Uttar Pradesh Rajarshi Tandon Open University

Bachelor of Science

DCEMM -110

Number Theory

Uttar Pradesh

RajarshiTandon
Open University

Bachelor Of Science

DCEMM -110

Number Theory

Block

1 Basic Introduction of Number Theory

Unit 1 **Analytic Number Theory**
Unit- 2 **Congruence's**
Unit -3 **Euler's Function and application**

Course Design Committee

Prof. Ashutosh Gupta, School of Computer and Information Science, UPRTOU, Prayagraj	**Chairman**
Prof. Sudhir Srivastav Dept. of Mathematics, DDU Gorakhpur University, Gorakhpur	**Member**
Prof. P. K. Singh Dept. of Mathematics, Allahabad Uiversity, Prayagraj	**Member**
Prof. Mona Khare Dept. of Mathematics, Allahabad Uiversity, Prayagraj	**Member**
Dr. A. K. Pandey Associate Professor, ECC Prayagraj	**Member**
Dr. Vikas Singh Academic Consultant, UPRTOU, Prayagraj	**Member**
Dr. S. S. Tripathi Academic Consultant, UPRTOU, Prayagraj	**Member**

Course Preparation Committee

Dr. P.N. Pathak Assistant Professor (Dept. of Mathematics), CSJM Kanpur university, Kanpur	**Author (Unit – 4 to 6)**
Dr. Raghvendra Singh Assistant Professor , (C.) School of Science, UPRTOU, Prayagraj	**Author (Unit – 1 - 3)**
Dr. S. S. Tripathi Ret. Associatet Professor (Dept. of Mathematics), ECC, Prayagraj.	**Editor (Unit 1 - 6)**
Dr. Raghvendra Singh Assistant Professor , (C.) School of Science, UPRTOU, Prayagraj	**Coordinator**

DCEMM – 110 : Number Theory
ISBN-

Printed By: Chandrakala Universal Pvt. 42/7 Jawahar Lal Nehru Road, Prayagraj.

DCEMM-110

NUMBER THEORY

BLOCK-1 (Basic Introduction of Number Theory)

UNIT-1 Analytic Number Theory

UNIT-2 Congruence's

UNIT-3 Euler's Function and Application

BLOCK-2 (Gauss Theorem & Applications)

UNIT-4 Quadratic Residue of Number Theory

UNIT-5 Gauss Theorem

UNIT-6 Arithmetic Function and Applications

COURSE INTRODUCTION

Block 1 :- Basic Introduction of Number Theory
Block 2 :- Gauss theorem & Applications

The block 1st is Basic Introduction of Number Theory organized into following three units as under:

Unit- 1 Analytic Number Theory

Unit- 2 Congruence's

Unit-3 Euler's Function and application

The Block 2nd is Gauss theorem & Applications:

Unit -4 Quadratic residues of Number Theory

Unit-5 Gauss theorem

Unit-6 Arithmetic Functions and applications

Block-1: Basic Introduction of Number Theory

Introduction

Number theory is a branch of pure mathematics devoted to the study of the set of positive whole numbers which are usually called the set of natural numbers. This provides an introduction to the important basic topics of number theory: Division Algorithm Euclids Algorithm, Congruences, Residue Classes, Chines Remainder Theorem, Euler's Function and application. Originally an abstract mathematical concept from the branch of number theory known as modular arithmetic, quadratic residues are now used in applications ranging from acoustical engineering to cryptography and the factoring of large numbers.

Objectives:

- To understand the difference between the quadratic residues and non residues.
- To verify the given number is Division Algorithm.
- To understand the Euclids Algorithm and its basic properties.
- To understand the Congruences.
- To differentiate the Residue Classes.
- To understand the definition of multiplicative functions.
- To understand the Chines Remainder Theorem.
- Use of Euler's Function and application.

LIST OF SYMBOLS USED

Symbol	Explanation
$a \in A$	a is an element of set A
$a \notin B$	a is not an element of the set B
$A \square B$	A is a subset of B
$A \square B$	B Contains A as a subset
$A \cup B$	A Union B
$A \cap B$	A Intersection B
$p \Rightarrow q$	p Implies q
$p \Leftarrow q$	p is implied by q
$p \Leftrightarrow q$	p implies and is implied by q
$a < b$	a Less than b
$a > b$	a greater than b
$\forall x$	For all x
$Z (or\ J)$	Set of all integers.
N	Set of all natural numbers.
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a \equiv b$(mod m)	a is congruent to b modulo m
A\B	The set of elements of A that are not in B
iff	If and only if
∃	There exist
∀	For every

UNIT-1 Analytic Number Theory

Structure

1.1 Introduction

In this unit we first discuss some basic definition of divisibility these concepts are fundamental to the study of any branch of mathematics in particular of Algebra.

We shall discus some analytic number theory. The primary aim of this section is to assemble a few facts that we will need in the rest of the course. We also hope to give you a glimps of the elegance of number theory .it is this elegance that led the mathematician gauss to call number theory the "queen of mathematics"

Number theory deals with the properties of integers….-3,-2,-1, 0, 1, 2, 3…….because it concerns with the simplest number system, with equally simple operations. Number theory has aroused great curiosity and interest from very early times, not only among professional mathematicians but also among many inquisitive amateur.

In this unit we discuss division algorithm, Euclid's algorithm for the greatest common divisor, prime numbers and fundamental theorem of arithmetic.

1.2 Objectives:

After reading this unit learner should be able to understand about:

- Define divisibility
- Use the division algorithm theorem
- Use the Euclid's algorithm theorem
- Define and use greatest common divisor
- Define prime number
- State and proof fundamental theorem of arithmetic.

1.3 Basic Definitions:

We have a basis of many other topics in Mathematics. Let us be begine by understanding various types of numbers.

1. **Natural Numbers:** All the counting numbers are called natural number.

Example-1: 1,2,3,4,5,……

(a).Even Numbers: The Numbers Which are exactly divisible by 2 are called even numbers.

Example:2,4,6,8……

(b).Odd Numbers: The Numbers which leave a remainder 1 when divided by 2 are called odd numbers.

Example:1,3,5,7……

(c) Prime Numbers: If a number is not divisible by any other number except 1 and itself.It is called a prime number.

Example:2,3,5,……

(d) Co-Primes: Two numbers which have no common factor between them are said to be Co-Prime to each other, the two numbers individually may be prime or composite.

Example:13 and 29 are Co-Primes.

(e) Composite Numbers: Numbers which are divisible by other numbers along with 1 and itself are called composite numbers.

Example:4,6,8,9,10……

2. **Whole Numbers:** Natural numbers along with ‘o’ form the set of whole numbers.

Example:0,1,2,3,4,5,……

3. Integers: All Counting numbers and their negatives along with zero are called integers.

Example:-4,-3,-2,-1,0,1,2,3,4……

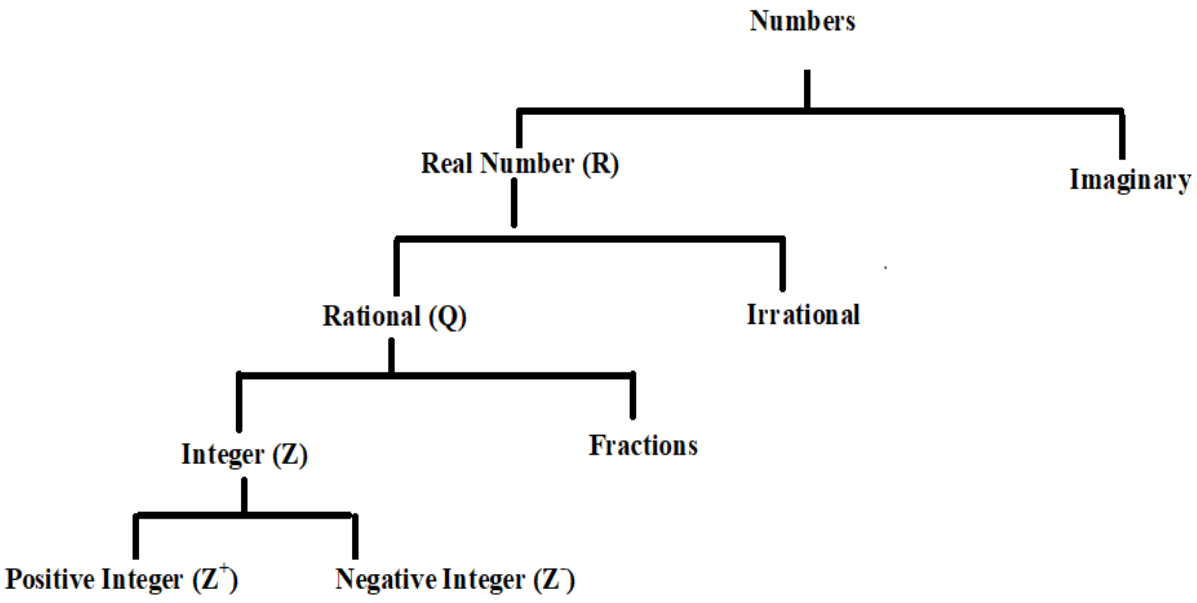
4. Rational and irrational Numbers: Any number which can be expressed in the form of p/q,where p and q are integers and q≠0 is a rational numbers.

Example:3/5,4,-6……

Numbers which are represented by non-terminating and non-recurring decimals are called irrational Numbers.

Example:$\sqrt{2} = 1.414$ ... , $\sqrt{3} = 1.732$ ...

5. Real Numbers: Rational and irrational number taken together are called real numbers.



We can summaries the above chart.

The symbol for showing that one set is a member of another set is $\subset$, so that $\mathrm{N} \subset \mathrm{Z} \subset \mathrm{Q} \subset \mathrm{R} \subset \mathrm{C}, \mathrm{C}$ is the set of complex number.

Well-Ordering Principal: Every non-empty subset S of non-negative integers contains a least element that is there is some integers 'a' in S such that $a \leq b$ for all b in S.

$$z \equiv Set\ of\ all\ integers$$

$$z \equiv \{\ldots -3, -2, -1,0,1,2,3 \ldots\} Set\ of\ all.$$

$$z^{+} \equiv \{0,1,2,3, \ldots.\}\ \text{non} - \text{negative integers.}$$

$If\ S_1 = \{5,3,100,2,125\} \subseteq z^{+}$

2 is least element of S_1.

'If $S \subseteq z^{+}$ then S has a least element'

1.4 Divisibility.

An integer b is said to be divisible by integer $a \neq 0$ if there exist some integer k such that $b = ka$

Example:

1. $\frac{35}{5} = 7, \text{here } 35 = 7 \times 5, 5/35$

2. $\frac{18}{4} = 4.5, here\ remainder\ is\ not\ zero.$

K in z such that $18 = k \times 4$, $4 \nmid 18$ or $4 \nmid 18$

3.-8 is divisor or 72 since $72 = (-9) \times (-8)$.

Notation:a/b; $if\ a\ divides\ b\ and\ a \nmid$ b ; if a does not divide b.

Properties of divisibility: For integer a, b, c the following hold:

Note: In following all cases when we are using any of a, b, c as a divisor; it is non-zero.

a. a/0,1/0,a/a(a/0 means 'a' divides 0)

b. a/1; if and only if $a = \pm b1$

c. $if a/b\ and\ c/d, then\ ac/bd$

Example-1:$2/4\ and\ 3/9 \Rightarrow (2 \times 3)/(4 \times 9)$

We have $6/36\ as\ 36 = 6 \times 6$

d.if a|b and b|c, then a|c

Example-2: 7|56 and 56|168

⇨7|168

$$56 = 8 \times 7 \ , 168 = 3 \times 56$$

$$\Rightarrow 168 = (8 \times 3)7 \ \ i.e. 168 = 24 \times 7$$

e. a|b and b|a if and only if $a = \pm b$

f. if a|b and b $\neq$ 0 then |a| $\leq$ |b|

g. if a|b and a|c, then a|(bx + cy) for arbitrary integers x and y.

Example-3: 5|25 and 5|50

$\Rightarrow$5|(4$\times$ 25 + 7 $\times$ 50)

$$i.e., 5|450.$$

Law of Trichotomy: For any $m, n \in Z$, one and only one of the following is true:

(i) $m = n$ (ii)$m > n$ (iii) $m < n$

The Absolute value of an integer x denoted by $|x|$ is defined as: |x| =

$$\begin{cases} 0, \text{if x} = 0 \\ \text{x if x is positive integer} \\ -\text{x if x is negative integer} . \end{cases}$$

Thus

$|0| = 0, \ |5| = 5 \ , |-5| = 5$

If $= b.c$, where a, b, c are integers, then it can be proved easily that

$|a| \geq b$, $|b| \geq c$.

Properties of absolute values of integers:

(i) $|a| = 0 \leftrightarrow a = 0$

(ii) $\|\boldsymbol{a}\| = |\boldsymbol{a}|, |\boldsymbol{a}.\boldsymbol{b}| = |\boldsymbol{a}|.|\boldsymbol{b}|$

(iii) $|a + b| \leq |a| + |b|$

(iv) $|ab| \geq |a|$ and $|ab| \geq |b|$

(v) If $a, b \in N$, then $|a - b| < Max(a, b)$

1.5 Division Process in Z.

Definition: An integer a is said to be divisible by an integer $(b \neq 0)$ if there exists an integer c, such that $a = bc$. the integer b is called a divisor of a and a is called a multiple of b.

When b is a divisor of a, we write b|a.

Note: Every integer b is a divisor of 0,

Since $0 = b.0 \; \forall \; b \in Z$. it is also apparent that +1, and +a are divisors of a$\in Z$.Divisors of a other than +1,+a are called proper divisors of a.

Division and its Properties:

Definition: Let a, b ∈ Z and a/0.Then a is said to divide b if there is an integer k such that b = a k. We denote it by a | b and a∤b means that a does not divide b.

Remark1.2. a | b is a statement, for example 2|6 is true, and 6|2 is false. Whereas 6|2 is a number equal to 3.

Following properties are easy to verify, hence we state them without proof.

(Few properties of division): Let a, b, and d be integers. Then, the following statements hold:

Reflexive property: a |a (every integer divides itself),a≠0

Transitivity property: d |a and a |b ⇒d |b.

Linearity Property: d |a and d |b ⇒d| a n + b m for all n and m.

That is if d |a, b, then d divides every integer linear combination of a and b.

Cancellation Property: ad |an and a/0⇒d|n.

Multiplication Property: d |n ⇒ad |an.

1**and**−1**divideseveryinteger:**1|n, −1|n ∀ n ∈ Z.

1 **and** −1 **are divisible by** 1**and**−1**only:** n |1⇒ n=±1.

Another equivalent way of stating the above two properties is: 1and−1are the only invertible elements in Z.

Every number divides zero: d | 0 ∀ d ∈ Z.

Comparison Property: If d and n are positive and d |n then d ≤ n.

1.6 Theorem: Division algorithm.

Let a be an integer and $b \neq 0$. Then there exist unique integers q, r, such that $a = bq + r$, where $0 \leq r < |b|$.

Proof: Consider the set

$$S = \{a - x|b| : x \in Z \text{ and } x|b| \leq a\}.$$

Now $-|a|.|b| \leq -|a| \leq a$.

Hence when $x = -|a| \; then \; x\,|b| \leq a$. therefore the set S is non empty. Further S is a set of non-negative integers and therefore by the well ordering property, S has a least element say $r = a - q'|b|$.

Now $r \geq 0. if \; r \neq 0, then \; r \; must \; be \; less \; than \; |b|$.

For if not, let $r > |b|$.then

$$a - (q' + 1)|b| = a - q'^{|b|} - |b| = r - |b| > 0.$$

Therefore $a-(q'+1)|b| \in S$ and $a-(q'+1)|b| < a-q'|b|$ which contradicts

That $a-q'|b|$ is the least element of S.

Hence $r < |b|$.

Thus we get $a = |b|q' + r$.

Where either $r = 0\ or\ 0 < r < |b|$.

Now if $b > 0$,then $|b| = b$. Putting $q' = q\ we\ get$

$$a = bq + r$$

if $b < 0$,then $|b| = -b$. Putting $q' = -q\ we\ get$

$$a = (-b)(-q) + r = bq + q$$

This Prove the existence of the integers $q\ and\ r$.

Now we prove their Uniqueness.

If possible, let there be a second pair of integer q_1, r_1

Such that $a = bq_1 + r_1, 0 \leq r_1 < |b|$.

Then $bq_1 + r_1 = bq + r$ or $r_1 - r = b(q - q_1)$

Which gives b to be a divisor of $r_1 - r$ which is not possible because

$r_1 < |b|. r < |b|$ and therefore $r_1 - r < |b|$.

Hence b can not be a divisor of $r_1 - r$ unless $r_1 - r = 0$

Therefore $r_1 = r$ and consequently we get $q_1 = q$,

$$since\ b \neq 0.$$

Corollary (1.1): If $a, b \in Z$ with $b > 0$, there exist unique integers q and r such that $a = qb + r$ where $0 \leq r_1 < |b|$.

Associate: If $a, b \in Z$ such that $a|b$ and $b|a$,then a and b are said to be associate to each other. In this case $a = \pm b$

$$a|b \Rightarrow b = ac$$

$$b|a \Rightarrow a = bd$$

So $ba = abcd \Rightarrow 1 = cd \Rightarrow c = \pm 1, d = \pm 1$

Thus $a = \pm b$

Thus it $a \in Z, a \neq 0$, then units and associates of a are always divisors of a called improper divisors. Other divisors are called proper divisors.

Common divisor: Let $a, b \in Z. c \in Z$ is called a common divisor of a and b if c|a and for Example, 2 is a common divisor of 2 and 4.

You know that 1 and -1 common divisors of $a \; and \; b$, for any $a, b \in Z$.

Thus, a pair of integers does have more than one common divisor. This fact leads us to the following definition.

Example: 1 No integer in the following sequence is a perfect square {11, 111, 1111, 11111,... }.

Solution: We already know that the square of any integer is either of the form 4r or 4r+1.

An arbitrary number of the form1111...1111=1111...1108+3 and 4 divides 1111...1108.Thus, all the numbers are of the form 4k+3.Hence, they cannot be perfect squares.

1.7. APPLICATION OF DIVISION ALGORITHM

Theorem 9: Every integer can be written in the form of 3n, 3n + 1 & 3n – 1.

Proof: Let "a" be any integer. Then for b = 3 > 0, the euclide theorem will be

a = 3q + r where $0 \leq r < 3$

Here $0 \leq r < 3$ implies that $r = 0, 1, 2$

Case-1: When $r = 0$

Then,

$a = 3q + 0$

$\Rightarrow a = 3q$

$\Rightarrow a = 3n$ by replacing q by n

Case-2: when $r = 1$

Then,

$a = 3q + 1$

$\Rightarrow a = 3n + 1$ by replacing q by n

Case-3: when $r = 2$

Then,

$a = 3q + 2$

$\Rightarrow a = 3q + 3 – 1$ since $2 = 3 – 1$

$\Rightarrow a = 3(q + 1) – 1$

$\Rightarrow a = 3n – 1$ by replacing $q + 1$ by n

This completes the proof.

