pmod{m} = d$. □

Example: 4.2.6. *Find the order of* $43 \pmod{18}$.

***Solution**:* $43 \equiv 7 \pmod{18}$.

Hence the order of $43 \pmod{18}$ $=$*the order* $7 \pmod{18} = 3$

for, $7^2 \equiv 13$, $7^3 \equiv 1 \pmod{18}$.

Theorem 4.2.7. *Let the order of a* $\pmod{m}$ *be d. Then the integers*

$$a, a^2, \ldots, a^d$$

are incongruent $\pmod{m}$.

Proof. Let us assume that the theorem is not true. Then it follows that

$$a^i \equiv a^j \pmod{m} \tag{4.10}$$

for some i and j such that $0 < i < j \leq d$. Since $(am) = 1$ we can write (4.10)

$$a^{j-i} \equiv 1 \pmod{m} \tag{4.11}$$

where $j - i$ is a positive integer $< d$. But congruence (4.11) is impossible because d is the smallest integer x which satisfies $a^x \equiv 1 \pmod{m}$. Hence the theorem is true. □

Theorem 4.2.8. *Let* $a^h \equiv a^k \pmod{m}$. *Then* $h \equiv k \pmod{d}$ *where d is the order of a* $\pmod{m}$.

Proof. Let

$$h = dq_1 + r_1, \ 0 \leq r_1 < d$$

$$k = dq_2 + r_2, \ 0 \leq r_2 < d$$

Then $a^h = a^{dq_1+r_1} = (a^d)^{q_1} a^{r_1} \pmod{m}$ since $a^d \equiv 1 \pmod{m}$. Similarly we can prove $a^k \equiv a^{r_2} \pmod{m}$. But $a^h \equiv a^k \pmod{m}$. Therefore $a^{r_1} \equiv a^{r_2} \pmod{m}$. So, by previous theorem $r_1 = r_2$ which implies $h - k = d(q_1 - q_2)$. Hence $h \equiv k \pmod{d}$. □

The following theorem is very important and should be committed to memory. It is the principal tool for deducing several of the results in this and the following few sections.

Theorem 4.2.9. *Let the order of a* $\pmod{m}$ *be d, and let*

$$a^h \equiv 1 \pmod{m}$$

. Then $d|h$.

Proof. This is very easy after Theorem 4.2.8. We have $a^h \equiv 1 \equiv a^0 \pmod{m}$. It follows that $h \equiv 0 \pmod{d}$. Hence d divides h. □

Corollary 4.2.10. *Let the order of $a \pmod{m}$ be d. Then d divides $\phi(m)$.*

Proof. For, by Fermat-Euler theorem $a^{\phi(m)} \equiv 1 \pmod{m}$. So, d divides $\phi(m)$.

Thus we see that the order of a given integer $\pmod{m}$ is to be found only among the divisors of $\phi(m)$. □

Example: 4.2.11. *Find the order of* $5 \pmod{29}$.

Solution: $\phi(29) = 28 = 2^2x7$. *Hence the divisors of* $\phi(29)$ *are* $1, 2, 4, 7, 14,$ *and* 28. *Then we have modulo* 29

$$\begin{aligned} 5^2 \equiv -4, 5^4 &\equiv 16 \\ 5^7 \equiv 5^4 \times 5^2 \times 5 \equiv 16 \times (-4) \times 5 &\equiv -1 \\ 5^{14} &\equiv 1. \end{aligned}$$

Thus the order of $5 \pmod 2)9$ *is* 14.

If we know the order of $a \pmod{m}$ then the orders of $a^2, a^3, \ldots$ are easily determined.

Theorem 4.2.12. *Let the order of $a \pmod{m}$ be d. Then the order of*

$$a^k \pmod{m}$$

is $\frac{d}{(k,d)}$.

