STUDY

ON

"CONGRUENCE AND ITS APPLICATION IN NUMBER THEORY"

A project report submitted in partial fulfilment of the requirements for the degree of MASTERS OF SCIENCE in MATHEMATICS (Gauhati University),

by Roni Paul (GU Roll Number: PS-221-019-0013)

to the

DEPARTMENT OF MATHEMATICS

JAWAHARLAL NEHRU COLLEGE BOKO

Boko-781123

CERTIFICATE

This is to certify that the work contained in this report entitled "A Project Report on "Congruece and its Application in Number Theory". Submitted by Roni Paul to the department of Mathematics, Jawaharlal Nehru College, Boko towards the partial requirement of the Degree of Master of Science has done under my supervision and guidance.

.....

Mr. Dipu Moni Nath.

Project Supervisor.

ACKNOWLEDGEMENT

At the very outset. I offer my heartiest thanks to Jawahar lal Nehru College, as the college has given the opportunity to work on some project from where I have got the platform for learning and making a project work.

I would like to offer my whole hearted gratitude Sri. Dipu Moni Nath, Asst. prof. of Mathematics department for his immense guidance and giving me his precious time to make my project on the topic "Congruence and its application" as succesful one which also helped me in doing a lot of research and I came to know about so many new things.

I would like to express my special thanks to H.O.D of mathematics Dr. Dipankar Sharma, who gave me the golden opportunity to do this wonderful project.

Finally, I would also like to thanks to my seniors and friends who helped me a lot in finalising this project within the limited time frame.

Roni Paul

DECLARATION

I hereby declare that the project entitled is an outcome of my own efforts under the guidance of Mr. Dipu Moni Nath. The project is submitted to the Department of Mathematics, Jawaharlal Nehru College, Boko under Guwahati University for the partial fulfilment of the Post Graduation of Science in Mathematics examination 2023.

I also declare that this project report has not been previously submitted to any other university.

Date: 25/12/2023
Place: Boko

Roni Paul
(PS-221-019-0013)

HISTORICAL BACKGROUND

Karl Friedrich Gauss (1777-1855) has been called the "Prince of Mathematics" for his many contribution to pure and applied mathematics. He was born to poore parents in Germany. His high intelligence was noticed early and nurtured by his mother and uncle, but his father never encouraged Gauss in his education.

One of Gauss's most important contributions to Number theory involved the invention of the idea of congruence in numbers and the use of what he called "modulos" or small measures sets of numbers. In effect, his theory of congruence allows people to break up the infinite series of whole numbers into smaller, more manageable chunks of number and perform computations upon them. This arrangement makes the everybody arithmetic involved in such things as telling time much easier to perform into computers.

Gauss said that if one number is substracted from another number $(a-b)$, and the remainder of the substraction can be divided by another number m, then a and b are congruent to each other by the number m. Gauss's formula as follows: a is congruent to b modulo c. For example, $720 - 480 = 240$ the remainder 240 can be divided by 60, 20, 10 and other numbers. Howevere for our purpose, we will focus on 60. using Gauss's expression, 720 is congruent to 480 by modulo 60 that is both 720 and 480 are related to third number (the remainder after 480 is substracted from 720), which can be multiplied by 60.

The importance of Gauss's Congruence theory is that he created the formulas that allowed an immense variety of arithmetic actions to be performed based on different sets of number.

ABSTRACT

In Number Theory, we describe some interesting application of congruence. As with so many concepts we will see, congruence is simple, perhaps familiar to you, yet enormously useful and powerful in the study of number theory. If n is a positive integer, we say the integer a and b are congruent modulo n, and write $a \equiv b \pmod{n}$, if they have the same remainder on divisible by n.

Congruence satisfy a number of important properties and are extremely useful in many areas of number theory, using congruences, simple divisiblity tests to check whether a given number is divisible by another number can sometimes be derived, using congruence we can find easily the remainder when a large number is divisible by an integer, also find easily last digit, last two digit of a large number, it is also useful to solve linear Diophantine equation, Chinese Remainder theorem, Fermat's theorem, Wilson's theorem, Euler's ϕ function.

Congruences application has uses in some other fields too which are mention in this report.

Keywords: Congruent, modulo, integer.

PREFACE

This Project Report which I have prepared contains the report regarding analysis of "Congruence And Its Application" in Number Theory that I understand during PG 3rd Semester Course. In this report a brief description of the concept and the notion of congruence technique in the study of divisibility in Number theory has been summarized.

I seek apology of unwilling mistakes that may crept over in preparing this project report.

CONTENTS

INTRODUCTION

The concept and the notion of congruence was first introduced by the German mathematician, Carl Fredrich Gauss in his 'Disquisitions Arithemetic' in the beginning of nineteenth century.

Congruence is a powerful technique for the study of divisibility in number theory. Using congruence, we can easily solve a complex and lengthy arguments into a couple of lines.

According to Gauss, "Number Theory is the Queen of Mathematics and I think congruence is the magic of Number Theory".

CONGRUENCE

Definition: Let a and b are two integers. If m be a fixed positive integers such that m divides a − b then a is said to be congruent to b modulo m and denoted as $a \equiv b \pmod{m}$.

Thus, $a \equiv b \pmod{m}$ iff $m \mid a-b$, so there exist an integer k such that $a - b = mk$ or $a = b + mk$.

Eg:- Since 5 divides 17 − 2 so

$$17 \equiv 2 \pmod{5}.$$

If a − b is not divisible by m then $a \not\equiv b \pmod{m}$ and simply we say a is not congruent to b modulo m.

Eg:- 25 is not congruent 12 (mod 7) because $7 \nmid 25 - 12$

It is to be noted that any two integers are congruent modulo 1 where as two integers are congruent modulo 2. when they are both even or both odd.

Related with Division Algorithm:

For a given integer a, let q and r be its quotient and remainder when divided by m, then we have from division algorithm.

Then by definition of congruence we get $a \equiv r \pmod{m}$

Thus, we see that every integer is congruent modulo m to exactly one of the values $0, 1, 2, 3, \ldots, (m-1)$.

In particular, $a \equiv 0 \pmod{m}$ i.e $m \mid a$.

Also, we see that $a \pmod{m}$ means the remainder when 'a' is divisible by m. Thus, $7 \pmod{2} = 1$.

Some Basic Properties Of Congruence

Congruence may be viewed as a generalised form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences as follows:

For all integers a, b, c and d and m be a positive integer then we get,

i) $a \equiv a \pmod{m}$

ii) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

So, $\equiv$ is an equivalence relation.

iv) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

(Note: Congruence to different modulo can not be added or multiple.)

v) If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for any positive integer n.

vi) If $a \equiv b \pmod{m}$ and $f(x)$ be polynomial with integral coefficients then $f(a) \equiv f(b) \pmod{m}$.