Theorem 5: Every odd integer can be written in the form of 4n + 1 & 4n – 1

Proof: Let "a" be any odd integer. Then for $b = 4 > 0$, the euclide theorem will be

$a = 4q + r$ where $0 \leq r < 4$

Here $0 \leq r < 4$ implies for odd integer that $r = 1, 3$

Case-1: when $r = 1$

Then,

$a = 4q + 1$

$\Longrightarrow a = 4n + 1$ by replacing q by n

Case-2: when $r = 3$

Then,

$a = 4q + 3$

$\Longrightarrow a = 4q + 4 - 1$ since $3 = 4 - 1$

$\Longrightarrow a = 4(q + 1) - 1$

$\Longrightarrow a = 4n - 1$ by replacing $q + 1$ by n

This completes the proof.

1.8 Euclidean Algorithm

Since gcd (a,b) = gcd (a,−b) = gcd (−a,−b) = gcd (−a,b) =gcd (|a|,|b|), we may assume that a and b are both positive. Since gcd(a,b)= gcd (b,a), we may assume $a \geq b$. Also, by ignoring the trivial case, gcd (a,a) =a, we suppose a>b. So, we have a > b >0.

Lemma (**Euclidean Algorithm):** Let a>b>0. If a = bq+r, then

$$\gcd(a,b) = \gcd(b,r).$$

Solution: In fact we prove more. That is, we show that $D_a \cap D_b = D_b \cap D_r$, or equivalently, **the common divisors of** a **and** b **are same as the common divisors of** b **and** r.

To show this, first let d|a and d|b. Note that $r = a - bq$, which is a linear integer combination of a and b. So, from the linearity property of division, d|r. Thus, d|b and d|r

Next assume d|b and d|r. Using linearity property of division again and the fact that a=bq+r is a linear combination of b and r, we have d|a. So, d|a and d|b. We have thus shown that $D_a \cap D_b = D_b \cap D_r$. Hence, gcd(a,b)=gcd(b,r).

Euclid's algorithm uses this repeatedly to simplify the calculation of greatest common divisors by reducing the size of the given integers

without changing their gcd.

Let gcd (a,b)=d.

- By division algorithm $a=q_1b+r_1$ with $0 \leq r_1<b$.If $r_1=0$, then b|a and gcd (a,b)=d=b.Stop.
- If $r_1 \neq 0$, then by division algorithm $b=r_1q_2+r_2$with$0 \leq r_2<r_1$.If$r_2=0$, then $d=r_1$. Stop.
- If $r_2 \neq 0$ then we continue in this way; since $b>r_1>r_2>\cdots \geq 0$, we must eventually get a remainder $r_n=0$ (after at most b steps).
- Sinced=gcd(a,b)=gcd(b,r_1)=gcd(r_1,r_2)=$\cdots$=gcd(r_{n-2},r_{n-1}) and from last equation

$$r_{n-2}=r_{n-1}.q_n+r_n=r_{n-1}q_n,$$

we have gcd (r_{n-2},r_{n-1})=r_{n-1}.

Example 2 .2. Find gcd (34,55).

Solution: we have

$$55=34.1+21$$

$$34=21.1+13$$

$$21=13.1+8$$

$$13=8.1+5$$

$$8=5.1+3$$

$$5=3.1+2$$

$$3=2.1+1$$

$$2=1.2+0.$$

Consequently,

gcd(55,34) = gcd (34,21) = gcd (21,13) = gcd (13,8) = gcd (8,5)

= gcd (5,3) = gcd (3,2) = gcd (2,1) = 1.

1.9. Common divisor

Suppose a and b be any two integers then a number "c" is called common divisor of a and b if

$$c/a \ \& \ c/b$$

Example-1:

2 is common divisor of the set {4, 8} because

$$2/4 \ \& \ 2/8$$

1.9.1. Greatest common divisor

The largest positive integer that divides both a and b is called greatest common of a and b. it is denoted as (a, b).

Example-1:

Let us calculate the g.c.d of 42 and 48

Divisor of 42 = {1, 2, 3, 6, 7, 14, 21, 42}

Divisor of 48 = {1, 2, 3, 4, 6, 8, 12, 16, 24, 48}

Common divisor of 42 & 48 = {1, 2, 3, 6}

Therefore,

(42, 48) = 6

1.9.2. Linear combination

Suppose a and b be any two integer then "m" is called linear combination of a and b $\forall x, y \in Z$, we have

$m = ax + by$

Remark:

The greatest common divisor of two numbers a and b is the smallest positive linear combination of a and b. That is,

(a, b) = ax + by

1.10. Relatively Prime

The integers a and b is called relatively prime if (a, b) = 1. More generally, it is defined as "The integers $m_1, m_2, \ldots\ldots\ldots\ldots m_n$ are relatively prime if every pair of m_i is relatively prime i.e.

$(m_i, m_j) = 1$, whenever $\neq j$"

Remark: Any two consecutive integers are relatively prime.

Proof: Assume that n and n + 1 are two consecutive integers. Then for all x, y ∈ Z, we have $(n, n + 1) = nx + (n + 1)y$

Take x = -1 & y = 1, then we have

$(n, n + 1) = n(-n) + (n + 1)1$

$\Longrightarrow (n, n + 1) = 1$

This completes the proof.

Theorem 5: If c is any common divisor of a and b, then c divides (a, b).

Proof: Suppose c is common divisor of a and b. Then by definition

c/a & c/b

Then by a result, we have

c/ax + by

$\Longrightarrow$ c/(a, b) Because (a, b) = ax + by

This proves the result.

Alternative Definition of G.C.D.

In view of the previous result we can reformulate the definition of g.c.d.

Definition: A positive integer d is called g.c.d of a and b if

i. $d \geq 0$

ii. d/a and d/b

iii. If some other integer e/a and e/b, the e\d

Theorem 6: The greatest common divisor of a & b is unique.

Proof: Suppose $(a, b) = d_1$ & $(a, b) = d_2$

Then, we have to show that

$d_1 = d_2$

if "d_2" is G.C.D of a & b and "d_1" is common divisor of a & b. Then, by definition of G.C.D, we have

d_1/d_2 (A)

if "d_1" is G.C.D of a & b and "d_2" is common divisor of a & b. Then, by definition of G.C.D, we have

d_2/d_1 (B)

From (A) & (B), we have

$d_1 = \pm d_2$

Since d_1 & d_2 are non-negative. Therefore.

$d_1 = d_2$

Theorem 20: if (a, b) = 1 then show that (a – b, a + b) = 1 or 2.

Proof:

Suppose that

$(a – b, a + b) = d$ (A)

This implies by alternative definition of G.C.D, we have

$d/a - b, d/a + b$

$\Rightarrow d/a - b + a + b \;\&\; d/a - b - a - b$

$\Rightarrow d/2a \;\&\; d/-2b$

$\Rightarrow d/2a \ldots\ldots$ (a) & $d/2b \ldots\ldots$ (b)

Since it is given that $(a, b) = 1$

$\Rightarrow \exists$ Two integers x & y such that

$ax + by = 1$

$\Rightarrow 2ax + 2by = 2 \ldots\ldots\ldots$ (i)

From (a) & (b) , we have

$d/2a \;\&\; d/2b$

$\Rightarrow d/2ax \;\&\; d/2by$

$\Rightarrow d/2ax + 2by$

$\Rightarrow d/2$ from (i)

Since 2 is a prime number. Therefore,

$d = 1$ or 2

Using $d = 1$ or 2 in equation (A), we have

$(a - b, a + b) = 1$ or 2

This is completes the proof.

Example. 1: Let a and b be integers. Then

(I) (ca.cb) = c(a, b) for any positive integer c;

(II) $\left(\frac{a}{d},\frac{b}{d}\right)$=1 if d = (a, b).

Solution:

I. (ca.cb) = c(a, b) for any positive integer c;

As we know "The greatest common divisor of two numbers a and b is the smallest positive linear combination of a and b". Therefore,

$(ca.cb) = ca(x) + cb(y) \qquad \forall\, x, y \in Z$

$(ca.cb) = c(ax + by) \qquad \forall\, x, y \in Z$

Here ax + by is the smallest linear combination of a and b. Therefore,

$ax + by = (a, b)$

It follows that,

(ca.cb) = c(a, b) for any integer c

II. $\left(\frac{a}{d},\frac{b}{d}\right)$=1 if d = (a, b).

Since d = (a, b). Then, $\frac{a}{d}$ & $\frac{b}{d}$ both are integers.

Now consider that,

$$d\left(\frac{a}{d},\frac{b}{d}\right) = \left(d.\frac{a}{d}, d.\frac{b}{d}\right)$$

$$\Longrightarrow d\left(\frac{a}{d},\frac{b}{d}\right) = (a, b)$$

$\Longrightarrow d\left(\frac{a}{d},\frac{b}{d}\right) = d$ since d = (a, b)

$\Longrightarrow \left(\frac{a}{d},\frac{b}{d}\right) = \frac{d}{d}$

$\Longrightarrow \left(\frac{a}{d},\frac{b}{d}\right) = 1$

This is completes the proof.

Example .2: If (a, b) =d then (ma.mb) = md.

Solution: Since it is given that (a, b) = 1

$\Longrightarrow \exists$ Two integers x and y such that

ax + by = d

$\Longrightarrow$ max + mby = md …….. (i)

Let (ma.mb) = d_1 …….. (A). Then, we have to show that d_1 = md

$\Longrightarrow d_1/ma \;\&\; d_1/mb$

$\Longrightarrow d_1/max \;\&\; d_1/mby$

$\Longrightarrow d_1/max + mby$

$\Longrightarrow d_1/md$ ……. (*)

As (a, b) = d. This implies by definition

d/a & d/b

$\Longrightarrow$ md/ma & md/mb

The above shows that “md” is common divisor of ma and mb. But from (A), d_1 is G.C.D of ma and mb. Then by definition of G.C.D, we have

md/d_1 ……. (**)

Now from (*) and (**), we have

$d_1 = md$

It follows that

$(ma.mb) = md$

This completes of proof.

Example .3: If a/bc and (a, b) = 1, then a/c.

Solution: Since it is given (a, b) = 1

$\Longrightarrow \exists$ Two integers x and y such that

$ax + by = 1$

$\Longrightarrow cax + cby = c$ (by multiplying c on both sides)

Since

a/cax (by division)

a/bcy (by supposition)

Therefore,

$a/cax + cby$

$\Longrightarrow a/c$ (by 1)

This completes the proof.

Example .4: Let a, b and c be integers.

(I) If (a, b) = (a, c) = 1, then (a, bc) = 1

(II) If a\c, b\c and (a, b) = 1, then ab\c.

Solution:

I. (a, b) = (a, c) = 1, then (a, bc) = 1

Since (a, b) = (a, c) = 1. Then, there exists the integers s, t, x & y such that

$as + bt = 1 \quad \Longrightarrow bt = 1 - as \quad (i)$

$ax + cy = 1 \quad \Longrightarrow cy = 1 - ax \quad (ii)$

Multiplying (i) & (ii), we have

$(bt)(cy) = (1 - as)(1 - ax)$

$\Longrightarrow bc(ty) = 1 - ax - as + a^2sx$

$\Longrightarrow bc(ty) = 1 - a(x + s - asx)$

$\Longrightarrow a(x + a - asx) + bc(ty) = 1$

$\Longrightarrow (a, bc) = 1$ (by definition)

II. a\b, b\c and (a, b) = 1, then ab\c.

since a\c & b\c. This implies that there exists two integers c_1 & c_2 such that

$c = ac1 \quad (i)$

$c = bc1$ (ii)

Also it is given that $(a, b) = 1$

$\Longrightarrow \exists$ Two integers x & y such that

$ax + by = 1$

$\Longrightarrow cax + cby = c$ (by multiplying c on both sides)

$\Longrightarrow (bc_2)ax + (ac_1)by = c$ (by using (i) & (ii))

$\Longrightarrow abc_2x + abc_1y = c$

$\Longrightarrow ab(c_2x + c_1y) = c$

$\Longrightarrow c = ab(c_2x + c_1y)$

$\Longrightarrow ab/c \qquad \forall c_2x + c_1y \in Z$

This completes the proof.

Example .5: if $(d_1, d_2) = 1, d_1/a$ & d_2/a then d_1d_2/a.

Proof: Since d_1/a & d_2/a. This implies that there exists two integers c_1 & c_2 such that

$a = d_1c_1$ (i)

$a = d_1c_2$ (ii)

Also it is given that $(d_1, d_2) = 1$

$\Longrightarrow \exists$ Two integers x & y such that

$d_1x + d_2y = 1$

$\Longrightarrow ad_1x + ad_2y = a$ (by multiplying c on both sides)

$\Longrightarrow (d_2c_2)d_1x + (d_1c_1)d_2y = a$ (by using (i) & (ii))

$\Longrightarrow d_1d_2c_2x + d_1d_2c_1y = a$

$\Longrightarrow d_1d_2(c_1x + c_1y) = a$

$\Longrightarrow a = d_1d_2(c_2x + c_1y)$

$\Longrightarrow d_1d_2/a \qquad \forall\ c_2x + c_1y \in Z$

This completes the proof.

Theorem 7: if (b, c) = 1 & a/c, then (a,b) = 1

Proof: If a/c, then there exist on integer c_1 such that

$c = ac_1$ …….(a)

Also it is given that (b, c) = 1

$\Longrightarrow \exists$ Two integers x & y such that

$bx + cy = 1$

$\Longrightarrow bx + ac_1y = 1$ ……..(b) since $c = ac_1$

Let (a, b) = d ……. (c)

Then we have to show that d = 1

As (a, b) = d. Then, by definition of G.C.D, we have

d/a & d/b

$\Longrightarrow d/ac_1y$ & d/bx

$\Rightarrow d/ac_1y + bx$

$\Rightarrow d/1$ from (b)

$\Rightarrow d = 1$ put in (c), we have

$(a, b) = 1$

This completes the proof.

Theorem .8: if (a, c) = 1 then (a, bc) = (a, b).

Proof: Suppose that

$(a, bc) = d_1$ (i)

$(a, b) = d_2$ (ii)

Then, we have to show that $d_1 = d_2$.

From (ii), we have

$(a, b) = d_2$

$\Rightarrow d_2/a$ & d_2/b

$\Rightarrow d_2/a$ & d_2/bc

Which shows that "d_2" is common divisor of a & bc. But from (i), it is clear that "d1" is G.C.D of a & bc. This implies by the definition.

d_2/d_1 ……(A)

Since (a, c) = 1

$\Rightarrow \exists$ Two integers x & y such that

$ax + cy = 1$

$\Longrightarrow bax + bcy = b$ (iii)

Now from (i), we have

$(a, bc) = d_1$

$\Longrightarrow d_1/a$ & d_1/bc

$\Longrightarrow d_1/bax$ & d_1/bcy

$\Longrightarrow d_1/bax + bcy$

$\Longrightarrow d_1/b$ from (iii)

d_1/a & d_1/b implies that "d_1" is common divisor of a & b. But from (ii), G.C.D of a & b is "d_2".

Then by definition of G.C.D, we have

d_1/d_2 …… (B)

from (A) & (B), we have

$d_1 = d_2$

Therefore

$(a, bc) = (a, b)$

This completes the proof.

Example .1: If a = bq + r then show (a, b) = (b, r)

Solution: Suppose that

$(a, b) = d_1$ ……. (i)

$(b, r) = d_2$ ……..(ii)

$a = bq + r$ …….. (iii)

From (ii), we have

$(b,r) = d_2$

$\Longrightarrow d_2/b$ & d_2/r

$\Longrightarrow d_2/bq$ & d_2/r

$\Longrightarrow d_2/bq + r$

$\Longrightarrow d_2/a$ from (iii)

d_2/a and d_2/b shows that "d_2" is common divisor of a & b. But from (i) G.C.D of a & b is "d_1". Then by definition of G.C.D, we have

d_2/d_1 ……. (A)

From (i), we have

$(a, b) = d_1$

$\Longrightarrow d_1/a$ & d_1/b

$\Longrightarrow d_1/a$ & d_1/bq

$\Longrightarrow d_1/a - bq$

$\Longrightarrow d_1/r$ since $r = a - bq$ from (iii)

d_1/b & d_1/r shows that "d_1" is common divisor of b & r. But from (ii), G.C.D of b & r is "d_2". Then by definition of G.C.D, we have

$$d_1/d_1 \text{ ……..(B)}$$

From (A) & (B), we have

$$d_1 = d_2$$

Therefore,

$$(a, b) = (b, r)$$

This completes the proof.

Example .2: If (b, c) = 1 then show that (a, bc) = (a, b)(a, c).

Proof:

Suppose that

$$(a, b) = d_1 \text{ ……. (i)}$$

$$(a, c) = d_2 \text{ ……(ii)}$$

$$(a, bc) = d_3 \text{ …….(iii)}$$

From (i), we have

$$(a, b) = d_1$$

$$\Rightarrow d_1/a \text{ \& } d_1/b$$

$$\Rightarrow d_1/a \text{ \& } d_1/bc$$

This show that "d_1" is common divisor of a & bc. But from (iii), G.C.D of a & bc is "d_3". Then by definition of G.C.D, we have

d_1/d_3 ……. (A)

From (ii), we have

$(a, c) = d_2$

$\Longrightarrow d_2/a$ & d_2/c

$\Longrightarrow d_2/a$ & d_2/bc

This shows that "d_2" is common divisor of a and bc. But from (iii), G.C.D of a & bc is "d_3". Then by definition of G.C.D, we have

d_2/d_3 ……. (B)

Since it is given that $(b, c) = 1$

$\Longrightarrow \exists$ Two integer x & y such that

$bx + cy = 1$ ……. (iv)

From (i) & (ii), we have

d_1/b & d_2/c

$\Longrightarrow \exists$ the integers m & n such that $b = d_1m$ & $c = d2n$

Put in (iv), we have

$d_1mx + d_2ny = 1$

$\Longrightarrow (d_1, d_2) = 1$……. (v) $\forall$ m, n, x, y, $\in Z$

From (A) & (B), we have

$d_3 = d_1 f$ …… (vi) &

$d_3 = d_2 g$ ……..(vii) $\forall$ f, g $\in$ Z

From (v), we have

$(d_1 . d_2) = 1$

$\Longrightarrow$ d1x + d2y = 1 $\quad \forall$ x, y $\in$ Z

$\Longrightarrow d_3 d_1 x + d_3 d_2 y = d_3$ multiplying with d_3

$\Longrightarrow (d_2 g) d_1 x + (d_1 f) d_2 y = d_3$

$\Longrightarrow d_1 d_2 (gx + fy) = d3$

$\Longrightarrow d_1 d_2 / d_3$ ……. (C)

From (i) $ax_1 + by_1 = d_1$ ……. (viii)

From (i) $ax_2 + cy_2 = d_2$ ……(ix)

Multiplying (viii) & (ix), we have

$(ax_1 + by_1)(ax_2 + cy_2) = d_1 d_2$

$\Longrightarrow ax_1 x_2 a + ax_1 cy_2 + ax_2 by_1 + bcy_1 y_2 = d_1 d_2$

$\Longrightarrow a(x_1 x_2 a + x_1 cy_2 + x_2 by_1) + bc(y_1 y_2) = d_1 d_2$

$\Longrightarrow (a, bc) = d_1 d_2$

$\Longrightarrow (a, bc) = (a, b)(a, c)$

This is complete the proof.