Proof. Let the order of $a^k \pmod{m} = h$ and let $(k,d) = c$. Then $\frac{k}{c}$ and $\frac{d}{c}$ are integers such that $(\frac{k}{c}, \frac{d}{c}) = 1$. Now $a^d \equiv 1 \pmod{m}$. Hence $(a^d)^{\frac{k}{c}} \equiv 1 \pmod{m}$. Therefore

$(a^k)^{\frac{d}{c}} \equiv 1 \pmod{m}$. It follows from Theorem 4.2.9 that

$$h \text{ divides } \tfrac{d}{c}$$

On the other hand $(a^k)^h \equiv 1 \pmod{m}$. Hence $a^{kh} \equiv 1 \pmod{m}$. So,$d$divides kh or $\frac{d}{c}$ divides $\frac{k}{c}h$. But $(\frac{d}{c}, \frac{k}{c}) = 1$. Therefore

$$\tfrac{d}{c} \text{ divides } h.$$

h = d/c = d/(k, d) Then it imply that $h = \frac{d}{c} = \frac{d}{(k,d)}$. □

Example: 4.2.13. *Find the order* $2^4 \pmod{17}$.

Solution*: Order of* $2 \pmod{17} = 18$. *Hence the order of* $2^4 \pmod{17}$ *is* $\frac{4}{(4,8)} = 2$.

A special case of the last theorem is important.

Theorem 4.2.14. *Let the order of* $a \pmod{m}$ *be* d. *Then the order of* $a^k \pmod{m}$ *is* d *if and only if* $(k,d) = 1$.

Proof. Clearly, $\frac{k}{(k,d)}$, the order of $a^k \pmod{m}$, is equal to d if and only if $(k,d) = 1$. □

4.3 Primitive Roots

In the last section we introduced the concept of the order of integers $\pmod{m}$. Here we continue to discuss the same topic but focus our attention on those whose order $\pmod{m}$ is $\phi(m)$.

Definition 4.3.1. If the order of $a \pmod{m}$ is $\phi(m)$ then a is called a primitive root of m, or a primitive root $\pmod{m}$.

Thus the statement that a is a primitive root of m implies

$$(a,m) = 1$$

.

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$a^h \not\equiv 1 \pmod{m}, 0 < h < \phi(m)$$

.

Example: 4.3.2. *Show that* 2 *is a primitive root of* 11.

Solution: *If* $a^d \equiv 1 \pmod{11}$ *then* d *divides* $\phi(11)$.

The divisors of $\phi(11) = 10$ *are* $2, 5$, *and* 10.

We then find $2^2 \equiv 4$, $2^5 \equiv -1$, $2^{10} \equiv 1 \pmod{11}$. *So the smallest integer* x *which satisfies* $2^x \equiv 1 \pmod{11}$ *is* 10. *This implies* 2 *is a primitive root of* 11.

Example: 4.3.3. *Show that* 5 *is a primitive root of* 18.

Solution: $\phi(18) = 6 = 2 \times 3$. *Hence the divisors of* $\phi(18)$ *are* $2, 3$, *and* 6.

$5^2 \equiv 7$, $5^3 \equiv -1$, $5^6 \equiv 1 \pmod{18}$. *It follows that* 5 *is a primitive root of* 18.

The following theorem indicates the general method of finding the primitive roots of any given modulus.

Theorem 4.3.4. *Let* $(a,m) = 1$ *then a is a primitive root of m if and only if*

$$a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod{m}$$

for every prime divisor p of $\phi(m)$.

Proof. Let a be such that

$$a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod{p}$$

for every prime divisor p of $\phi(m)$. Let us assume that under this condition a is not a primitive root of m. Then it follows that the order of $a \pmod{m}$ is some integer k less than $\phi(m)$. This implies that k divides $\phi(m)$. Thus $\frac{\phi(m)}{k}$ is an integer and is therefore divisible by some prime divisor p of $\phi(m)$. Hence

$$a^{\frac{\phi(m)}{p}} = (a^k)^{\frac{\phi(m)}{kp}} \equiv 1 \pmod{m}$$

because $a^k \equiv 1 \pmod{m}$. This contradicts above. So, our assumption is untenable and therefore a is a primitive root of m.