Theorem-9: (Fundamental Theorem of Arithmetic):

Every integer $n > 1(|n| > 1)$ can be written as $= p_1, p_2, \ldots\ldots\ldots p_n$, where $p_1, p_2, \ldots\ldots\ldots p_n$ are prime numbers. This representation is unique, except for the order in which the prime factors occur.

Proof: We will first prove the existence of such a factorisation. Let $p(n)$ be the statement that $n + 1$ is a product of primes. $p(1)$ is true, because 2 is a prime number itself.

Now let us assume that $p(m)$ is true for all positive integers $m < k$. we want to show that $p(k)$ is true. If $(k + 1)$ is a prime, $p(k)$ is true. If $k + 1$ is not a prime, then we can write $k + 1 = m_1 m_2$, where $1 < m_1 < k + 1$ and $1 < m_2 < k + 1$. But then $p(m_1 - 1)$ and $p(m_2 - 1)$ are both true. Thus, $m_1 = p_1, p_2, \ldots\ldots\ldots p_r, m_2 = q_1, q_2, \ldots\ldots\ldots q_s$, where

$p_1, p_2, \ldots\ldots\ldots p_r, q_1, q_2, \ldots\ldots\ldots q_s$ are primes. Thus,

$k + 1 = p_1, p_2, \ldots\ldots\ldots p_r . q_1, q_2, \ldots\ldots\ldots q_s$.i.e $p(k)$ is true. Hence , by $p(n)$ is true for every $n \ni N$.

Now let us show that the factorization is unique.

Let $n = p_1, p_2, \ldots\ldots\ldots p_r = q_1, q_2, \ldots\ldots\ldots q_s$ where

$p_1, p_2, \ldots\ldots\ldots p_r. q_1, q_2, \ldots\ldots\ldots q_s$ are primes. We will use induction on t.

If $t = 1$, then $p_1 = q_1, q_2, \ldots\ldots\ldots q_s$ but p_1 is prime. Thus, its only factors are 1 and itself.

Thus, $s = 1$ and $p_1 = q_1$.

Now suppose $t > 1$ and the uniqueness holds for a product of $t - 1$ Primes. Now $p_1 | q_1, q_2, \ldots\ldots\ldots q_s$ and hence, by $p_i | q_i$ for some i. by re-ordering $q_1, q_2, \ldots\ldots\ldots q_s$ we can assume that $p_1 | q_1$. But both p_1 and q_1 are primes. Therefore, $p_1 = q_1$. But then $p_1, p_2, \ldots\ldots\ldots p_r = q_1, q_2, \ldots\ldots\ldots q_s$. so by induction, $t - 1 = s - 1$ and $p_1, p_2, \ldots\ldots\ldots p_r$ are the same as $q_1, q_2, \ldots\ldots\ldots q_s$, in some order. Hence we have proved the uniqueness of the factorization.

This theorem is also known as the **Unique Prime Factorisation Theorem.**

The primes that occur in the factorization of a number may be repeated, just as 5 is repeated in the factorization $50 = 2 \times 5 \times 5$. by collecting the same primes together we can give the following corollary to theorem.

Corollary: Any natural number n can be uniquely written as

$n = {p_1}^{m_1}, {p_2}^{m_2}, \ldots\ldots\ldots {p_r}^{m_r}$,Where for $i = 1,2,3 \ldots\ldots r.$ each $m_i \in N$ and each p_i is a prime with $1 < p_1 < p_2 < \cdots < p_r$.

As an application of theorem, we give the following important theorem, due to the ancient Greek mathematician Euclid.

1.10. SUMMARY

In this unit we have covered the following points.

1) Properties of divisibility in, like the division algorithm and unique prime factorization.
2) Proof of the indefinite of primes and its variants.
3) How to complete the gcd of two numbers from a factorization or from the Euclidean Algorithm.
4) Statement of the Fundamental Theorem of Arithmetic.

1.11TERMINAL QUESTION.

1. The value of 155 mod 9 is?

2. Find the remainders obtained on division of the following:

(a) 3^{50} by 101 (b) 159^{7654} by 23

3. If a and b are prime numbers show that

$$a^{b-1} + b^{a-1} - 1 \equiv 0(\, mod\ ab)$$

4. Prove that $(28)! - 666$ is divisible by 899.

5. Find the g.c.d. of 163 and 34 and express it in the form $163m + 34n$ in two ways.

UNIT-2 CONGRUENCES

Structure

2.1 Introduction

51 The so called Arithmetic dealt with in elementary test books was separated by the Greeks into two distinct compartments, logistica and arithmetica. The former deals with the practical applications of reckoning to trade and daily life in general. The latter which is known as the theory of Number is concerned with the properties of numbers and it is one of the most extensive and most elegent disciplines in the field of mathematics. Gauss, Lagrange, Euler, Fermat, are some of the mathematicians who contributed mnch to the development of the theory of numbers.

Congruence which has influenced many branches of mathematics, is one of the most important concepts in the theory of numbers. Its notation is the invention of Gauss. Karl Friedrich Gauss (1777 – 1855) was one of the leading mathematicians of his time. He is regarded as one of the three greatest mathematicians of all time, the other two being Archimedes and Newton. This chapter is devoted to an elementary approach to linear congruences.

2.2 Objectives.

After reading this unit the learner should be able to understand about:

- Congruence's
- Linear Congruence's
- To find the solution of Linear Congruence's
- State and proof Chines Remainder Theorem
- To Solve Chines Remainder Theorem based problem

2.3 Congruence's:

Definition: Let m be a positive integer. An integer a is said to be congruent to an integer b modulo m, denoted by $a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Example: $5 \equiv 3 \pmod{2}$. $1 \equiv 16 \pmod{5}$ $-4 \equiv 5 \pmod{3}$

$73 \equiv 33 \pmod{8}$

We write $a \not\equiv b \pmod{m}$ iff $m \nmid (a - b)$; then we say that a is incongruent to b modulo m. The following are the consequences of the definition:

$a \equiv b \pmod{m}$, iff there exists an integer k such that , $a = b + km$.

$a \equiv b \pmod{m}$, iff both a and b give the same remainder on formal division by m.

Suppose $a \equiv b \pmod{m}$. if $a < b$ and $a \leq a < m$, then a will be the remainder obtained when b is divided by m.

Theorem 2.1 If m is a given positive integer, the relation $a \equiv b \pmod{m}$ as defined above, in the set integers, is an equivalence relation.

Proof: Let a, b, c be any integers.

(1) For every a, $a \equiv a \pmod{m}$, because, zero is divisible by any integer other than zero. Hence the congruence relation is reflexive.

(2) Assume $a \equiv b \pmod{m}$. So the congruence relation is symmetric.

Since -k is also an integer, $b = a \pmod{m}$. So the congruence relation is symmetric.

(3) Assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.

By (i) $a = b + km$ and $b = c + k'm$ where $k, k' \in Z$.

$\therefore a = (c + k'm) + km = c + (k + k')m$.

Since $(k + k')$ is an integer, $a \equiv c \pmod{m}$.

Hence the congruence relation is transitive.

Thus “congruence modulo m” is an equivalence relation.

2.4 Arithmetic of Congruence's:

In this section we prove some elementary properties of congruence's.

Theorem 2.2 If $a \equiv b \pmod m$ and $c \equiv d \pmod m$

Then (i) $a + c \equiv b + d \pmod m$

(ii) $a - c \equiv b - d \pmod m$

(iii) $ac \equiv bd \pmod m$

Proof: $a \equiv b \pmod m \Rightarrow a = b + km, k \in Z$

$c \equiv d \pmod m \Rightarrow c = d + k'm, k' \in Z$

(i) $a + c = b + d + (k + k')m$ and $k + k' \in Z$

$\therefore a + c \equiv b + d \pmod m$.

(ii) $a - c = b - d + (k + k')m$ and $k + k' \in Z$

$\therefore a - c \equiv b - d \pmod m$.

(iii) $ac = bd + (kd + k'b + k'k)m$ and $kd + k'b + k'k \in Z$

$\therefore ac \equiv bd \pmod m$

Corollary: If $a \equiv b \pmod m$ and c is any integer,

Then (i) $a + c \equiv b + c \pmod{m}$

(ii) $a - c \equiv b - c \pmod{m}$

(iii) $ac \equiv bc \pmod{m}$

Check Your Progress

---

(1). Determine which of the following are true:

(a) $15 \equiv 3 \pmod{4}$ (b) $28 \equiv 0 \pmod{7}$

(c) $47 \equiv -9 \pmod{5}$ (d) $-6 \equiv -54 \pmod{12}$

(e) $-49 \equiv 3 \pmod{3}$

(2) Find any two values of k which satisfy each of the following congruences.

(a) $33 \equiv k \pmod{5}$ (b) $-14 \equiv 6 \pmod{k}$

(c) $k \equiv 5 \pmod{7}$ (d) $k \equiv -3 \pmod{6}$

(3) Find the values of $x > 0$ and less than the modulus m in each of the following congruences.

(a) $x \equiv 6 + 9 - 3 \pmod{5}$ (b) $x - 3 \equiv 15 - 49 \pmod{14}$

(c) $2x + 9 \equiv x - 14 + 12 \pmod 8$

(4) Prove that if $a \equiv b \pmod m$ and n is a positive factor of m then $a \equiv b \pmod n$

(5) Prove that if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ then $a \equiv b \pmod{m_2}$ then $a \equiv b \pmod{[m_1, m_2]}$ where $[m_1, m_2]$ is the L.C.M. of m_1 and m_2.

Given $a \equiv b \pmod m$ and $(a, m) = 1$, show that $(m, b) = 1$.

Prove that if $a \equiv b \pmod m$ then $a' \equiv b' \pmod m$ where r is a positive integer.

If p is a prime number, prove that $(a + b)^p \equiv a^p + b^p \pmod p$.

Find the first 10 powers of 7 (mod 11) with minimum effort.

[Hint : $7^2 = 49 = 5 \pmod{11}$ $7^3 = 7^2 7 = 5.7 = 2 \pmod{11}$ $7^4 = (7^2)^2 = 5^2 \pmod{11}$

$\therefore 7^4 = 3 \pmod{11}$.

Reduce the following congruences, modulo m, to the form with non-negative coefficients less than m.

(a) $55x + 3 = -15 \pmod{12}$

[we have, -3 = -3 (mod 12)

Adding 55x = -18 (mod 12)

Now -18 = 6 (mod 12)

But 55 = 7 (mod 12) $\therefore$ 55x = 6 (mod 12)

$\therefore$ 7x = 7 (mod 12)

(b) 136 x = 71 (mod 5)

(c) 48x – 23 = 34 (mod 15)

(d) (4x – 8)(3x – 5) = 10 (mod 6)

2.3 we know that the cancellation law, $c \neq 0$, $ac = bc \Rightarrow a = b$ holds for integers. Does the cancellation law for congruences, $c \neq 0 \pmod m$, $ac = bc \pmod m \Rightarrow = b \pmod m$ hold? To answer this consider the following examples:

(1) $3 \neq 0 \pmod 4$ and $3.6 = 3.2 \pmod 4 \Rightarrow 6 = 2 \pmod 4$

(2) $2 \neq 0 \pmod 4$ and $2.1 = 2.3 \pmod 4$ but $1 \neq 3 \pmod 4$

Now it is clear that the cancellation law with respect to multiplication does not always hold. The following theorem gives the condition under which it is true.

Theorem 2.3: Cancellation law: If $ac = bc \pmod m$ and $(c, m) = 1$, then $a \equiv b \pmod m$

Proof: $ac \equiv bc \pmod m \Rightarrow m\ (a - b)$

Since $(c, m) = 1$, $m \mid (a - b)$. Hence $a \equiv b \pmod m$

Theorem 2.4: If p is a prime number, $c \neq 0 \pmod p$ and $ac = bc \pmod p$, then $a \equiv b \pmod p$.

Proof: Since $c \neq 0 \pmod p$ and p is a prime number $(c, p) = 1$, Hence, by the theorem 5.3, $ac \equiv bc \pmod p$ implies $a \equiv b \pmod p$.

Theorem 2.5: If $ac \equiv bc \pmod m$, then $a \equiv b \pmod k$ where $d = (a, m)$ and $kd = m$.

Proof: Now $d = (c, m)$ and $kd = m$

Let $c = k'd$. then $(k, k') = 1$

$ac \equiv bc \pmod m$.

$\therefore ac = bc + 1\ m_n t \in Z_n$

Substituting for c and m, $ak'd = bk'd + tkd$.

$\therefore ak' = bk' + tk \Rightarrow ak' = bk' \pmod k$

Since (k, k') = 1 by the theorem 5.3, $a \equiv b \pmod{k}$.

Exercises 2.2:

1. Prove that the remainder obtained on dividing a positive integer n by 9, in equal to that on dividing the sum of the digits of n by 9.

[We know that in the decimal representation $3576 = 3.10^3 + 5.10^3 + 7.10 + 6$.

In general, if n is nay positive integer, then $n = a_0 + a_1.10 + a_3.10^2 + \ldots..+a_k.10^k$ where $a_0, a_1, \ldots..a_k$ are digits of the integer $n = a_k a_{k-1} \ldots\ldots a_1 a_0$.

Since $10 = 1 \pmod 9$ $\quad \therefore 10^r = 1 \pmod 9$ for any $r \in Z$

$\therefore a_0 + a_1.10 + a_2.10^2 + \ldots\ldots + a_k 10^k \equiv a_0 + a_1 + a_2 + \ldots\ldots + a_k \pmod 9$

2. Prove that we can replace 9 by 3

3. Prove that $11 \mid n$ iff $11 \mid [a_0 - a_1 + a_2 - \ldots\ldots\ldots + (-1)^k a_k]$. Where the decimal representation of n is $a_0 + a_1.10 + a_2.10^2 + \ldots\ldots + a_k 10^k$.

4. If $a_0, a_1, a_2, a_3, a_4, a_5$ are the digits commencing from the units place, in the decimal notation of a number n, prove that $n = (a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5) \pmod 7$

2.4 Residue Classes.

Theorem 2.6 If m is a positive integer, no two integers of the set S = {0, 1, 2, …..(m – 1)} are congruent modulo m and every integer is congruent modulo m to one and only one integer of S.

Proof: Let b and c be any two distinct elements of S since 0≤ b, c < m and b ≠ c, $0 < |b - c| < m,$ and m ∤ (b – c). Hence b ≠ c (mod m).

Let a be any integer. By the division algorithm for the integers a and m, there exists unique integers q and r such that a = qm + r, 0 ≤ r < m. Therefore a ≡ r (mod m) and r ∈ S.

Since r is unique for a given pair a and m, any integer a is congruent (mod m) to one and only one integer ∈ S.

Definition: The set {0, 1, 2, …..(m – 1)} is called "the set of the least non-negative residues modulo m"

Definition: The set of all integers which give the remainder r, when divided by a positive integer m is called "the r-residue class modulo m" and is denoted by the symbol $\bar{r}$ (mod m).

The integer of r-residue class modulo m, are of the form r + km where k is an integer. Thus r = {……..r – 2m, r – m, r, r + m, r + 2m ……}

[Show that $\bar{r} = \bar{s}$ for any s. $\in \bar{r}$]

The elements of $\bar{r}$ are the terms of an arithmetic progression of common difference m and are mutually congruent (mod m). Thus it is easily seen that a residue class is an equivalence class.

As there are only m non-negative integers less than m, there exist exactly m residue classes (mod m)

For example, the five residue classes modulo 5 are

0 = {……-10, -5, 0, 5, 10 , ….}

$\bar{1}$ = {……..-9, -4, 1, 6, 11, …..}

$\bar{2}$ = {…….-8, -3, 2, 7, 12, …..}

$\bar{3}$ ={…….-7, -2, 3, 8, 13,…….}

$\bar{4}$ = {…….-6, -1, 4, 9, 14, ……}

Theorem 2.7. Let m be any positive integer, and $\bar{s}$ and $\bar{t}$ residue classes (mod m).

If $\bar{s} \cap \bar{t} \neq \emptyset$, then $\bar{s} = \bar{t}$.

Proof: Let $x \in \bar{s} \cap \bar{t}$ then $x \in \bar{s}$ and $x \in \bar{t}$

This implies that x = s + km and x = t + lm by subtraction, 0 = (x – t) + (k – l)m.

$\therefore$ s ≡ t (mod m)

$\therefore \bar{s} = \bar{t}$ thus $\bar{s} \cap \bar{t} \neq \emptyset \Rightarrow \bar{s} = \bar{t}$

The contrapositive of the above theorem viz., $\bar{s} \neq \bar{t} \Rightarrow \bar{s} \cap \bar{t} \neq \emptyset$, is true.

That is , distinct residue classes have no element in common.

Now it is clear that the equivalance relation, congruence (mod m) decomposes the set Z of all integers into m distinct, equivalence classes which are none other than the m residue classes (mod m).

2.5 Special Residue Systems (mod m)

Let $\bar{0}, \bar{1}, \ldots\ldots\ldots\bar{\imath}, \ldots\ldots\ldots\overline{(m-1)}$, be the m residue classes (mod m).

Then the set S = $\{x_0, x_1. \ldots\ldots x_{n-1}\}$ where each $x_i \in \bar{t}$ for all i = 0, 1, 2, ….., (m – 1) is called a complete system of residues (mod m).

Examples: (1) {0, 1, 2, …….(m – 1)} is the complete system of least non-negative residues (mod m).

(2) {1, 2, ……, m} is the complete system of least positive residues (mod m).

(3) $\left\{-\left(\frac{m}{2}\right), \ldots\ldots\ldots -2, -1, 0, 1, 2, \ldots\ldots\ldots \frac{m}{2}\right\}$ is the completes system of residues (mod m), of least absolute value where m is even.

When m is odd this will be $\left\{-\left(\frac{m-1}{2}\right), \ldots\ldots\ldots -2, -1, 0, 1, 2, \ldots\ldots\ldots \frac{m-1}{2}\right\}$

(4) Any m consecutive numbers will form a complete residue system (mod m). Prove.

Check Your Progress

---

1) If (a, m) = 1 and x is in the residue class $\bar{a}$ (mod m), Prove that (x, m) = 1.

2) If (x_1, x_2, ……x_m) is a complete set of residues modulo m, prove that {$ax_1 + b$, $ax_2 + b$, ……$ax_m + b$} is a complete set of residues modulo m provided (a, m) = 1.

Out line of proof:- Show that $ax_i + b = ax_j + b \pmod m \Rightarrow i = j$

∴ if p_0, p_1, ……p_{m-1} are the least non negative residues (mod m) of thse numbers, then, p_0, p_1, ……p_{m-1} are only 0, 1, 2, ……, (m – 1) in some order.

In particular, choosing (x_1, x_2, ……x_m) = 0, 1, 2, ……, (m – 1) we find that {b, b + a, b + 2a, ……..b + (m – 1)a} is a complete residue system modulo m.

∴ The number of numbers among {b, b + a, b + 2a, ……..b + (m – 1)a} which are relatively prime to m is the same as that of numbers among 0, 1, 2, ……, (m – 1) which are relatively prime to m, i.e. to $\emptyset(m)$.

Hence we may state the following proposition:-

If a is relatively prime to m, the number of terms in the arithmetical progression:

b, b + a, b + 2a, ……..b + (m – 1)a which are relatively prime to m is $\emptyset(m)$.

2.6 Alternative Development of the formula for the Euler's Totient $\emptyset(m)$.

The proposition obtained above can be used with the advantage of simplicity, to prove the multiplicative property of $\emptyset(m)$, and hence to derive the formula for$\emptyset(m)$.

Theorem 2.8 If m and n are relatively prime, the $\emptyset(mn) = \emptyset(m).. \emptyset(n)$.

Proof: Let us arrange the numbers 1, 2, 3, ……..mn is n rows and m columns as shown below:

1	2	l	m	
m + 1	m + 2	m + 1	2m,	
2m + 1	2m + 1	2m + 1	3m,	
……	……	……	……..	
(n – 1)m – 1	(n – 1)m – 2	(n – 1)m + 1	nm	

Since (m, n) = 1, any number which is relatively prime to mn is relatively prime to both m and n.

$\therefore \emptyset(mn)$ is the number of numbers from 1 to mn which are relatively prime to both m and to n. Each of the numbers in the column headed by 1 will be relatively prime to m iff I is relatively prime to m. Thus, there are exactly $\emptyset(m)$ columns in the above arrangement, which contain numbers from 1 to nm, which are relatively prime to m.

Now each column is an arithmetical progression containing n terms. Each column contains $\emptyset(n)$ numbers which are relatively prime to n.

Thus the numbers which are relatively prime to both m and n are actually the numbers which are relatively prime to n found in each of the $\emptyset(m)$ columns headed by the $\emptyset(m)$ numbers which are relatively prime to m; and in each such column there are $\emptyset(n)$ such numbers. Hence the number of numbers which are relatively prime to both m and n and hence to mn is equal to $\emptyset(m).\emptyset(n)$.

$\therefore \emptyset(mn) = \emptyset(m).\emptyset(n)$

corollary: If $m_1, m_2, \ldots\ldots m_k$ are relatively prime to one another, then

$\emptyset(m_1, m_2, \ldots\ldots m_k) = \emptyset(m_1).\emptyset(m_2)\ldots\ldots\emptyset(m_k)$,

For $(m_1, m_2, \ldots\ldots m_k)$ = the g.c.d. of $m_1, m_2, \ldots\ldots m_k = 1$

∴ $\emptyset(m_1, m_2, \ldots\ldots m_k) = \emptyset(m_1).\emptyset(m_2)\ldots\ldots\ldots \emptyset(m_k)$, and so on.

Theorem 2.9 If p is a prime, then $\emptyset(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$

Proof: When $\alpha = 1$, the result is obviously true.

When $\alpha > 1$, consider the numbers 1, 2, 3, ……p^α

Among them those that are not relatively prime to p^α are p1.p2.p3.p……..$p^{\alpha-1}$.p .

Their number is $p^{\alpha-1}$

∴ Number of numbers less than p^α and relatively prime to it

$$= (p^\alpha) - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

Corollary: Let $m = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots\ldots\ldots\ldots\ldots\ldots\ldots p_k^{\alpha_k}$

Be the canonical resolution of m into the production of powers of distinct primes $p_1, p_2, \ldots..p_k$.

∴ by theorem 2.8, we have

$$\emptyset(m) = \emptyset\left(p_1^{\alpha_1}\right).\emptyset\left(p_2^{\alpha_2}\right)\ldots\ldots\ldots\emptyset\left(p_k^{\alpha_k}\right)$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right).p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\ldots\ldots..p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$$

$$\therefore \quad \emptyset(m) = m\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots \left(1 - \frac{1}{p_k}\right)$$

Which is the required formula for $\emptyset(m)$

2.7 The Linear Congruence

A Congruence of the form ax ≡ b (mod m) is called a "linear congruence" in x. An integer α which when substituted for x satisfies the congruence, is called a "solution" or a "root" of the congruence.

Example: 5 is a root of the congruence 3x ≡ 1 (mod 7), -2, 12, 19 are also roots of this congruence. Note that they are all congruent to one another (mod 7).

If α is a solution of ax ≡ b (mod m), then all the integers which are congruent to α (mod m) are also its solutions. In other words, all the integers of the residue class α (mod m) satisfy the congruence.

For, if α' ≡ α (mod m) then aα' ≡ aα (mod m). Since α is a solution aα = b (mod m). by the transitivity of congruence aα' ≡ b (mod m). This implies that α' is a solution.

Therefore we find that whenever α is a root of (1) $ax = b \pmod m$, then any integer from the residue class $\bar{\alpha} \pmod m$, is also a solution. So we write this solution in one of the forms $x = \alpha \pmod m$ or $x = \bar{\alpha} + tm$ where $t \in Z$.

It may turn out as will be seen in example 3 given below, that (1) has another root $\beta \neq \alpha \pmod m$, i.e. $\notin \bar{\alpha}$: then we say that α and β are two distinct (mod m) or incongruent (mod m) roots; of the congruence (1). Thus in counting the number of roots of a given congruence, we take into account only incongruent (mod m) roots.

Consider the following example:

---

(1) $2x = 3 \pmod 4$

By substituting each of the integers 0, 1, 2, 3, in succession, we find that none of them satisfies the congruence. Therefore it has no solution in any one of the residue classes $\bar{0}, \bar{1}, \bar{2}$ and $\bar{3}$. But these classes comprise all the integers. Thus the congruence has no solution.

(2) $3x = 1 \pmod 5$

Among the integers 0, 1, 2, 3, 4 only 2 satisfies the congruence.

Hence the congruence has the unique solution $x \equiv 2 \pmod 5$ or $x = 2 + 5t.$, $t \in Z$.

(3) $2x \equiv 4 \pmod 6$ Of the integers, 0, 1, 2, 3, 4, 5, both 2 and 5 satisfy the congruence.

Hence the congruence has 2 solution, namely $x = 2 + 6t$ and $x = 5 + 6t$ where $t \in Z$.

Thus a linear congruence may or may not have a solution. It may even have more than one solution whereas a linear algebraic equation has one and only one solution. The following two theorems reveal the conditions for the existence of a solution and the number of solution when they exist.

Theorem 2.10 If $(a,m) = 1$, then $as \equiv b \pmod m$ has a unique solution.

Proof:- Since $(a, m) = 1$, there exists two integers p and q such that $pa + qm = 1$

$\therefore$ $bpa + bqm = b$

$A(pb) = b + (-qm)m$ and $-qb \in Z$.

$\therefore$ a . (pb) = b (mod m)

Thus p b is a solution of $ax \equiv b \pmod{m}$

If possible, let a be another solution of $ax \equiv b \pmod{m}$. then $a\alpha \equiv b \pmod{m}$. by symmetric and transitive properties of congruence, $a\alpha \equiv apb \pmod{m}$. Since (a, m) = 1 by the cancellation law, $a \equiv pb \pmod{m}$. That is α and pb are not incongruent solutions. Hence the solution is unique.

Theorem 2.11 Let ax = b (mod m) and (a, m) = d.

Then (i) if $d \nmid b$, the congruence has no solution.

(ii) if $d \mid b$, the congruence has exactly d solutions.

Proof:- (i) $ax \equiv b \pmod{m}$

1 let $d \nmid b$, if (i) has a solution x_0 then $ax_0 \equiv b \pmod{m}$

And $ax_0 = b + km$ $(k \in Z)$

Since d = (a, m) $d \mid a$ and $d \mid m$

$\therefore$ $d \mid ax_0 - km$. i.e., $d \mid b$.

This is a contradiction

$\therefore$ if $d \nmid b$ (1) has no solution

(ii) let $d \mid b$, then $b = dB$.

$d = (a, m)$ $\therefore a = Ad$, $m = Md$ and $(A, M) = 1$.

$\therefore$ on substitution in (1) we get

$Adx = Bd \pmod{Md}$

$\therefore Md \mid Adx - Bd \Rightarrow M \mid Ax - B$.

$\therefore Ax \equiv B \pmod{M}$……(2)

Since $(A, M) = 1$, by the theorem 5.8. It has a unique solution. Let it be $\alpha + tM$, $(t \in Z)$.

Now we shall prove that $\alpha + tM$ is a solution of (1) also

Since $\alpha + tM$ is a solution of (2), $M \mid A(\alpha + tM) - B$.

$\therefore Md \mid Ad(\alpha + tM) - Bd$.

$\therefore m \mid a(\alpha + tm) - b$.

$\therefore a(\alpha + tm) \equiv b \pmod{m}$

$\therefore \alpha + tm$ is a solution of $ax \equiv b \pmod{m}$

Thus every solution of (2) is a solution of (1) also.

III. Consider $S = (\alpha. A + M, \alpha + 2M, \ldots\ldots \alpha + (d - 1)M)$ which is a subset of $\bar{\alpha} \pmod{M}$. Clearly, the elements of S are the solutions of (2). Hence those of (1) also.

Now let us prove that any integer of the form $\alpha + tM$ is congruent (mod m) to one and only one element of S.

By the division Algorithm, $t = qd + r$, $0 \leq r < d$ and q, r are unique.

$\therefore \alpha + tM = \alpha + (qd + r)M = \alpha + rM + qdM = (\alpha + rM) + qm$

$\therefore \alpha + tM \equiv \alpha + rM \pmod{m}$

Since $0 \leq r < d$, $\alpha + rM \in S$. Since r is unique $\alpha + rM$ is congruent (mod m) to one and only one element of α.

IV Now we shall prove that the elements of S are incongruent modulo m.

Assume $\alpha + rM = \alpha + sM \pmod{m}$ where $\alpha + rM, \alpha + sM \in S$, i.e. $0 \leq r, s < d$.

Then $rM \equiv sM \pmod{m}$

$r \equiv s \pmod{d}$ since $m = Md$.

Since $0 \leq r, s < d$, $r \neq s \pmod{d}$. This is a contradiction. $\therefore \alpha + rM \neq \alpha + sM \pmod{m}$. Thus the elements of S are incongruent (mod m) and consequently S contains exactly d distinct elements.

Hence by (III) and (IV) it follows that $ax \equiv b \pmod{m}$ has exactly d solutions and they are the elements of the set S.

Note in general we write the d solutions of (1) as

$\alpha + tm, \alpha + \frac{m}{(a,m)} + tm, \alpha + \frac{2m}{(a,m)} + tm$ ……

$\alpha + \frac{(d-1)m}{(a,m)} + tm$, where t is any integer and α is the solution of (2) which is called the reduced congruence of (1).

5.8 The following examples illustrate several indirect and easy ways of solving linear congruences.

Example I. Solve $2x \equiv 3 \pmod{5}$.

$(2, 5) = 1$ and $1 \mid 3$. Hence by the theorem 5.9, it has only one solution.

Now let us find the solution.

I Method: Of the integers 0, 1, 2, 3, 4, it can be easily verified that only 4 satisfies the congruence. Therefore 4 is the solution or $x \equiv 4 \pmod 5$ is the solution.

II Method: $3 \equiv 8 \pmod 5$ Hence $2x \equiv 8 \pmod 5$.

2, the common factor of 2 and 8, is prime to 5.

$\therefore x \equiv 4 \pmod 5$

4 is the solution or $x \equiv 4 \pmod 5$ is the solution.

III Method: $2x \equiv 3 \pmod 5$.

Since it has a solution $2x = 3 + 5k$, where $x, k \in Z$.

$x = \frac{3+5k}{2}$ is an integer.

$\frac{3+5k}{2} = 2k + 1 + \frac{1+k}{2}$

$\frac{1+k}{2}$ must be an integer. Let $\frac{1+k}{2} = t$. Then $k = 2t - 1$.

Setting $t = 0$, we get $k = -1$. Hence $x = -1$ or $x = -1 \pmod 5$

i.e. $x \equiv 4 \pmod 5$ is the solution.

Example 2. Find all the integers x, $-20 < x \leq 20$ satisfying the congruence $2x \equiv 3 \pmod 5$

From the example (1) 4 is a solution. All the integers congruent to 4(mod 5) satisfy the congruence. Hence the required integers are 4, 4 + 5, 4 + 2 x 5, 4 + 3 x 5, 4 – 5, 4 – 2 x 5, 4 – 3 x 5, 4 – 4 x 5, i.e. 4, 9, 14, 19, -1, -6, -11, -16.

Example 3. Solve $150x \equiv 4 \pmod{31}$.

$(150, 31) = 1$. And $1 \mid 4$, $\therefore$ it has only one solution.

Since 31 is a big number, the I method described in example (I), is laborious.

I Method: Now $150 \equiv -5 \pmod{31}$

Since $150x \equiv 4 \pmod{31}$ $\therefore -5x = 35 \pmod{31}$

$4 \equiv 35 \pmod{31}$ $\therefore -5x = 35 \pmod{31}$

-5, the common factor of -5 and 35, is relatively prime to 31.

$\therefore x \equiv -7 \pmod{31}$

$\therefore x \equiv 24 \pmod{31}$. It is the solution.

II Method: $150x \equiv 26 \pmod{31} \Rightarrow -5x \equiv 4 \pmod{31}$

$-5x = 4 + 31k$

$X = -\frac{(4+31k)}{5} = -6k - 1 - \frac{k-1}{5}$

Setting $\frac{-1+k}{5} = t$, $k = 5t + 1$.

Taking $t = 0$, we get $k = 1$ and $x = -7$

$\therefore x \equiv -7 \pmod{31}$ i.e., $x \equiv 24 \pmod{31}$

Example 4: Solve $36x + 12 \equiv 0 \pmod{15}$

$36x = -12 \pmod{15}$ ..... (1)

$(36, 15) = 3$, $3 \mid (-12)$. Therefore it has 3 solutions, the reduced congruence of (I) is obtained by dividing figures in (1) by 3. Thus $12x \equiv$

-4 (mod 5), $2x \equiv -4 \pmod 5$. 2 is the g.c.d. of 2 and -4 and $(2, 5) = 1$, $\therefore x \equiv -2 \pmod 5$, $x \equiv 3 \pmod 5$.

Thus 3 is a root of (2)

The first three values of x satisfying (2) are 3, $3 + 1 \times 5 = 8$ and $3 + 2 \times 5 = 13$. Thus the solutions of (1) are $3 + 15t$, $8 + 15t$ and $13 + 15t$ where $t \in Z$. They can also be written as $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$ and $x \equiv 13 \pmod{15}$.

Example 5. Find all integer x, $-10 \leq x \leq 40$ satisfying the congruence $36x \equiv -12 \pmod{15}$. From the example, 4. The solutions of the congruence are $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$ and $x \equiv 13 \pmod{15}$.

The integers congruent to 3 (mod 15) and lying between -10 and 40 are 3, 18, 33. The integers between – 10 and 40 and congruent to 8 (mod 15) and 13 (mod 15) are -7, 8, 23, 38 and -2, 13, 28 respectively.

Thus the required integers are -7, -2, 3, 8, 13, 18, 23, 28, 33 and 38.

Check Your Progress

---

1. Find b in order that the following linear congruences may have solutions.

   (a) $15x \equiv \pmod{16}$ (d) $15x \equiv b \pmod{63}$

   (b) $6x \equiv b \pmod{15}$ (e) $8x \equiv b \pmod{13}$

   (c) $5x \equiv b \pmod{35}$ (f) $11x \equiv b \pmod{17}$

2. Find all integers between -40 and 30 which satisfy the following congruences.

   (i) $3x \equiv 2 \pmod{11}$ (iii) $10x \equiv 8 \pmod{14}$

   (ii) $36x \equiv -12 \pmod{8}$ (iv) $8x \equiv 12 \pmod{16}$

3. Solve the following:-

   (i) $16x \equiv 25 \pmod{17}$ (vi) $121x \equiv 21 \pmod{17}$

   (ii) $89x \equiv 15 \pmod{40}$ (vii) $4x + 9 \equiv 3 \pmod{15}$

   (iii) $37x \equiv 51 \pmod{34}$ (viii) $5x + 3 \equiv 2x - 1 \pmod{35}$

   (iv) $6x \equiv 52 \pmod{24}$ (ix) $117x \equiv 45 \pmod{360}$

   (v) $24x \equiv 12 \pmod{30}$ (x) $66x \equiv 121 \pmod{737}$

2.9 Simultaneous Congruences

We shall describe a method of solving simultaneous congruence of the form $x_i = a_i \pmod{m}$ $i = 1, 2, \ldots\ldots\ldots k$. In this connection we state and prove a theorem for a set of two congruences: it can be generalised easily.

Theorem 2.12 The Chinese Remainder theorem

If $(m_1, m_2) = 1$, then the congruences (1) $x \equiv a_1 \pmod{m_1}$ and (2) $x \equiv a_2 \pmod{m_2}$ have a common solution which is unique modulo m_1m_2.

Proof: The solution of (1) is $a_1 + k_1m_1$, where k_1 is an integer. Suppose this is a common solution of (1) and (2). $\therefore a_1 + k_1m_1 \equiv a_2 \pmod{m_2}$. $\therefore k_1m_1 \equiv (a_2 - a_1) \pmod{m_2}$. Since $(m_1, m_2) = 1$, k_1 has a value which satisfies the congruence and it will be of the form $b + k_2m_2$ where b and k_2 are integers. Therefore the common solution is

$$a + k_1m_1 = a_1 + (b + k_2m_2)m_1 = (a_1 + bm_1) + k_2m_1m_2$$

$$\therefore a_1 + k_1m_1 \equiv (a_1 + bm_1) \pmod{m_1m_2}$$

Thus the common solution of (1) and (2) is an integer congruent to $a_1 + bm_1 \pmod{m_1m_2}$

Now let us prove the uniqueness of the solution. Suppose α and β are two common solutions. Then $\alpha \equiv a_1 \pmod{m_1}$ and $\beta \equiv a_1 \pmod{m_1}$ $\therefore \alpha \equiv \beta \pmod{m_1}$, Thus $m_1/(\alpha - \beta)$. Similarly it can be proved that $m_2//(\alpha - \beta)$

Since $(m_1, m_2) = 1$, $m_1m_2 \mid /(\alpha - \beta)$. That is $\alpha \equiv \beta \pmod{m_1m_2}$. Thus the solution is unique.

The following is the formal generalisation of the above theorem. :if m_1, m_2, ……m_r are relatively prime to each other, then the congruences $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$…..$x \equiv a_r \pmod{m}$ have a common solution which is unique modulo (m_1m_2,….m_r)

Example I. Solve the simultaneous congruences. (i) $x \equiv 3 \pmod 5$ and (ii) $x \equiv 4 \pmod 7$.

Let the solution, $3 + 5k$ of (i) be a solution of (ii)

Then $3 + 5k \equiv 4 \pmod 7$.

$$5k \equiv 1 \pmod 7$$

Solving for k, we get $k \equiv 3 \pmod 7$ i.e. $k = 3 + 7k'$ where $k' \in Z$. Hence the common solution of (i) and (ii) is $(3 ' + 5k) = 3 + 5(3 + 7k') = 18 + 35k'$

i.e., $x \equiv 18 \pmod{35}$

Example 2. Find two least positive integers which give remainders 2, 3, 2 when divided by 3, 5, 7 respectively. (An old Chinese problem. Sun tsu – first Century).