Let a be primitive root of m. Then it follows that

$$a^{\phi}(m) \equiv 1 \pmod{m}$$

and

$$a^h \not\equiv 1 \pmod{m}, 0 < h < \phi(m)$$

. This means that $a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod{p}$ for every prime divisor p of $\phi(m)$. □

Theorem 4.3.5. *Let g be a primitive root of m, and let*

$$g_1 \equiv g \pmod{m}.$$

Then g_1 is also a primitive root of m.

Proof. The order of $g \pmod{m}$ is $\phi(m)$. Hence the order of $g_1 \pmod{m}$ is $\phi(m)$. This implies g_1 is a primitive root of m. □

The usefulness of the concept of primitive roots arises chiefly from the following theorem.

Theorem 4.3.6. *Let g be a primitive root of m. Then the set*

$$S = \{g, g^2, \ldots, g^\phi(m)\}$$

is a reduced system $\pmod{m}$.

Proof. (1) There are $\phi(m)$ integers in S. Now $(g,m) = 1$. Hence

(2) the integers of S are all relatively prime to m.. The order of $g \pmod{m}$ is $\phi(m)$. Therefore

(3) the integers $g, g^2, \ldots, g^\phi(m)$ are all incongruent $\pmod{m}$.

It follows from (1), (2) and (3) that S is a reduced system $\pmod{m}$. □

Since $g^\phi(m) \equiv 1 \pmod{m}$ we have the following obvious corollary.

Corollary 4.3.7. *If g is a primitive root of m then the set $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ is a reduced system* $\pmod{m}$.

Chapter 5

QUADRATIC CONGRUENCES

5.1 Quadratic Congruences

The general form of a quadratic congruence in one variable is

$$Ax^2+Bx+C\equiv 0 \pmod{m} \tag{5.1}$$

Where A is not divisible by m.

To solve this congruence there exists no general and direct method unlike the case of linear congruence. However we are able to penetrate fairly deep into the problem. Thanks mainly to the researches of Euler, Legendre, Jacobi, and above all, Gauss. The first step in the solution of congruence (5.1) is to bring it to simpler form.

The following theorem shows that this is always possible when $(2A,m)=1$.

Theorem 5.1.1. *The congruence*

$$Ay^2 + By + C \equiv 0 \pmod{m}, (2A, m) = 1$$

can be reduced to the form $x^2 \equiv a \pmod{m}$.

Proof. Multiplying (5.1) by $4A$ we obtain

$$4A^2y^2 + 4ABy + 4AC \equiv 0 \pmod{m}.$$

This can be written as

$$(2Ay + B)^2 \equiv B^2 - 4AC \pmod{m} \tag{5.2}$$

If we set

$$x \equiv 2Ay + B \pmod{m}$$
$$a \equiv B^2 - 4AC \pmod{m}$$

then (5.2) is reduced to the required form

$$x^2 \equiv a \pmod{m}. \tag{5.3}$$

Suppose now that $x = x_0$ satisfies (5.3). Then we have

$$2Ay + B \equiv x_0 \pmod{m} \tag{5.4}$$

This congruence which enables us to find the values of y satisfying (5.1) is solvable since $(2A,m)=1$.

This completes the proof of the theorem. □

Example: 5.1.2. *Solve the congruence* $3y^2+5y+9\equiv 0 \pmod{11}$

Solution: *Here* $(2\times 3,11)=1$. *Hence the required condition is satisfied.*

Multiplying the congruence by $4\times 3=12$, *we obtain*

$$36y^2+60y+108\equiv 0 \pmod{11}$$

This reduces to

$$(6y+5)^2\equiv 5 \pmod{11}$$

If we put

$$x\equiv 6y+5 \pmod{11}$$

the given congruence transformed to

$$x^2\equiv 5 \pmod{11}.$$

The solutions of this by the method of trial are

$$x\equiv \pm 4 \pmod{11}.$$

It follows that

$$6y+5\equiv \pm 4 \pmod{11}$$

This gives the solutions of the given congruence as

$$y \equiv 4, 9 \pmod{11}.$$

The condition in last theorem that $2A$ should be relatively prime to m is always satisfied if m is an odd prime p unless p divides A. The following theorem is therefore an immediate consequence.

In what follows p is supposed to be an odd prime.

Theorem 5.1.3. *If the congruence*

$$x^2 \equiv a \pmod{p}, (a, p) = 1 \tag{5.5}$$

is solvable then it has exactly two solutions.

Proof. Let $x = x_0$ be a least solution of (5.5). Then we have $x_0^2 \equiv a \pmod{p}$.

It follows that

$$(p - x_0)^2 \equiv x_0^2 \equiv a \pmod{p}.$$

Hence $x = p - x_0$ is another least solution of (5.1).

Also x_0 and $p - x_0$ are incongruent $\pmod{p}$ for their difference $p - 2x_0$ is not divisible by p.

Thus there exist two incongruent solutions of (5.5) namely

$$x \equiv x_0, p - x_0 \pmod{p}.$$

But we know congruence (5.5) cannot have more than two solutions because it is of degree 2.

Let x_1 be a third solution other than x_0 and $p-x_0$. Then we have

$$x_1^2 \equiv a \pmod{p}$$
$$x_0^2 \equiv a \pmod{p}$$

Hence

$$x_1^2 \equiv x_0^2 \pmod{p}$$

$\Longrightarrow$ $(x_1-x_0)(x_1+x_0)$ is divisible by p.

It follows that either p divides (x_1-x_0) or p divides (x_1+x_0).

In the first case $x_1 \equiv x_0 \pmod{p}$ and in the

second case $x_1 \equiv p-x_0 \pmod{p}$

Thus it is seen that x_1 is not a distinct solution. So, Congruence (5.5) cannot have more than two solutions. □

Theorem 5.1.4. *Let* $(a,p)=1$, *then either*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad or \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Proof. By Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$. Hence

$$(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p}.$$

Therefore p divides either $a^{\frac{p-1}{2}}-1$ or $a^{\frac{p-1}{2}}+1$; it cannot divide both since in that case

$$(a^{\frac{p-1}{2}}+1)-(a^{\frac{p-1}{2}}-1)=2$$

would be divisible by p, which is impossible. This proves the theorem. □

Theorem 5.1.5. *The congruence*

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \tag{5.6}$$

has exactly $\frac{p-1}{2}$ *solutions namely* $x \equiv 1^2, 2^2, \ldots, (\frac{p-1}{2})^2 \pmod{p}$.

Proof. Let

$$S=\{1^2,2^2,\ldots,(\frac{p-1}{2})^2\}.$$

If t^2 is any integer of S, then $(t,p)=1$ so that by Fermat's theorem we have

$$t^{p-1} \equiv 1 \pmod{p}$$

which can be written as $(t^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Thus

$$\text{every integer of } S \text{ is a solution of (5.6)} \tag{5.7}$$

Also

$$\text{the integers of } S \text{ are all incongruent (mod p)} \tag{5.8}$$

For, if $u^2 \equiv v^2 \pmod{p}$. such that $1 \le u \le v \le \frac{p-1}{2}$ then it would follow that $(u-v)(u+v)$would be divisible by p. But this is impossible since both $(u-v)$ and

$(u+v)$ are numerically less than p. Moreover $\frac{p-1}{2}$ divides $p-1$.

Therefore (5.6) has exactly $\frac{p-1}{2}$ solutions.