Suppose x is one of the required integers. Then (i) $x \equiv 2 \pmod 3$, (ii) $x \equiv 3 \pmod 5$ and (iii) $x \equiv 2 \pmod 7$.

Thus x is a common solution of (i), (ii) and (iii).

Let $x = 2 + 3k$, be a solution of (i) then from (ii) $2 + 3k \equiv 3 \pmod 5$.

Solving this we get $k_1 \equiv 2 \pmod 5$, i.e. $k_1 = 2 + k_2\, 5$.

Hence $x = 2 + 3(2 + 5k_2) = 8 + 15k_3$

Substituting in (iii), $8 + 15k_2 = 2 \pmod 7$.

Solving for k_2, we get $k_2 = 1 \pmod 7$ $k_2 = 1 + 7k_3$.

Therefore $X = 8 + 15(1 + 7k_2) = 23 + 105k_2$

$$x = 23 \pmod{105}$$

The required two smallest positive integers are 23 and $23 + 105 = 128$

Example: Let n and k be positive integers. Show that there exists a sequence of n consecutive composite integers such that each is divisible by at least k distinct prime numbers. Using this result, find the smallest sequence of four consecutive integers divisible by 3,5,7 and 11 respectvely.

Solution: Let p_r stand for the r-th prime number. for each integer $i, 1 \leq i \leq n$, let $m_i = p_{(i-1)k+1}.p_{(i-1)k+2}.p_{(i-1)k+3}.....p_{ik-1}.p_{ik,}$ and consider the system of congruences

$$\begin{cases} \boldsymbol{x \equiv -1} & \boldsymbol{(mod\ m_1)} \\ \boldsymbol{x \equiv -2} & \boldsymbol{(mod\ m_2)} \\ & . \\ & . \\ & . \\ & . \\ & . \\ \boldsymbol{x \equiv -n} & \boldsymbol{(mod\ m_n)} \end{cases}$$

Since the $m_i's$ are pairwise coprime, the Chinese Remainder theorem guarantees a solution x_0.

Then, $m_1|(x_0+1), \ldots . m_n|(x_0+n)$. Therefore, $x_0+1, x_0+2, \ldots \ldots . x_0+n$ is a sequence of n consecutive intgers which are divisible by at least k prime numbers.

For the second part ($n = 4\ and\ k = 1$), we must solve

$$\begin{cases} x \equiv -1\ (mod\ 3), \\ x \equiv -2\ \ (mod\ 5), \\ x \equiv -3\ \ \ (mod\ 7), \\ x \equiv -4\ \ (mod\ \ 11). \end{cases}$$

In this case,$x \equiv 788\ (mod\ 1155)$and therefore $x_0 = 788$. The four numbers are therefore 789,790,791 and 792.

Check Your Progress

---

1. Solve the following simultaneous congruences.

(a) $x \equiv 2\ (\text{mod } 3), x \equiv 3\ (\text{mod } 7)$

(b) $x \equiv 4\ (\text{mod } 9), x \equiv 7\ (\text{mod } 12)$

(c) $x \equiv 5\ (\text{mod } 11), x \equiv 6(\text{mod } 5), x \equiv 3\ (\text{mod } 4)$

2. Find three least positive integers which leave the remainders 2, 3, 4 when divided by 3, 4, 5 respectively.

3. Find a number having remainders 2, 3, 4, 5 when divided by 3, 4, 5, 6 respectively (Brahmaguptha – 7^{th} century)
4. A father has 7 children of whom 4 were sons. When he divided gold coins that he has equally among his children 5 were left over and when divided among his daughters 1 was left over. Find the smallest number of coins he had.

2.10 Classical Theorem

We shall now prove some important classical theorems on congruences.

Fermat (1601 - 65), the founder of modern number theory discovered a most important theorem known as Fermat's theorem. It is of indispensable use in many branches of mathematics the first proof was given by Leibnitz.

Theorem 2.13 Fermat's theorem: If p is a prime number and p ł a then $a^{p-1} = 1 \pmod{p}$.

To prove this, let us prove the more general theorem "If p is a prime number and a is any integer, $a^p = a \pmod{p}$".

Proof:- Case (I) Let a be a positive integer $1^p = 1 \pmod p$. Hence the theorem is true when $a = 1$.

Assume the theorem to be true when $a = r$, i.e. $r^p = r \pmod p$

Now $(r + 1)^p = r^p + {}_pC_1 r^{p-1} + \ldots\ldots\ldots + {}_pC_{p-1} r + 1^p$

${}_pC_i = 0 \pmod p$ for $(1 \leq i \leq p - 1)$ because p is a prime

$\therefore\ (r + 1)^p \equiv r^p + 1^p \pmod p$

Bur, by the assumption it follows that $(r^p + 1^p) \equiv r + 1 \pmod p$

Hence $(r + 1)^p = r + 1 \pmod p$. Thus the theorem is true when $a = r + 1$.

Therefore by induction, the theorem holds for all positive integers a.

Case 2 The theorem is clearly true when $a = 0$

Case 3 Let a be a negative integer and $a = -b$ where b is a positive integer.

Then by Case (i) $b^p = b \pmod p$

$\therefore\ \ -b^p = -b \pmod p$

$\therefore\ (-b)^p = -b \pmod p$ when p is an odd prime.

When $p = 2$, $b^2 + b = (-b)^2 + b = -b(-b - 1) = 0 \pmod 2$

$\therefore ap = a \pmod p$, for all prime p.

Thus $ap = a \pmod p$ for all a and for any primes p.

Now if $p \nmid a$, p being a prime $(a, p) = 1$

By cancellation law $a^{p-1} = 1 \pmod p$

Now we state and prove a lemma which will be used in the proof of a more general theorem which includes Fermat's theorem as a particular case.

Lemma: if $(a_1, m) = 1$ and $(a_2, m) = 1$ then $(a_1a_2, m) = 1$.

For, if $(a_1a_2, m) =$ gthen $g|a_1a_2, p|m$.

If now $g > 1$, then it has a prime factor p, where $p \mid g$ and $g \mid a_1a_2$

$\therefore p \mid a_1a_2$

Since p is a prime number , $p \mid a_1$ *or* $p \mid a_2$

Therefore $(a_1, m) \neq 1$, $(a_2, m) \neq 1$ which is a contradiction to the hypothesis,

$\therefore g \not> 1, g = 1$

Theorem 2.14 Euler's Theorem: If (a, m) = 1 then $a^{\emptyset(m)} = 1(\text{mod } m)$,

Proof:- Let $S = \{r_1, r_1, \ldots\ldots\ldots\ldots r_{\emptyset(m)}\}$, where the elements of S are positive integers each less than and prime to m.

{S is called the reduced system of least positive residues (mod m)}

1. Consider the set $S' = \{r_1, r_1, \ldots\ldots\ldots\ldots r_{\emptyset(m)}\}$,

The elements are incongruent (mod m). For, if $(s \neq t)$ and $ar_r \equiv ar_t$ (mod m). then a being prime to m, $r_s \equiv r_t$ (mod m). But $r_s \neq r_t$ and $0 < r_s, r_t < m$ $\therefore r_s \neq r_t$ (mod m). This contradicts $r_s \equiv r_t$ (mod m) $\therefore ar_t \neq ar_s$ (mod m).

II. Each ai, $1 \leq i \leq \emptyset(m)$ is prime to m and a is prime to m. Hence, by the Leema each ar_i is prime to m.

The remainder A_i that is obtained when ar_i is divided by m, is also prime to m (Exercise V,.I problem 6) $\therefore A_i \in S$.

Now, the elements of S are incongruent (mod m) and all the remainders are elements of S. Besides they are all distinct.

Hence $ar_1 \equiv A_1 \pmod{m}$

$ar_2 \equiv A_2 \pmod{m}$

……..

$ar_{\emptyset(m)} \equiv A_{\emptyset(m)} \pmod{m}$

and $A_1A_2\ldots\ldots A_{\emptyset(m)} = r_1r_2\ldots\ldots r_{\emptyset(m)}$

Multiplying these congruences

$ar_1.ar_2\ldots\ldots ar_{\emptyset(m)} = A_1.A_2\ldots\ldots A_{\emptyset(m)} \pmod{m}$

$= r_1.r_2\ldots\ldots r_{\emptyset(m)} \pmod{m}$

Since (ri, m) = 1 for $1 \leq i \leq \emptyset(m)$, by the cancellation law $a^{\emptyset(m)} = \text{mod}$ (m)

Corollary: Fermat's Theorem

If p is a prime number and p ∤ a then $a^{p-1} = 1 \pmod{p}$

Proof:- p is a prime number and p ∤ a. ∴ (p, a) = 1. Hence by Euler's theorem $a^{p(m)} = 1 \pmod{p}$. But $\emptyset(m) = p - 1$ ∴ $a^{p-1} = 1 \pmod{p}$

Theorem 2.15 Lagrange's Factor Theorem.

Let f(x) be a polynomial. If a is root of $f(x) \equiv 0 \pmod m$, then there exists a polynomial g(x) such that $f(x) = (x - a)g(x) \pmod m$ and conversely.

Proof: Suppose that a is a root of $f(x) \equiv 0 \pmod m$. Then $f(a) \equiv 0 \pmod m$. By the division of f(x) by (x – a), $f(x) = (x - a)g_e(x) + r$.

Suppose that the coefficients of $g_e(x)$ are replaced by their least non negative residues (mod m) and the polynomial so obtained is denoted by g(x). Then $g(x) = g_e(x) \pmod m$

$\therefore f(x) \equiv (x - a)g(x) + r \pmod m$.

Substituting a or any integer congruent to a (mod m) for x.

$f(a) \equiv (a - a)g(a) + r \pmod m$.

Since $f(a) \equiv 0 \pmod m$, $0 \equiv r \pmod m$

$f(x) \equiv (x - a)g(x) \pmod m$

Conversely, if $f(x) \equiv (x - a)g(x) \pmod m$ then a is a root of $f(x) \equiv 0 \pmod m$.

For $f(x) = (x - a)\, g(x) \pmod m \Rightarrow f(a) \equiv 0 \pmod m \Rightarrow$ a is a root of $f(x) \equiv 0 \pmod m$.

Definition: The congruence $f(x) \equiv 0 \pmod p$ is said to be of degree n, if the polynomial f(x) is of degree n.

Theorem 2.16. The congruence $f(x) \equiv 0 \pmod p$ where the polynomial $f(x) = a_0x' + a_1a^{n-1} + a_n$, $a_0 \neq 0 \pmod p$ has at most n roots where p is a prime.

Proof:- (1) When the degree of f(x) is one, the congruence will be a linear congruence, since $a_0 \neq 0 \pmod p$ and p, being a prime $(a_0, p) = 1$. By theorem 5.8 it has one solution. Thus the theorem is true when $n = 1$.

(2) Assume that every congruence of degree r has at most r roots. Lets a be a root of the $(r + 1)$th degree congruence, $f(x) = 0 \pmod p$, where $f(x) = a_0x^{r+1} + a_1x^r + \ldots\ldots\ldots a_{r+1}$. Then by the factor theorem $f(x) \equiv (x - a)\, g(x) \pmod p$. Where g(x) is of degree r. By our assumption $g(x) \equiv 0 \pmod p$ has at most r roots. Let them be $c_1, c_2, \ldots\ldots\ldots\ldots c_r$, where $a < s \leq r$.

If c is a root of $f(x) \equiv 0 \pmod p$ then $(c - a)\, g(c) \equiv 0 \pmod p$. Hence p being a prime number either $c - a \equiv 0 \pmod p$ or $g(c) \equiv 0 \pmod p$. Thus

either $c \equiv a \pmod{p}$ or c is one of the values $c_1, c_2, \ldots\ldots\ldots\ldots c_s \pmod{p}$. Therefore $f(x) \equiv 0 \pmod{p}$, whose degree is $(r + 1)$ has $(x + 1)$ roots, where $s \leq r$. i.e. $s + 1 \leq r + 1$.

The theorem is true for a congruence of degree $r + 1$. Hence by the first principle of induction of theorem follows.

Theorem 2.17. If p is a prime and r is any positive integer; less than $(p - 1)$ and the sum of all the products of integers 1, 2, ……..$(p - 1)$ taken r at a time, is denoted a_r, then $a_r \equiv 0 \pmod{p}$.

Proof:- p being a prime number, by Fermat's theorem 1, 2, 3, ……..$(p - 1)$ are the roots of $x^{p-1} \equiv 1 \pmod{p}$, because 1, 2, 3, …….$(p - 1)$ are relatively prime to p. By the theorem 5.14, it can not have any more roots.

Hence $x^{p-1} - 1 \equiv (x - 1)(x - 2) \ldots\ldots\ldots\ldots\ldots (x - p + 1) \pmod{p}$ is an identity. That is, for all integers x, this is a true congruence. Since $x^{p-1} \equiv 1 \pmod{p}$.

$(x - 1)(x - 2) \ldots\ldots\ldots\ldots\ldots (x - p + 1) \equiv 0 \pmod{p}$

$\therefore x^{p-1} - a_1x^{p-2} + a_2x^{p-3} - \ldots\ldots\ldots\ldots\ldots\ldots - a_{p-2}x + (p - 1)! \equiv 0 \pmod{p}$

Where ar, denoted the sum of the integers 1, 2, 3, ……..(p – 1) taken r at a time.

Since $x^{p-1} \equiv 1 \pmod{p}$.

$- a_1x^{p-2} + a_2x^{p-3} - \ldots\ldots\ldots\ldots + \{(p-1)! + 1\} \equiv 0 \pmod{p}$

Since this is an identity, coefficients of various powers of x are congruent 0 (mod p).

$\therefore a_r \equiv 0 \pmod{p}$ for $1 \leq r < p - 1$

Theorem 2.18 Wilson's Theorem

An integer p is a prime number if and only if $(p-1)! + 1 \equiv 0 \pmod{p}$.

Proof:- Suppose that p is a prime number.

Then we have the identity

$- a_1x^{p-2} + a_2x^{p-3} - \ldots\ldots\ldots\ldots + \{(p-1)! + 1\} \equiv 0 \pmod{p}$

(Refer to the identity A in theorem 5.15)

Putting $x = 0$, we get $(p-1)! + 1 \equiv 0 \pmod{p}$.

II. Suppose that $(p - 1)! + 1 \equiv 0 \pmod{p}$.

Then $p / (p - 1)! + 1$. If p is a composite number, it has a factor d, $1 < d < p$. d divides both p! and $(p - 1)! + 1$. Since $d \neq 1$ this is impossible.

$\therefore$ p is not a composite number. Besides $p \neq 1$. Hence p is a prime number.

This theorem stated by John Wilson (1741 – 93), was proved first by Lagrange (1736 – 1813)

2.9 Summary

We conclude with summarizing what we have covered in this unit.

(1) We have defined Congruence, linear Congruence and algorithm with examples.

(2) We have discussed Arithmetic of Congruence's.

(3) We have defined Residue Classes with examples and discussed its Wilson theorem.

(4) Statement and Proved in Chinese Remainder Theorem

2.10 Terminal Questions

I. Verify the following:

(a) $5^6 = 1 \pmod 7$

$(7, 5) = 1$ and $\emptyset(7) = 6$ ∴ By Euler's theorem $5^6 \equiv 1 \pmod 7$

$5^2 = 25 = 4 \pmod 7$

$5^6 = (4)^3 \equiv 1 \pmod 7$

(b) $3\emptyset(8) \equiv 1 \pmod 8$. (c) $7^{22} \equiv 1 \pmod{23}$. (d) $2^{46} \equiv \pmod{47}$

2. Find the remainders obtained on division of the following:

(a) 2^{23} by 47 (b) 3^{50} by 101 (c) 2^{460} by 47

(d) 2^{1000} by 17 (e) 2^{1000} by 13 (f) 159^{7654} by 23

(b) $3^4 = 81 \equiv -20 \pmod{101}$

$3^8 \equiv 20^2 \equiv -4 \pmod{101}$

$3^{48} \equiv (-4)^6 \equiv 4^6 \pmod{101}$

Now $4^4 = 256 \equiv 54 \pmod{101}$ ∴ $4^6 \equiv 54 \times 16 \equiv 108 \times 8 \equiv 7.8 \pmod{101}$

∴ $3^{50} \equiv 3^{48} \times 3^2 \equiv 56 \times 9 \equiv 8^{100} \pmod{802}$.

∴ The remainder that is obtained on dividing 350 by 102 is 100.

(f) $7654 = 247 \times 22 + 20$

$(159, 23) = 1$ ∴ By Euler's theorem, $159^{22} \equiv 1 \pmod{23}$.

∴ $(159^{22})^{247} \equiv 1^{247} \equiv 1 \pmod{23}$

$159 \equiv -2 \pmod{23}$

$(159)^{20} \equiv (-2)^{20} \equiv (2^5)^4 \equiv 9^4 \equiv (81)^2 \equiv 12^2 \equiv 6 \pmod{23}$

∴ $159^{7654} = (159^{22})^{247} \times (159^{22}) \equiv 1 \times 6 \equiv 6 \pmod{23}$

∴ The remainder is 6.

3. If p is an odd prime and (a, p) = 1, prove that

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

   $[ap - 1 - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right). \textit{use Euler's Theorem}\ ]$

4. Use Fermat's theorem to show that every prime except 2 and 5 divides infinitely many integers of the form 9, 99, 999, …….

5. If p is a prime, show that $[1^{p-1} + 2^{p-1} + \ldots\ldots\ldots\ldots\ldots + (p-1)^{p-1} + 1$ is a multiple of p.

6. If a and b are prime to n-show that $n \mid a^{n-1} - b^{n-1}$.

7. If a and b are prime numbers show that $a^{b-1} + b^{a-1} - 1 \equiv 0 \pmod{ab}$

   $A^{b-1} \equiv 1 \pmod{b}$ and $b^{a-1} \equiv 1 \pmod{a}$

   $a^{b-1} = 1 + kb$ and $b^{a-1} = 1 + k'a$. where $k, k' \in 1$.

   $a^{b-1} + b^{a-1} = 2 + kb + k'a$, $a^{b-1}b^{a-1} = 1 + kb + k'a + kk'ab$.

   $\therefore a^{b-1} + b^{a-1} + ab(1 - kk' + a^{b-2}b^{a-2})$

   $\therefore a^{b-1} + b^{a-1} \equiv 1 \pmod{ab}$

8. Prove that $n^5 - n$ is divisible by 30 where n is any integer.

   $30 = 5.3.2$ and 5, 3, 2 are prime

   For any integer n, $n5 \equiv n \pmod{5}$ $\quad \therefore 5 \mid n^5 - n$.

   Similarly $3 \mid n^3 - n$ and $2 \mid n^2 - n$

   $n^5 - n = n(n - 1)(n + 1)(n^2 + 1)$. Thus $n^3 - n$, $n^2 - n$ are the divisors

   of $n^5 - n$

   $\therefore$ 2 and 3 divide $n5 - n$. $\therefore 30 \mid n^5 - n$.