Hence the proof. □

Example: 5.1.6. *19 is a prime and* $\frac{19-1}{2} = 9$. *Hence* $x^9 \equiv 1 \pmod 9$ *has exactly 9 solutions, namely*

$$\begin{aligned} x &\equiv 1^2, 2^2, \ldots, 9^2 \pmod{19} \\ &\equiv 1, 4, 9, 16, 6, 17, 11, 7, 5 \pmod{19}. \end{aligned}$$

Theorem 5.1.7. ***Euler's Criterion***

The congruence

$$x^2 \equiv a \pmod p, (a,p) = 1 \tag{5.9}$$

has a solution if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Proof. Let $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Then obviously a is a solution of

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p$$

.

Therefore a is congruent $\pmod p$ to one of the integers $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

Let this integer be t^2. This means $t^2 \equiv a \pmod p$. Therefore $x = t$ is a solution of (5.9).

Conversely, Let congruence (5.9) have a solution say, $x \equiv b \pmod p$.

It follows that $b^2 \equiv a \pmod p$. Hence

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \pmod p \equiv 1 \pmod p$$

by Fermat's theorem, since $(b,p)=1$.

This completes the proof. □

The following is the complementary part of Euler's Criterion.

Theorem 5.1.8.

$$x^2 \equiv a \pmod{p}, (a,p)=1 \tag{5.10}$$

has no solution if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Proof. (i) Let $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Then it follows that $a^{\frac{p-1}{2}} \not\equiv 1 (mod\ p)$. Therefore we conclude that (5.10) has no solution.

(ii) Let (5.10) be not solvable. Then it follows that $a^{\frac{p-1}{2}} \not\equiv 1 (modp)$. So we have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

□

Corollary 5.1.9. *If* $(a,p)=1$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

Proof. There are only two possibilities. The congruence $x^2 \equiv a \pmod{p}$ has a solution or has no solution.

In the first case we have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and in the second case we have

$$a^{\frac{p-1}{2}} \equiv -1(mod\ p).$$

It follows that in either case $a^{p-1} = 1 \pmod{p}$. □

5.2 Quadratic Residues

In this section we continue the discussion of quadratic congruences, but here we approach the subject from a slightly different angle. In what follows it should be remembered that p is an odd prime.

Definition 5.2.1. Let (a,p)=1 Then

1. If $x^2 \equiv a \pmod{p}$ is solvable, we call 'a' a **quadratic residue** of p, or a quadratic residue of $\pmod{p}$..
2. If $x^2 \equiv a \pmod{p}$ is not solvable, we call 'a' a **quadratic non-residue** of p.

The definition given above implies that a is a quadratic residue of p if and only if

1. $(a,p) = 1$
2. a is congruent $\pmod{p}$ to some square integer.

Example: 5.2.2. *(1) 5 is a quadratic residue of 29 because* $(5,29) = 1$ *and* $(\pm 11)^2 \equiv 5(mod 29)$.

(2) $x^2 \equiv 3 \pmod 7$ *has no solution, hence 3 is a quadratic non-residue of 7.*

(3) 1 is a quadratic residue of every p because $x^2 \equiv 1 \pmod 7$ *is always solvable.*

Theorem 5.2.3. *Let* $a \equiv b(modp)$. *If a is a quadratic residue of p then b is also a quadratic residue of p.*

Proof. a is a quadratic residue of p. $x^2 \equiv a \pmod p$ is solvable. But a $\pmod p$. Hence $x^2 \equiv b \pmod p$ is also solvable. This implies that b is a quadratic residue of p. □

In view of what has been proved above we will consider a and b as the same quadratic residue of p, if $a \equiv b \pmod p$. Thus two quadratic residues of p are distinct if and only if they are incongruent $\pmod p$. It follows that all the distinct quadratic residues of p lie in any reduced system $\pmod p$. Usually by quadratic residues of p we will mean those which lie in the reduced system $R = \{1, 2, ..., p-1\}$. But those which lie outside R may also be referred to as residues of p and if any distinction is necessary the former will be called least quadratic residues of p.