9. Prove that if n is an integer prime to 2, 3, 7 then $42 \mid n^6 - 1$.

10. Prove that if n is a prime > 7, then $504 \mid n^6 - n$.

11. Show that the 4^{th} power of any integer is of the form 5m or 5m + 1.

    For any integer a, 5 being a prime $a^5 \equiv a \pmod{5}$.

$\therefore 5 \mid a(a^4 - 1)$. $5 \mid a$ or $5 \mid a^4 - 1$.

If $5 \mid a$, a is a multiple of 5 and so also a^4.

If $5 \mid a^4 - 1$, $5 \mid a^2 - 1$ or $5 \mid a^2 + 1$.

$a^2 = 5k + 1$ or $5k - 1$. $\therefore a^4 = 5(5k^2 \pm 2k) + 1$.

Thus a^4 is of the form $5m + 1$ or $5m$.

12. Show that the 6^{th} and 12^{th} powers of any integer are of the forms $7m$ or $7m + 1$ and $13m$ or $13m + 1$ respectively

13. Show that 9^{th} power of any integer is of the form $19m$ or $19m \pm 1$. [$a^{19} \equiv a \pmod{19}$, / $19a(a^{9-1})(a^{9+1})$]

14. Prove that the 8^{th} power of any integer is of the form $17m$ or $17m \pm 1$.

15. Show that 5^{th} power of any integer n has the same right hand digit as n.

[Show that $10 \mid n^5 - n$. Then $n^5 - n = 10k$ ($k \in Z$). If a_0 is the right hand digit in n then $n = 10m + a_0$ where $m \in Z$. $n^5 = 10(k + m) + a_0$]

16. Prove that $712! + 1$ is divisible by 719.

719 being a prime number, by Wilson's Theorem

$718! + 1 = 0 \pmod{719}$.

$\therefore 718.717, 716, 715, 714, 713\ (712)! + 1$

$\equiv (-6)(-5)(-4)(-3)(-2)(-1)(712)! + 1$

$\equiv 720(712)! + 1 \equiv (712)! + 1 \ \ 0 \pmod{719}$

17. If p is a prime number, show that $2(p - 3)! + 1$ is divisible by p

[Prove $(p - 1)! - 2 \times (p - 3)!$ Is a multiple of p and use Wilson's theorem]

18. Prove that $(28)! - 666$ is divisible by 899.

Now we have $899 = 29.31$

$666 \equiv -1 \pmod{29}$ and $28! \equiv -1 \pmod{29}$.

$\therefore 28! \equiv 666 \pmod{29}$ i.e. $29 \mid (28! - 666)$

$666 \equiv 15 \pmod{31}$ and $30! \equiv -1 \pmod{31}$

$\therefore 30.29\ (28)! + 1 \equiv (-1)(-2)28! + 1 \equiv 2 \times 28! - 30 \pmod{31}$.

Since $(2, 31). \ 1, 28! - 15 \equiv 0 \pmod{31}$.

$\therefore 28! - 666 \equiv 0 \pmod{31}, 31 \mid 28! - 666$.

$\therefore 899 = 31 \times 29 \mid 28! - 666$

19. Prove that (a) $18! + 1 \equiv 0 \pmod{437}$ (b) $28! + 233 \equiv 0 \pmod{899}$.

20. If p is a prime of the form $4n + 1$ obtain the solution of $x^2 \equiv -1 \pmod{p}$

[Apply Wilson's theorem: use $r \equiv -(p - r) \pmod{p}$ to pair the factors $(p - 1)!$]

21. Find all the solutions of $x^{12} \equiv 1 \pmod{13}$.

22. If $(a, b) = 1$ and $m \neq 0$ show that there exists an integer x such that $(ax + b, m) = 1$.

23. Show that every square is congruent to 0 or 1 (mod 8).

24. If a is odd, show that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$. [use Induction]

UNIT-3 Euler's Function & Application

Structure

3.1 Introduction:

This is unit in number theory of Leonhard Euler introduced the function in 1763. It is written using the Greek letter phi as ∅(n). It is number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor gcd(n, k) is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

In 1879, J.J.Sylester coined the term totient for this function, so it is also referred to as Euler's totient function, the Euler totient or Euler's totient. Jordan's totient is a generalization of Euler's. The cototient of n is defined as $n - \emptyset(n)$. It counts the number of positive integers less than or equal to n that have at least one prime factor in common with n.

3.2 Objectives.

After reading this unit the learner should be able to understand about:

- Euler's Function

- Application of Euler's Function
- Properties of the Phi function
- Statement and Prove Gauss Theorem
- Multiplicative Function
- Properties of the Multiplicative Function

3.3 Totient Function or Euler's Function (∅ - Function)

Definition:

Euler's function ∅(n) for all positive integers n is defined by ∅(n) = 1 for n = 1 and for n > 1, ∅(n) = number of positive integers less than n and co-prime to n.

∅(n), where n = 1 than ∅(1)= 1

There is three standard method:

1. **If n is prime:** Let n is a prime number, then $\emptyset(n) = n - 1$.

Example:1 ∅(2) means number of positive integers <2, that are co-prime to 2.

$$\emptyset(2) = 1$$

Example:2 $\emptyset(3)$ means number of positive integers < 3, that are co-prime to 3. Clearly, 1 and 2 are co-prime to 3.

$$\emptyset(3) = 2$$

Example:3 $\emptyset(8)$ means number of positive integers < 8, that are co-prime to 8. Clearly, 1, 3, 5, 7 are co-prime to 8

$$\emptyset(8) = 4$$

Similarly we have $\emptyset(4) = 2$, $\emptyset(6) = 2$ and $\emptyset(7) = 6$ etc.

2. If n is product of distinct prime numbers: Let $n = p \times q \times r$,

$$then\ \emptyset(n) = \emptyset(\ p \times q \times r)$$

$$\emptyset(n) = \emptyset(\ p) \times \emptyset(q) \times \emptyset(r)$$

$$\emptyset(n) = (\ p - 1) \times (q - 1) \times (r - 1)$$

Example:4 Find the value $\emptyset(10)$.

Solution: Let $n = 10$,then $\emptyset(10) = \emptyset(2 \times 5)$

$$= \emptyset(2) \times \emptyset(5)$$

Since $\emptyset(10) = (2-1) \times (5-1) = 4$

$$\emptyset(10) = 4$$

Example:5 Find the value $\emptyset(15)$.

Solution: Let $n = 15$,then $\emptyset(15) = \emptyset(3 \times 5)$

$$= \emptyset(3) \times \emptyset(5)$$

Since $\emptyset(15) = (3-1) \times (5-1) = 2 \times 4$

$$\emptyset(15) = 8$$

Example:6 Find the value $\emptyset(42)$.

Solution: Let $n = 42$,then $\emptyset(42) = \emptyset(2 \times 3 \times 7)$

$$= \emptyset(2) \times \emptyset(3) \times \emptyset(7)$$

Since $\emptyset(42) = (2-1) \times (3-1)(7-1)$

$$\emptyset(42) = 1 \times 2 \times 6$$

$$\emptyset(42) = 12$$

3. If n is a number of prime-power: Let $n = p^k, then$

$$\emptyset(n) = \emptyset(p^k) = p^k - p^{k-1}$$

Example:7 Find the value $\emptyset(8)$.

Solution: Let $n = 8$,then $\emptyset(8) = \emptyset(2^3)$

$$= (2^3) - (2^{2-1})$$

Since $\emptyset(8) = (8 - 4)$

$$\emptyset(8) = 4$$

Example:8 Find the value $\emptyset(49)$.

Solution: Let $n = 49$,then $\emptyset(49) = \emptyset(7^2)$

$$= (7^2) - (7^{2-1})$$

Since $\emptyset(49) = (49 - 7)$

$$\emptyset(49) = 42$$

3.4 Applications of Euler phi Function $\emptyset(n)$:

1.Number of Generators in Cyclic group of order n are $\emptyset(n)$.

Example :1 Let G be a cyclic group of order 18. find the generators.

Solution: We know that Z_{18},The number of generators in G are $\emptyset(18)$.

$$\emptyset(18) = \emptyset(2 \times 3^2)$$

$$\emptyset(18) = \emptyset(2) \times \emptyset(3^2)$$

$$= (2^1 - 2^0) \times (3^2 - 3^1)$$

$$= (2 - 1) \times (9 - 3) = 1 \times 6 = 6$$

$$\emptyset(18) = 6$$

2.Number of Elements of order d in Cyclic group are $\emptyset(d)$.

Example :1 Let G be a cyclic group of order 100, then number of elements of order 20 are

Solution: We have Z_{100},Then $\emptyset(20) = \emptyset(2^2 \times 5)$

$$= \emptyset(2^2)\emptyset(5)$$

$$= (2^2 - 2^1)\emptyset(5^1 - 5^0)$$

$$= (4-2)(5-1) = 2 \times 4 = 8$$

3.Order of Group of units i.e., order of $\boldsymbol{U(n)}$ $\boldsymbol{are}$ $\boldsymbol{\emptyset(n)}$.

Example: Order of Group $\boldsymbol{U(100)}$ is

Solution: We have $\emptyset(\mathbf{100}) = \emptyset(\mathbf{2^2 \times 5^2})$

$$= \emptyset(2^2)\emptyset(5^2)$$

$$= (2^2 - 2^1)(5^2 - 5^1)$$

$$= (4-2)(25-5) = 2 \times 20 = 40$$

$$\emptyset(\mathbf{100}) = \mathbf{40}$$

4. Number of Cyclic subgroups of order $\boldsymbol{d}$ in any

group$= \frac{\boldsymbol{number\ of\ elements\ of\ order\ d}}{\emptyset(\boldsymbol{d})}$

Example: Number of cyclic subgroups of order 2 in Klien's 4 group

Solution: We have number of elements of order $d = 2$

group$= \frac{\boldsymbol{number\ of\ elements\ of\ order\ 2}}{\emptyset(\mathbf{2})}$

$$= \frac{3}{\emptyset(2)} = \frac{3}{2^1 - 2^0}$$

$$= \frac{3}{2-1} = 3$$

3.5 Multiplicative Function:

A function f(x) defined on the set of positive integers is said to be a multiplicative function if f(ab) = f(a).f(b) for all co-prime positive integers a and b.

Example:1- Let $f(x) = x^3$ (a, b) = 1

$f(ab) = (ab)^3 = a^3b^3 = f(a).f(b)$

Some theorems on ∅-function:-

Theorem 1: If p is a prime and k be any positive integer, then

$$\emptyset(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1-1/p)$$

Proof:- Let S = {1, 2, 3, ……. p^k}

The set S has pk elements. The numbers which are divisible by p in set S are p, 2p, 3p, …….p^{k-1}.p. Then are p^{k-1} in all and these numbers are not relatively prime to p^k.

Now, ∅(pk) = number of integers in S which are relatively prime to p^k.

$$P^k - p^{k-1} = p^k(1-1/p)$$

Example:- ∅(9) p = 3, k = 2

$\emptyset(9) = \emptyset(3^2)$

$\emptyset(9) = p^k(1-1/p)$

$= 3^2(1-1/3)$

$= 9(2/3)$

∅(9) = 6

Note: $\emptyset(3^2) = 3^2 - 3 = 9 - 3 = 6$

Here 1, 2, 4, 5, 7, 8 are co-prime to 3^2. Where 3, 6, 9 (three in number) are not co-prime to 3^2.

Theorem:2- Euler's function $\emptyset$ is a multiplicative function or if m and n are relatively prime, then $\emptyset(mn) = \emptyset(m).\emptyset(n)$

Proof:- *for m = 1 or n = 1, the result in obviously true, as* $\emptyset(1) = 1$

$\because \emptyset(mn) = \emptyset(m)\emptyset(n)$

Let $m = 1$ then $\emptyset(n) = \emptyset(1)\emptyset(n)$ $\qquad \because \emptyset(1) = 1$

$\therefore \emptyset(n) = \emptyset(n)$

Again let n = 1

$\emptyset(m) = \emptyset(m).\emptyset(1)$

$\emptyset(m) = \emptyset(m)$

For $m > 1$ and $n > 1$

Let us arrange the integers 1, 2, ………………. Mn in m columns and n rows as follows

$1 \quad 2 \quad \ldots\ldots\ldots\ldots \quad r \quad \ldots\ldots\ldots\ldots \quad m$

$m + 1 \quad m + 2 \ldots\ldots\ldots \quad m + r \quad \ldots\ldots\ldots\ldots \quad 2m$

…… …… …… ……

(n-1)m + 1 (n-1)(m+2) (n-1)(m+r) …… mn

Here ∅(mn) = number of entries that are relatively prime to mn.

= number of integers that are relatively prime to both m and n

∵ *g.c.d.(a, b, c) = 1 if g.c.d.(a, b) = 1 and g.c.d(a, c) = 1*

Consider the entries in the rth column

r, m+r, …….. (n-1)m+r …….. (i)

The entries of (i) form an A.P. of n terms with common difference m relatively prime to n. Also, each term of (i) is relatively prime to m if (r, m) =1

But (r, m) = 1 for ∅(m) values of r.

Thus, there are exactly ∅(m) columns in which every integer is relatively prime to m. Now, each column in the above array contains exactly ∅(n) integers relatively prime to n.

∴ There are in all ∅(m)∅*(n) integers less than mn and relatively prime to both m and n.*

Hence $\emptyset(mn) = \emptyset(m)\,\emptyset(n)$

Cor. If $n_1, n_2, n_3, \ldots\ldots nr$ *are pairwise relatively prime, then* $\emptyset(n_1, n_2, n_3, \ldots n_r) = \emptyset(n_1).\emptyset(n_2)\ldots\ldots\ldots \emptyset(n_r)$

Theorem:3- For any positive integer n > 1, $\emptyset(n) = n\left(1 - \frac{1}{p}\right)$ **or**

If the integer n > 1 has the prime factorization n = $p_1^{k_1}.p_2^{k_2} \ldots\ldots\ldots\ldots.. p_r^{k_r}$

Then $\emptyset(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \ldots\ldots\ldots\ldots.. \left(p_r^{k_r} - p_r^{k_r-1}\right)$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots\ldots\ldots\ldots.. \left(1 - \frac{1}{p_r}\right)$$

Proof:- Let n = $p_1^{k_1}.p_2^{k_2} \ldots\ldots\ldots\ldots.. p_r^{k_r}$ be the standard form of n

Now, since $p_1^{k_1}.p_2^{k_2} \ldots\ldots\ldots\ldots.. p_r^{k_r}$ = 1

i.e. all pi's are distinct primes.

$\therefore \emptyset(n) = \emptyset\left(p_1^{k_1}.p_2^{k_2}.p_3^{k_3} \ldots\ldots\ldots\ldots.. p_r^{k_r}\right)$

$= \emptyset\left(p_1^{k_1}\right).\emptyset\left(p_2^{k_2}.p_3^{k_3} \ldots\ldots\ldots\ldots.. p_r^{k_r}\right)$

$\because \emptyset(mn) = \emptyset(m)\,.\emptyset(n)$ for (m, n) = 1

$= \emptyset\left(p_1^{k_1}\right).\emptyset\left(p_2^{k_2}\right).\emptyset\left(p_3^{k_3} \ldots\ldots\ldots\ldots..p_r^{k_r}\right)$

$\because p_1^{k_1}.p_2^{k_2}.p_3^{k_3} \ldots\ldots\ldots\ldots..p_r^{k_r} = 1$

Proceeding like this, we get

$\emptyset(n) = \emptyset\left(p_1^{k_1}\right).\emptyset\left(p_2^{k_2}\right) \ldots\ldots\ldots\ldots\emptyset\left(p_r^{k_r}\right)$

$= p_1^{k_1}\left(1-\frac{1}{p_1}\right).p_2^{k_2}\left(1-\frac{1}{p_2}\right) \ldots\ldots\ldots\ldots\ldots p_r^{k_r}\left(1-\frac{1}{p_r}\right)$

Using theorem 1

$$\Longrightarrow p_1^{k_1}.p_2^{k_2}.p_3^{k_3} \ldots\ldots\ldots\ldots..p_r^{k_r}\left(1-\frac{1}{p_1}\right).\left(1-\frac{1}{p_2}\right)\ldots..\left(1-\frac{1}{p_r}\right)$$

$= n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$

Or $\emptyset(n) = n\prod_{p/n}\left(1-\frac{1}{p}\right)$

Example:1- Evaluate $\emptyset(600)$

Solution: $\because$ n = 600

$n = 2^3.3^1.5^2$

$k_1 = 3, k_2 = 1, k_3 = 2$

$p_1 = 2, p_2 = 3, p_3 = 5$

$\because \emptyset(n) = \emptyset(2^3.3^1.5^2)$

$\because \emptyset(p^k) = p^k\left(1 - \frac{1}{p}\right)$

$$\Longrightarrow 2^3\left(1 - \frac{1}{2}\right).3^1\left(1 - \frac{1}{3}\right).5^2\left(1 - \frac{1}{5}\right)$$

$$\Longrightarrow 2^3.3^1.5^2\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$= 600 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$

$\emptyset(600) = 160$ Ans.

Example:2 Find the value $\emptyset(200)$.

Solution: Since $200 = 2 \times 3 \times 5 \times 7$

$\therefore \boldsymbol{\emptyset(200)} = 2 \times 3 \times 5 \times 7 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3}) \times (1 - \frac{1}{5}) \times (1 - \frac{1}{7})$

$$\emptyset(200) = 210 \times \left(\frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7}\right)$$

$$\boldsymbol{\emptyset(200) = 48}$$

Example:3 Find the value ∅(100).

Solution: Since $100 = 2^2 \times 5^2$

$\therefore$ **∅(100)** = $2^2 \times 5^2 \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$

$$\emptyset(100) = 100 \times \left(\frac{1}{2} \times \frac{4}{5}\right)$$

$$\emptyset(\mathbf{100}) = \mathbf{40}$$

Theorem 4:- For n > 2, ∅(n) is an even integer

Proof:- Case I – Let n = 2k, k > 1

i.e. n is power of 2 only

Then ∅(n) = ∅(2^k) = $2^k\left(1 - \frac{1}{2}\right)$

= $2^k . \frac{1}{2} = 2^{k-1}$

Since k > 1. Therefore 2^{k-1} is even.

∅(n) = 2^{k-1} an even integer

Thus ∅(n) is even if n > 2.

Case II:- When n is not a power of 2, then n is divisible by an odd prime p (say)

Let $n = p^k m$, where $k \geq$ and $(p^k, m) = 1$

$$\therefore \emptyset(n) = \emptyset(p^k m) = \emptyset(p^k)\emptyset(m)$$

$$\because \emptyset \text{ is a multiplicative function}$$

$$Or\, \emptyset(n) = p^k \left(1 - \frac{1}{p}\right) \emptyset(m) = even$$

$Hence\, \emptyset(n)$ *is even when* $n > 2$.

Theorem 5:- Let m and n be positive integers. If every prime divisor of n is a prime divisor of m, then

$$\emptyset(\boldsymbol{m\, n}) = \boldsymbol{n}\emptyset(\boldsymbol{m})$$

Also, in particular, $\emptyset(m^2) = m\emptyset(m)$

Proof: Let us assume that

$$n = p_1^{a_1} p_2^{a_2} \ldots\ldots\ldots\ldots\ldots\ldots . p_r^{a_r}$$

And m= $p_1^{b_1} p_2^{b_2} \ldots\ldots\ldots\ldots\ldots\ldots . p_r^{b_r} . q_1^{c_1} q_2^{c_2} \ldots\ldots\ldots\ldots\ldots\ldots . q_r^{c_r}$

Where p_i's q_i's are all distinct primes and

$a_i \geq 1$, $b_i \geq 1$, $c_i \geq 1$ for all i.

Therefore

$$\emptyset(m\,n) = p_1^{a_1+b_1} p_2^{a_2+b_2} \dots\dots\dots\dots\dots\dots p_r^{a_r+b_r} . q_1^{c_1} q_2^{c_2} \dots\dots\dots\dots\dots\dots q_r^{c_r}$$

$$= mn\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\dots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\dots\dots\left(1-\frac{1}{q_r}\right)$$

$$= n\left\{m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\dots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\dots\dots\left(1-\frac{1}{q_r}\right)\right\}$$

= n. ∅(m) …… (1)

Put n = m is equation .(1)

We get $\emptyset(m^2)$= m$\emptyset(m)$

Example:1- Find $\emptyset(n)$ for n = 68

Solution:- We have n = 68 = 2^2.17 = $p_1^{k_1} . p_2^{k_2}$

Here $p_1 = 2$, $p_2 = 17$, $k_1 = 2$, $k_2 = 1$

Using $\emptyset(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\dots\left(1-\frac{1}{p_r}\right)$ we have

$$\emptyset(68) = 68\left(1-\frac{1}{2}\right)\left(1-\frac{1}{17}\right)$$

$$= 68\left(\frac{1}{2}\right)\left(\frac{16}{17}\right) = 32$$

$$\therefore \emptyset(68) = 32$$

Example:2-$\emptyset(\mathbf{462})$

Solution:- we have n = 462 = $2^1.2^1.7^1.11^1 = p_1^{k_1}.p_2^{k_2}p_3^{k_3}.p_4^{k_4}$

Here $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, $p_4 = 11$

$k_1 = k_2 = k_3 = k_4 = 1$

Example:3- Show that $\emptyset(15^k) = \emptyset(15)$ x 15^{k-1}, where k is a positive integer

Solution:- We have $\emptyset(15) = \emptyset(3.5)$

$\Rightarrow$ $\emptyset(3).\emptyset(5)$

$\Rightarrow$ $(3 - 3^0)(5 - 5^0)$ $\because \emptyset(p) = p - 1$ where p is prime

$\because$ $\emptyset(p^k) = p^k - p^{k-1}$ for any prime p. where k is a positive integer

$\Rightarrow$ $(3 - 1)(5 - 1)$

$= 2.4 = 8$

$\therefore$ $\emptyset(15) = 8$ …… (1)

Now $\emptyset(15k) = \emptyset(3k.5k) = \emptyset(3k).\emptyset(5k)$

$= (3^k - 3^{k-1})(5^k - 5^{k-1})$

$= 3^{k-1}(3 - 1).5^{k-1}(5 - 1)$

$= 3^{k-1}(2).5^{k-1}(4)$

$= 8.(3x5)^{k-1}$

$= 8.15^{k-1}$ using (1) we get

$\emptyset(15^k) = \emptyset(15)$ x 15^{k-1}

Example:4- Show that $2^4 \mid \emptyset(1155)$

Solution:- we have $1155 = 3.5.7.11$

$$\emptyset(1155) = \emptyset(3.5.7.11) = \emptyset(3).\emptyset(5).\emptyset(7).\emptyset(11)$$

We know that $\emptyset(n)$ is even if n > 2

$\therefore$ $\emptyset(3), \emptyset(5), \emptyset(7), \emptyset(11)$ all are even.

$\Rightarrow$ $2 \mid \emptyset(3).2 \mid \emptyset(5).2 \mid \emptyset(7).\ 2 \mid \emptyset(11)$

$\Rightarrow$ $2^4 \mid \emptyset(3), \emptyset(5), \emptyset(7), \emptyset(11)$

$\Rightarrow \quad 24 \mid \emptyset(1155)$

Example:5- Show that $\emptyset(n) = \emptyset(n-1) = \emptyset(n+2)$ for n = 5186.

Solution:- We have n = 5156 = 2.2593

$$\emptyset(n) = \emptyset(5186)$$

Using $\emptyset(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\left(1-\frac{1}{p_r}\right)$ we have

$$\emptyset(5186) = 5186\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2593}\right)$$

$$= 5186\left(\frac{1}{2}\right)\left(\frac{2592}{2593}\right) = 2592 \quad \ldots\ldots\ldots\ldots\ldots\ldots \ (1)$$

Now n + 1 = 5187 = 3.7.13.19

$\therefore \quad \emptyset(n+1) = \emptyset(5187)$

$$= 5187\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{19}\right)$$

$$= 5187\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\left(\frac{12}{13}\right)\left(\frac{18}{19}\right) = 2592 \quad \ldots\ldots\ldots\ldots\ldots\ldots \ (2)$$

Now $\emptyset(n+1) = \emptyset(5188)$

$$= 5188\left(1-\frac{1}{2}\right)\left(1-\frac{1}{1297}\right)$$

$= 5188\left(\frac{1}{2}\right)\left(\frac{1296}{1297}\right) = 2592$ …… (3)

From (1), (2), (3) we have

$\emptyset(n) = \emptyset(n+1) = \emptyset(n+2)$ for n = 5186

We have $\emptyset(n) = \emptyset(5186)$

$= \emptyset(2.2593)$

$= \emptyset(2).\emptyset(2593)$ ($\because\emptyset$ is multiplicative)

= (21 – 20).(25931 = 25930)

$\therefore$ $\emptyset(p^k) = p^k - p^{k-1}$ for any prime p. where k is a positive integer.

= (2 – 1).(2593 – 1) = 2592 ……(1)

$\emptyset(n+1)$ = $\emptyset$(5187)

= $\emptyset$(3.7.13.19)

= $\emptyset$(3).$\emptyset$(7).$\emptyset$ (13).$\emptyset$(19)

$= (3-1)(7-1)(13-1)(19-1) = 2.6.12.18$

$= 2592$ …… (2)

$\emptyset(n+2) = \emptyset(5188)$

$= \emptyset(2^2.1297)$

$= \emptyset(2^2).\emptyset(1297)$

$= (2^2 - 2).(1297 - 1)$

$= 2.1296$

$= 2592$ ..... (3)

From (1), (2) and (3)

$\emptyset(n) = \emptyset(n+1) = \emptyset(n+2)$ for n = 5186

Example:6- Prove that $\emptyset(n) = \emptyset(n+2)$ is satisfied by n = 2(2p –1) whenever p and 2p – 1 are both odd prime.

Solution:- Let p and 2p – 1 be odd primes. Then $\emptyset(n) = \emptyset[2.(2p-1)]$

$= \emptyset(2).\emptyset(2p-1)$ ∵ $\emptyset$ is multiplicative as (2, 2p - 1) = 1

= (2 – 1).(2p – 1 – 1) ∵ for any prime p, $\emptyset$(p) = 1

= 2(p – 1) ……. (1)

Also $\emptyset(n+2) = \emptyset[2(2p-1)+2]$

$= \emptyset(4p) = \emptyset(2^2.p)$

$= \emptyset(2^2).\emptyset(p)$ $[\because (2^2, p) = 1$, so $\emptyset$ is multiplication]

$= (2^2 - 2).(p-1)$ $\because \emptyset(pk) = p^k - p^{k-1}$ for any prime p

Where k is a prime

$= 2(p-1)$ ..... (2)

The from (1) and (2), we have $\emptyset(n) = \emptyset(n+2)$

Example:7- Prove that $\emptyset(n) = \frac{n}{2}$ if $n = 2^k$ for some integer $k \geq 1$

Solution:- Let $\emptyset(n) = \frac{n}{2}$

Since $\emptyset(n)$ is an integer for all positive integers n, therefore $\frac{n}{2}$ is an integer.

$\Rightarrow$ n is an even integer $[\because \emptyset(n) = \frac{n}{2}]$

Let $n = 2^k.m$, where $k \geq 1$ and m is odd

Now, $\emptyset(n) = \frac{n}{2}$

$\Rightarrow \quad \emptyset(2^k.m) = \frac{2^k.m}{2}$

$\Rightarrow \quad \emptyset(2k).\emptyset(m) = 2^{k-1}.m$

$\Rightarrow \quad (2^k - 2^{k-1}).\emptyset(m) = 2^{k-1}.m$

$\Rightarrow \quad 2^{k-1}(2 - 1)\emptyset(m) = 2^{k-1}.m$

$\Rightarrow \quad \emptyset(m) = m \qquad$ if $m = 1$

$\emptyset(1) = 1 \qquad n = 2^k.m = 2^k$

(2) $n = 2k, \quad k \geq 1$

$\emptyset(n) = \frac{n}{2}$

$\emptyset(n) = \emptyset(2^k) = 2^k - 2^{k-1}$

$= 2^{k-1}(2 - 1) = 2^{k-1} = \frac{2^k}{2} = \frac{n}{2}$ hence prove

3.6 Properties of the Phi function:-

1. If p is prime then prove that $\emptyset(p^k) = p^k - p^{k-1}$
2. If a and b are co-prime to each other, prove that $\emptyset(a, b) = \emptyset(a),\emptyset(b)$

3. Prove that $\emptyset(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots\left(1 - \frac{1}{p_r}\right)$
4. Prove that $\emptyset(m^2) = m\,\emptyset(m)$, for every positive m.
5. If m > 1. Prove that the sum of positive integers $\emptyset(m)$. Which are less than m and relatively prime to m is $m[\emptyset(m)/2]$
6. If p is prime then $\emptyset(p) = p - 1$

Theorem-6: Gauss Theorem:-

For each +ve integer n.$\sum_{d/n} \emptyset(d) = n$

Where sum is carried over all +ve divisors of n.

Proof:- Let d to be +ve divisor of n and $s_d = \{l/\gcd(l, n); 1 \leq l \leq n\}$

We know that gcd.(l, n) = d if gcd (l/d, n/d) = 1

Thus the number of integers in the set s_d is equal to number of +ve integers less than n/d which are co-prime to n/d i.e. equal to $\emptyset\left(\frac{n}{d}\right)$. {by def. $\emptyset(n)$}

As each integer in the set

T = {1, 2, 3, ……..n} lies in exactly one class sd

$\therefore n = \sum_{d/n} \emptyset(\frac{n}{d}) = n = \sum_{e/n} \emptyset(e)$

($\because$ n/d = e $\Rightarrow$ n= de $\Rightarrow$ e/n)

$= \sum_{d/n} \emptyset(d)$ hence $\sum_{d/n} \emptyset(d) = n$

Example:1- for n = 10 the +ve divisor are 1, 2, 5, 10

$\therefore S_1 = \{l/gcd(l, 10) = 1; 1 \leq l \leq 10\}$

$= \{1, 3, 7, 9\}$

$S_2 = \{l/gcd(l, 10) = 2; 1 \leq l \leq 10\} = \{2, 4, 6, 8\}$

$S_5 = \{l/gcd(l, 10) = 5; 1 \leq l \leq 10\} = \{5\}$

$S_{10} = \{l/gcd(l, 10) = 10; 1 \leq l \leq 10\} = \{10\}$

Here S1 contains 4 elts i.e. $\emptyset(10)$ elts$\emptyset(1) = 4$, $\emptyset(5) = 4$, $\emptyset(2) = 1$, $\emptyset(10) = 1$

$\therefore \sum_{d/10} \emptyset(d) = \emptyset(10) + \emptyset(5) + \emptyset(2) + \emptyset(1)$

$\Rightarrow$ 4 + 4 + 1 + 1 = 10 = n

Cor:- for any positive integer n

$$\sum_{d/n} \emptyset\left(\frac{n}{d}\right) = n$$

Proof:- we have $\therefore \sum_{d/n} \emptyset(d) = n$

As d/n

$\therefore$ n = de, e $\in$ z

$\frac{n}{d} = e$ and e/n

Thus n = $\sum_{d/n} \emptyset(d) = \sum_{e/n} \emptyset(e)$

= $\sum_{d/n} \emptyset\left(\frac{n}{d}\right) = n$

3.7 Summary :

We conclude with summarizing what we have covered in this unit.

Euler's Function we shall introduce the concept of complete Residue System (mod m) and Residue system (mod m) which have important application in the field of number theory.

1 We have defined the Euler's Function with Example.

2 We have discussed the Euler's Function Properties and Proved.

3 We have defined the Multiplication Function and Properties of Euler's Function with Example.

Terminal Questions:

1. Find the value of $\emptyset(m) if\ m = 63$.
2. Find the value of $\emptyset(m) if\ m = 500$.
3. Let G be a cyclic Group of order 50, find the number of elements of order 10.
4. For odd integer 'n' prove that $\emptyset(2n) = \emptyset(n)$
5. Evaluate $\emptyset(m)$ for $m = 1,2,3 \ldots . 12$.
6. If $\emptyset(m) = \emptyset(mn)$ and $n > 1$, prove that $n = 2$ and m is odd.
7. Find the value $\emptyset(360)$.
8. Show that $\emptyset(15^k) = \emptyset(15) \times 15^{k-1}$,where k is positive integer.
9. Show that $\emptyset(n) = \emptyset(n+1) = \emptyset(n+2)\ for\ n = 5186$
10. .Show that $\emptyset(n) = \frac{n}{2} iff\ n = 2^k$ for some integer $k \geq 1$.

Uttar Pradesh

RajarshiTandon
Open University

Bachelor Of Science

DCEMM -110
Number Theory

Block

2 Gauss theorem & Applications

UNIT- 4
Quadratic residues of Number Theory

UNIT-5
Gauss theorem

UNIT-6
Arithmetic Functions and applications

Course Design Committee

Prof. Ashutosh Gupta, School of Computer and Information Science, UPRTOU, Prayagraj	**Chairman**
Prof. Sudhir Srivastav Dept. of Mathematics, DDU Gorakhpur University, Gorakhpur	**Member**
Prof. P. K. Singh Dept. of Mathematics, Allahabad Uiversity, Prayagraj	**Member**
Prof. Mona Khare Dept. of Mathematics, Allahabad Uiversity, Prayagraj	**Member**
Dr. A. K. Pandey Associate Professor, ECC Prayagraj	**Member**
Dr. Vikas Singh Academic Consultant, UPRTOU, Prayagraj	**Member**
Dr. S. S. Tripathi Academic Consultant, UPRTOU, Prayagraj	**Member**

Course Preparation Committee

Dr. P.N. Pathak Assistant Professor (Dept. of Mathematics), CSJM Kanpur university, Kanpur	**Author (Unit – 4 to 7)**
Dr. Raghvendra Singh Assistant Professor , (C.) School of Science, UPRTOU, Prayagraj	**Author (Unit – 1 - 3)**
Dr. S. S. Tripathi Ret. . Associatet Professor (Dept. of Mathematics), ECC, Prayagraj.	**Editor (Unit 1 - 6)**
Dr. Raghvendra Singh Assistant Professor , (C.) School of Science, UPRTOU, Prayagraj	**Coordinator**

DCEMM – 110 : Number Theory
ISBN-

Printed By: Chandrakala Universal Pvt. 42/7 Jawahar Lal Nehru Road, Prayagraj.

Block- 2: Gauss theorem & Applications

Introduction

Number theory is a branch of pure mathematics devoted to the study of the set of positive whole numbers which are usually called the set of natural numbers. This provides an introduction to the important basic topics of number theory: Euler's function, congruence, module and arithmetic functions, gauss lemma, quadratic residue and Euler's criterion. Originally an abstract mathematical concept from the branch of number theory known as modular arithmetic, quadratic residues are now used in applications ranging from acoustical engineering to cryptography and the factoring of large numbers.

Objectives:

- To understand the difference between the quadratic residues and non residues.
- To verify the given number is quadratic residue or non residue by using Euler's criterion.
- To understand the Legendre symbols and its basic properties.
- To understand the quadratic reciprocity law.
- To differentiate the Jacobi symbol with Legendre ones.
- To understand the definition of Arithmetic functions and multiplicative functions.
- To understand the mobius function and mobius inversion formula.
- Use of Gauss lemma and gauss reciprocity theorem.

Unit-4: Quadratic Residue of Number Theory

Structure

4.1 Introduction

This is unit of important in number theory**.** The prime numbers, their properties, and their relation to the composite numbers have fascinated mathematicians for thousands of years. Yet it was not until the 1700s that the first really deep result about prime numbers was discovered, by Leonhard Euler. The *Quadratic Reciprocity Theorem* was proved first by Gauss, in the early 1800s, and reproved many times thereafter (at least eight times by Gauss). We conclude our brief study of number theory with a beautiful proof due to the brilliant young mathematician Gotthard Eisenstein, who died tragically young, at 29, of tuberculosis. The proof is similar to one by Gauss, but it replaces a complicated lemma by an ingenious geometrical argument. This is a good place to leave number theory, as it hints at the wonderful but difficult and subtle areas of the subject; we hope it makes you want to explore number theory further. See the bibliography for some starting points. we discuss the structure of the groups Zn.

Suppose p is an odd prime and p does not divide b. Then b is a **quadratic residue** (mod p) if $b \equiv c^2 \pmod{p}$ for some c, and otherwise b is a **quadratic**

nonresidue. In other words, a quadratic residue is a "perfect square" in the world of modular arithmetic.

It is easy to see that $x^2 \equiv (p-x)^2 \equiv (-x)^2$ for any x, so at most half of the elements of $\{1,2,3,\ldots,p-1\}$ are quadratic residues modulo p. It is also not hard to see that $x^2 \equiv y^2$ implies that $y \equiv \pm x$, so in fact exactly half of the elements of $\{1,2,3,\ldots,p-1\}$ are quadratic residues.

4.2 Objectives

After reading this unit learner should be able to understand about:

- To understand the difference between the quadratic residues and non residues.
- To understand the definition of Group of units of

$$Zn = \{0, 1, 2, \ldots\ldots, n-1\}$$

- To verify the given number is quadratic residue or non residue by using Euler's criterion.
- To understand the Legendre symbols and its basic properties.
- To understand the quadratic reciprocity law.

- To differentiate the Jacobi symbol with Legendre ones.

4.3 Group of units of Zn

Let n∈ N. we write Un = $\{x \in N | \ 1 \leq x \leq n, (x,n) = 1\}$. So, U_n is set of all numbers from 1 to n that are relatively prime to n.

For example, U_8 = {1, 3, 5, 7}

U_{12} = {1, 5, 7, 11}, Up = (1, 2, 3, …… p-1).

Why are we interested in these numbers?

$Z_n|$ {0} is not a group with respect to multiplication.

As we know Z_n = {0, 1, 2, ……n-1} forms a group with respect to addition modulo n. But, in general Z_n^* = $Z_n|$ {0} does not form a group with respect to multiplication modulo n.