What has been proved and discussed in the last section applies equally well to quadratic non-residues of p. We only state the theorem.

Theorem 5.2.4. *Let* $a \equiv b \pmod p$. *If a is a quadratic non-residue of p, then b is also a quadratic non-residue of p.*

The following theorem shows how to find the quadratic residues of any given p.

Theorem 5.2.5. *p has exactly* $\frac{p-1}{2}$ *incongruent quadratic residues namely*

$$1^2, 2^2, ..., (\frac{p-1}{2})^2 \tag{5.11}$$

Proof. Every square number relatively prime to p is a quadratic residues of p. It follows that integers (5.11) are all quadratic residues of p. Moreover it has been proved that these quadratic residues are all incongruent $\pmod p$.

It remains to prove that there are no more quadratic residues of p. Suppose b is a quadratic residues of p outside the integers (5.11). Then by definition there exists an integer c such that

$$b \equiv c^2 \pmod p, 0 \leq c \leq p-1.$$

This implies

$$b \equiv c^2 \equiv (p-c)^2 \pmod p$$

.But evidently either c^2 or $(p-c)^2$ is included among the numbers (5.11). It follows that b is not a new quadratic residue of p. □

Example: 5.2.6. *Find all the quadratic residue of 29.*

Solution: $p = 29$ *and* $\frac{p-1}{2} = 14$.

Hence the quadratic residues of 29 *are* $1^2, 2^2, ..., 14^2$ *the residues of these number* (mod 29) *and arranging them in ascending order, the quadratic residues of* 29 *are* $1, 4, 5, 67, 9, 13, 16, 20, 22, 23, 24, 25, 28$.

Table of quadratic residues

p	Quadratic residues
3	1
5	1,4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 5, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16
19	1, 4, 5, 6, 7, 9, 11, 16, 17
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28
31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36

Theorem 5.2.7. *Every odd prime p has exactly $\frac{p-1}{2}$ quadratic non-residues.*

Proof. Any given integer is either a quadratic residue of p or a non-residue.

Hence the least quadratic residues and non-residues of p together form a reduced system

$S = \{1, 2, ..., p-1\}$modulo p.

But $\frac{p-1}{2}$ integers of S are quadratic residues of p.

It follows that the remaining integers of S are non-residues. □

Example: 5.2.8. *Find the least quadratic non-residues of* 17.

Solution: *The least quadratic residues of* 17 *are* $1,2,4,8,9,13,15,16$.

Deleting these integers from $\{1,2,...,16\}$ *we find that the non-residues of* 17 *are* $3,5,6,7,10,11,12,14$.

There is a close relation between the quadratic residues of p and its primitive roots.

Theorem 5.2.9. *Let g be a primitive root of p. Then the quadratic residues of*

$$g^2, g^4, ..., g^{p-1} \tag{5.12}$$

Proof. The integers (5.12) are

(i) square numbers,

(ii) relatively prime to p, and

(iii) incongruent $\pmod p$ because they form a subset of the reduced system $\{g, g^2, ..., g^{p-1}\}$. Hence $g^2, g^4, ..., g^{p-1}$ are $\frac{p-1}{2}$ distinct quadratic residues of p. The theorem then follows immediately since we know that p has exactly $\frac{p-1}{2}$ quadratic residues.

□

Example: 5.2.10. 2 *is a primitive root of* $p = 19$. *Therefore the quadratic residues of* 19 *are* 2^2 ,2^4 ,2^6 ,2^8 ,2^{10} ,2^{12} ,2^{14} ,2^{16} *and* 2^{18}. *The least residues of these integers modulo p are 4, 16, 7, 9, 17, 11, 6, 5, and 1 respectively.*

Therefore the quadratic residues of p are 1, 4, 5, 6, 7, 9, 11, 16, and 17.

Euler's criterion can now be stated in a slightly different form:

Theorem 5.2.11. *(i) a is a quadratic residue of p if and only if* $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(ii) a is a quadratic non-residue of p if and only if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

We shall now derive some properties of quadratic residues and non-residues.

Theorem 5.2.12. *The product of two quadratic residues of p is a quadratic residue.*

Proof. Let a_1 and a_2 be two quadratic residues of p. Then we have

$$a_1 a_1^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$
$$a_2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Hence

$$(a_1 a_2)^{\frac{k-1}{2}} \equiv 1 \pmod{p}.$$

Therefore $a_1 a_2$, is a quadratic residue of p. □

Example: 5.2.13. *Find all the quadratic residues of 23.*

Solution: *There are in all* $\frac{r-1}{2} = \frac{32-1}{2} = 11$ *quadratic residue of* 23. *Of these* $1, 4.9,$ *and* 16 *are known at once because integers less than* 23.

The rest are calculated as follows:

$$4 \times 9 \equiv 13, 4 \times 16 \equiv 18$$

and

$$9 \times 16 \equiv 6 mod 23).$$

Hence $13, 18, 6$ *are quadratic residues of* 23.

Again we have

$$9 \times 13 \equiv 2, \quad 4 \times 18 \equiv 3, \quad 6 \times 9 \equiv 8, \quad 4 \times 3 \equiv 12 \pmod{23}.$$

Therefore $2, 3, 8,$ *and* 12 *are also quadratic residues of* 23. *Thus all the* 11 *quadratic residues are now calculated.*

Theorem 5.2.14. *The product of a quadratic residue and a non-residue of p is a non-residue of p.*

Proof. Let a be a quadratic residue of p and b a quadratic non-residue of p. Then we have

$$a_1^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad b^{\frac{n-1}{7}} \equiv -1 (mod p).$$

So,

$$(ab)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Hence ab is a non-residue of p. □

Theorem 5.2.15. *The product of two quadratic non-residues of p is a quadratic.*

Proof. Let b_1 and b_2 be two quadratic non-residues of p. Then we have

$$b_1^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \quad b_2^{\frac{p-1}{2}} \equiv -1 (mod p).$$

These two congruences imply $(b_1 b_2)^{\frac{r-1}{2}} \equiv +1 mod p)$ which proves the theorem. □

Chapter 6

ANALYSIS AND CONCLUSIONS

Chapter 1 is the Introductory stage of this Project report based on overview of Congruences and the history of number theory.

Chapter 2 deals with the Concept of Congruences. In this topic we have discussed the Elementary Properties of Congruences, also have discussed topics like Complete Residue System and Reduced Residue System with examples.

Un **Chapter 3** we have introduced a type of congruence, that is, Linear Congruences. The main aim over here was to prove some basic result concerning this type of congruences, and, in particular, some name theorems with proof that are related to this topic, for example, Fermat's Theorem, Euler's Theorem and so on. We have also discussed one application here.

Chapter 4 deals with another type of congruence that is, Identical Congruences. Our main focus was on topics like Order of Integers and Primitive roots which are often used in solving problems in congruences.

Chapter 5 deals with one more type of congruence, that is, Quadratic Congruences. This topic includes the Quadratic Congruences and Quadratic Residues.

Bibliography

[1] Tom M. Apostol. *Introduction to analytic number Theory*. Springer Science Business Media, June 2013.

[2] K. C. Chowdhury. *A first course in theory of numbers*. July 2007.

[3] Hsiung. *Elementary Theory of numbers*. Allied Publishers, Jan. 1995.

[4] Sadanand G. Telang. *Number theory*. Jan. 1996.

[5] Anthony Vazzana, Martin Erickson, and David Garth. *Introduction to Number Theory*. CRC Press, Oct. 2007.