For example

Z_6 = {0, 1, 2, 3, 4, 5} is a group with respect to addition modulo 6, but Z_6^* = $Z_6|$ {0} = {1, 2, 3, 4, 5} is not a group with respect to multiplication modulo 6 as 2 * 3 = 6 ≡ 0 (mod 6). Also, the elements 2, 3 and 4 do not have multiplicative inverses modulo

6, or equivalently. Exe is congruent to 1 mod 6 does not have solution whenever a is equal to 2 or 3 or 4 so that is why you are looking for U_n.

$U_n = \{x \in N \mid 1 \leq x \leq n, (x, n) = 1\}$ a group with respect to

Next obvious equation is "$U_n = \{x \in N \mid 1 \leq x \leq n, (x, n) = 1\}$ a group with respect to multiplication modulo n." (Answer yes verify it)

The next question is "Is $U_n = \{x \in N \mid 1 \leq x \leq n, (x, n) = 1\}$ cycle group $\forall n \in N$?

Solution: No, for example U_8 is not cyclic. In general, U_n is cyclic whenever n = 2, 4, p^k, $2p^k$ $k \geq 1$. Where p is an odd prime.

For n = 2, 4, p^k, $2p^k$ $k \geq 1$. The generators of U_n are called primitive roots modulo n.

Example:1- for n = 5, $U_5 = \{1, 2, 3, 4\}$ and 2, 3 are primitive roots modulo 5.

Solution: As $U_5 = \{2^0, 2^1 \equiv 2 (\text{mod } 5), 2^2 \equiv 4 (\text{mod } 5), 2^3 \equiv 3 (\text{mod } 5).\}$ so we are getting all the elements in U_5 so 2 in one of the generators so 2 is a primitive root modulo 5.

Similarly we can verify that 3 is a primitive root modulo 5 so that me 2 and 3 are generation of the cyclic group.

Order of an integer: - fix a positive integer n then by Euler's theorem, for any a∈N, gcd(a, n) = 1, one has $a^{\emptyset(n)} \equiv 1$ (mod n). Therefore, there exists a smallest positive integer say *x* such that $a^x \equiv 1$ (mod n) and $a^k \not\equiv 1$ mod n for 1 ≤ k ≤ x – 1

.

4.4 Primitive roots modulo n

Definition: - Fix a positive integer n and let a∈N with gcd (a, n) = 1.

Then, the least positive integer x such that $a^x \equiv 1$ (mod n) is called the order of a modulo n, denoted $ord_n(a)$.

If $ord_n(a) = \emptyset(n)$ then, a is said to be a primitive root modulo n.

For example, for n = 13, 3 power 1 is 3 congruent mod (13).

$3^1 = 3$ (mod 13), $3^2 \equiv 9$ (mod 13), $3^3 \equiv 1$ (mod 13) so $ord_{13}(3) = 3$. $12^2 \equiv 1$ (mod 13) so $ord_{13}(12) = 2$.

In fact n – 1 ≡ -1 (mod n) every n and hence $ord_n(n-1) = 2$

Example for non-existence of primitive roots:

Example:1- Show that there are no primitive roots modulo 16.

Solution.: U_{16} = {1, 3, 5, 7, 9, 11, 13, 15}.

So $\emptyset(16) = |U_{16}| = 8$ verify that $a^4 \equiv 1 \pmod{16}$. For all $a \in U_{16}$.

Hence there is no element a with (a, 16) = 1 such that $ord_{16}(a) = 8 = \emptyset(16)$

Example:2- for a positive integer n and let $a \in N$ such that gcd (a, n) = 1. If a is primitive root of n and Un= $\{a_1, a_2, \ldots\ldots a_{\emptyset(n)}\}$ then $\{a_1, a_2, \ldots\ldots a_{\emptyset(n)}\} \equiv \{a_1, a_2, \ldots\ldots a^{\emptyset(n)}\} \pmod{n}$

Solution: .: As a is a primitive root modulo n. The numbers ai(mod n) and aj (mod n) are distinct, whenever $1 \leq i \neq j \leq \emptyset(n) - 1$. Moreover, gcd(a, n) = 1 implies that gcd (ak, n) = 1 for all $1 \leq k \leq \emptyset(n)$. Thus the required result follows.

Example:3- Fix a positive integer n and assume that n has a primitive root. Then, the number of primitive roots of n equal $\emptyset(\emptyset(n))$.

Solution:- Note that if a is a primitive root modulo n then, $ord_n(a) = \emptyset(n)$. Now observe that for $1 \leq k \leq \emptyset(n)$.

$Ord_n(a^k) = \emptyset(n)$

If and only if gcd(k, $\emptyset(n)$) = 1 But by definition

$$\left|\{k: 1 \leq k \leq \emptyset(n), \gcd(k, \emptyset(n)) = 1\}\right| = \emptyset(\emptyset(n))$$

Example:4- Find all primitive roots modulo 13.

Solution: Using the example given before, we see that 2 is a primitive root modulo 13. As $\emptyset(13)$ = 12 and the number 1, 5, 7 and 11 are coprime to 12. We see that $2 = 2^1$, $6 \equiv 2^5 \pmod{13}$, $11 \equiv 2^7 \pmod{13}$ and $7 \equiv 2^{11} \pmod{13}$ are the primitive roots modulo 13. Thus the number of primitive roots modulo 13 equal 4 = $\emptyset(\emptyset(13)) = \emptyset(12)$.

Theorem:1- Let n = 2k, for some positive integer k. then, n has a primitive root modulo n (U_n is cyclic) whenever k = 1 or k = 2.

Proof:- If k = 1 or k = 2 then $U_2 = \{1\}$ and $U_4 = \{1, 3\}$ are indeed cyclic. So, we now show that $U_2k(x) < \emptyset(2^k) = 2^{k-1}$, for all $x \in U_2k$. In fact, we will use induction to show that $x^{2^{k-2}} \equiv 1 \pmod{2^k}$. for all $x \in U_2k$ when ever k ≥ 3.

Base case k = 3, $U_8 = \{1, 3, 5, 7\}$ it is easy to check that $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$

Hence ord8(9) ≤ 2 for all a ∈ U_8. Thus U8 is not cyclic and hence no primitive root modulo 8.

We prove the base case now induction hypothesis suppose the result is true for k, where k ≥ 3.

i.e. we assume $x^{2^{k-2}} \equiv 1(mod\ 2^k)\ \forall x \in U_2 k$ with k ≥ 3.

Or equivalently $x^{2^{k-2}} = 1 + m2^k$ for some positive integer m. we will now prove the result for k + 1 that is we need to show that for every $y \in U_{2^{k-2}}$ $y^{2^{k-2}} \equiv 1\ (mod\ 2^{k-2})$

So, Let ∈ $U_{2^{k-2}}$. Then either $1 \le x \le 2^k$ *or* $y = x + 2^k$ with $1 \le x \le 2^k$. In either case , $y = x + t2^k$, where $t \in \{0, 1\}$ and $1 \le x \le 2^k$. Hence using k ≥ 3 and the binomial theorem, we have

$y^{2^{k-2}} = (x + t2^k)^{2^{k-2}} \equiv x^{2^{k-2}}$ (mod 2^{k-2})

$\equiv \left(x^{2^{k-2}}\right)^2$(mod 2^{k-2}).

Thus, using $x^{2^{k-2}}$ = 1 + m2^k for some positive integer m and k ≥ 3. We get

$y^{2^{k-2}} \equiv \left(x^{2^{k-2}}\right)^2$ (mod 2^{k-2}) ≡ (1 + m2^k)^2

= 1 + m2^{k+1} + m$^2 2^{2k}$ ≡ 1 (mod 2^{k+1})

i.e. Un is cyclic.

4.5 Quadratic Residues and Non-Residues

Definition :- Let p be an odd prime and let (a, p) = 1. Then a is said to be a quadratic residue (mod p) if ∃ an integer x such that

$$x^2 \equiv a \pmod{p}$$

otherwise, we say that a is a quadratic non-residue (mod p).

Remark :- If a is a quadratic residue (mod p) ∃ x ($1 \leq x \leq p - 1$) such that $x^2 \equiv a \pmod{p}$

Quadratic Residues:-

Let P be an odd prime and a ∈ N such that gcd(a, p) = 1. If the quadratic congruence $x^2 = a \pmod{p}$ has a solution. Then a is said to be quadratic residue modulo p.

Two basic problems:- Note that if a is a quadratic residue modulo p then, a + kp is also a quadratic residue modulo p for all k ∈ z and hence. Our proofs will mostly consider those a for which $0 \leq a \leq p - 1$.

Two basic problems dominate the theory of quadratic residues.

1. Given a prime p, finding all n ∈ N such that n is a quadratic residue modulo p or finding all m∈N that are quadratic non residue modulo p.

2. Given a number n finding those primes p for which n is a quadratic residue modulo p or the prime q for which n is quadratic non residue modulo q.

Solution: Let p be an odd prime. Then, by definition, a number a∈N can be a quadratic residue modulo p only if gcd(a, p) = 1. Hence, the quadratic residues other than 0 are relatively prime to p.

1 is always a quadratic residue modulo any number n as x1 = 1 (mod n), has solutions 1 and -1 for all n∈N.

Example:-1: To find quadratic residues modulo 1^1. We look at the number 1^2 (mod.11), 2^2 (mod 11), 3^2 (mod. 11).

$5 \equiv 4^2$ (mod 11),

$3 \equiv 6^2$ (mod 11), …….. 10^2 (mod 11) to obtain 1, 4, 9, 5 and 3 as quadratic residues modulo 11.

Similarly, It can be easily verified that 1, 3, 4, 9, 10 and 12 modulo 13.

Now that, In general, if p is a prime then, it suffices to square only the numbers.

1, 2, …….$\frac{p-1}{2}$ as for any x with $\frac{p-1}{2}$ ≤ x ≤ p – 1, we can find y ∈ $\left\{1, 2, \ldots \ldots \ldots \frac{p-1}{2}\right\}$ such that $x = p - y$ and hence $x^2 = y^2$ (mod p)

Moreover, It can be easily verified that for any two numbers *x, y,* ∈ $\left\{1, 2, \ldots \ldots \ldots \frac{p-1}{2}\right\}$, $x^2 \neq y^2$ (mod p). Hence, we obtain the following result.

Theorem:-2: Let p be an odd prime. Then, every reduced residue system modulo p contains exactly $\frac{p-1}{2}$ quadratic residues and exactly $\frac{p-1}{2}$ quadratic non-residues modulo p.

Further more, the quadratic residue classes correspond to the numbers

1^2 (mod p), 2^2 (mod p), ……$(\frac{p-1}{2})^2$ (mod p).

4.6 Legendre Symbol:

Definition: - The Legendre Symbol denoted by $\left(\frac{a}{p}\right)$, where (a, p) = 1 is defined as

$\left(\frac{a}{p}\right)$ = 1 if a is a quadratic residue (mod p) and

$\left(\frac{a}{p}\right)$ = 1, if a is a quadratic non-residue (mod p).

Remark: - If a ≡ b (mod p), clearly $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ provided (a, b) = 1

4.7 Properties of Legendre Symbol: -

Theorem:3- Let p be an odd prime and let a and b be two integers that are relatively prime to p then, the Legendre symbol satisfies the following Properties: -

If $a \equiv b \pmod p$ then, $(a/p) = (b/p)$

$(a^2/p) = 1$

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

$(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$

$(ab/p) = (a/p)(b/p)$

Proof:- Let $a \equiv b \pmod p$. Then $a = b + kp$ for some $k \in z$.

hence $x^2 \equiv a \equiv b + kp = b \pmod p$.

Thus, $(a/p) = 1$ if and only if $(b/p) = 1$, or equivalently, $(a/p) = (b/p)$

Clearly, the quadratic equivalence $x^2 \equiv a^2 \pmod p$ has $\pm a$ as a solution and hence $a^2/p = 1$.

By theorem 2 (Euler's criterion) a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. Also (a/p) = 1 if and oly if a is a quadratic residue modulo p and hence, $a/p = a^{(p-1)/2} \pmod{p}$

Follows form the previous statement.

We know that ab is a quadratic residue modulo p if and only if either "both a and b are quadratic residues modulo p" or "both a and b are quadratic non-residues modulo p" or equivalently, either "both (a/p) = (b/p) = 1" or both (a/p) = (b/p) = -1"

Thus, (ab/p) = (a/p)(b/p). In other words legendre symbol is a completely multiplicative function for a fixed prime p.

Theorem:-4: Let p be an odd prime, then

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$$

$$\left(-\frac{1}{p}\right) = \begin{cases} 1, if\ p = 4k+1 \\ -1, if\ p = 4k+3 \end{cases}$$

Proof 1:-

Since p is an odd prime, by theorem (2) the number of quadratic residues modulo p and the number of quadratic non-residues modulo p is the same and this number equals $\left(\frac{p-1}{2}\right)$.

Thus, the numbers 1 and -1 appear exactly $\frac{p-1}{2}$ times in

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right), \text{ and hence } \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$$

Proof 2:- By theorem 5 (-1/p) = $(-1)^{\frac{p-1}{2}}$ so (-1/p) = 1 if and only if $\frac{p-1}{2}$ = 2k for some positive integer k. But this holds if and only if p = 4k + 1. Thus the required result follows.

Example:1-Let p be an odd prime dividing $9^n + 1$ for some positive integer n. Then, prove that p ≡ 1 (mod 4).

Solution: Let p be an odd prime dividing $9^n + 1$. Then $9^n + 1 \equiv 0 \pmod{p}$ or equivalently, $(3^n)^2 \equiv -2 \pmod{p}$.

Thus, (-1/p) = 1 and hence by theorem (6.2)(Previous theorem), p ≡ 1 (mod 4).

Theorem:5- There are infinitely many primes of the form 4k + 1.

Proof:- Let if possible, suppose there are only finitely many primes of the form 4k + 1 say p_1, p_2, …… p_n. Consider the positive integer N = $(2p_1p_2, \ldots..p_n)^2 + 1$. Then N > 1 is odd and hence there is an odd prime, say p dividing N. Hence $(2p_1p_2\ldots.p_n)^2 \equiv -1 \pmod{p}$ that is (-1/p) = 1 and hence by theorem (6.2), p ≡ 1 (mod 4) clearly p ≠ pi for 1 ≤ i ≤ n Hence, the required result follows.

Cont.: Let p be a prime with p ≡ 1 (mod 4). Then, verify that the sum of the quadratic residues modulo p that lie in the set (1, 2, ….. p-1) is equal to $\frac{p(p-1)}{4}$.

Proof:- Let a_1, a_2, …….ar be all the quadratic residues modulo p that are less than p/2. Since p ≡ 1 (mod 4) (-1/p) = 1 and hence the number p – a, p – a_2 ….., p – ar are all the quadratic residues modulo p that are greater than p/2. As the number of quadratic residues modulo p equals $\frac{p-1}{2}$, we see that $r = \frac{p-1}{4}$. Thus the required sum equals

$$\sum_{i=1}^{r} a_i + \sum_{i=1}^{r} (p - a_i) = \sum_{i=1}^{r} p = pr = \frac{p(p-1)}{4}$$

Example:4- Let p be an odd prime and a, b ∈ N such that gcd (ab, p) = 1. Then exactly one of a or b or ab is a quadratic residue modulo p.

Let p be an odd prime. Then, show that there are $\frac{p-1}{2} - \emptyset(p-1)$ quadratic non-residues which are not primitive roots modulo p.

For any odd prime p there are $\frac{1}{4}(p-4-(-1))^{p-1/2}$ consecutive pairs of quadratic residues exists.

Solution: If both k and k + 1 are quadratic residues then $\left(\frac{k}{p}\right) = \left(\frac{k+1}{p}\right) = 1$. Other wise $\left(1+\frac{k}{p}\right)$ or $\left(\frac{k+1}{p}\right)$ is zero.

Hence the number of consecutive pairs of quadratic residues is $\frac{1}{4}\left[\sum_{k=1}^{p-2}\left(1+\left(k/p\right)\right).\left(1+\left(\frac{k+1}{p}\right)\right)\right]$. If we simplify and use the fact that $\sum_{a=1}^{p=1}\left(\frac{a}{p}\right) = 0$, we get

$\Rightarrow \frac{1}{4}\left[p-2+\sum_{k=1}^{p=2}\left(\frac{k}{p}\right)+\sum_{k=1}^{p=2}\left(\frac{k+1}{p}\right)+x\right]$,

Where $x = \sum_{k=1}^{p=2}\left(\frac{k(k+1)}{p}\right) = \sum_{k=1}^{p=2}\left(\frac{k^2}{p}\right)\left(1+\frac{k-1}{p}\right)$

$\Rightarrow \sum_{k=1}^{p=2}\left(1+\frac{k^{-1}}{p}\right) = -1$

Hence the required answer is

$$\Rightarrow \frac{1}{4}\left[p-2-\left(\frac{p-1}{p}\right)-\left(\frac{1}{p}\right)-1\right]$$

$$\Rightarrow \frac{1}{4}\left[p-4-\left(\frac{p-1}{p}\right)\right]=\frac{1}{4}\left[p-4-(-1)^{(p-1)/2}\right]$$

Example:5- Check whether $x^2 \equiv 73 \pmod{173}$ is solvable or not?

Solution: .: First note that $x^2 \equiv 73 \pmod{173}$ is solvable if and only if $\left(\frac{73}{173}\right)=1$.

Hence it is sufficient to compute $\left(\frac{73}{173}\right)$.

$\left(\frac{73}{173}\right)=\left(\frac{-100}{173}\right)=\left(\frac{-1}{173}\right)=1$ as 173 is prime of the form 4k + 1.

Theorem :6- Let p be an odd prime and let gcd (a, p) = 1 then

$$\underline{p-1} = -\left(\frac{a}{p}\right).a^{\frac{1}{2}(p-1)} \pmod{p}$$

Proof :- Let S = {1, 2,…, p – 1} is a reduced set of residues (mod p).

Consider any x such that

1 ≤ x ≤ p – 1 then

xS = {x, 2x,…, (p – 1)x}

is also a reduced set of residues (mod p)

So there exists y in S such that $xy \equiv a \pmod{p}$

Now distinguish two cases

Case I: $\left(\frac{a}{p}\right) = 1$ then ∃ such that $1 \leq x \leq p - 1$

$$x^2 \equiv a \pmod{p}$$

Let us find out all the solutions of the quadratic congruence

$$x^2 \equiv a \pmod{p} \quad \text{.....(I)}$$

Then (I) has at least one solution X = x. We know two solutions x_1 and x_2 are said to be same if $x_1 \equiv x_2 \pmod{p}$. Let x_1 & x_2 be two solutions of (I) then

$$x_1^2 \equiv a \text{ (mos p)}$$

and $$x_2^2 \equiv a \text{ (mos p)}$$

$$x_1^2 \equiv x_2^2 \pmod{p}$$

$$p \text{ divides } (x_1^2 - x_2^2)$$

$$p \mid (x_1 + x_2)(x_1 - x_2)$$

then $$p \mid (x_1 + x_2) \text{ or } (x_1 - x_2) \quad (\because p \text{ is a prime})$$

either $x_1 + x_2 \equiv 0 \pmod{p}$

or $x_1 - x_2 \equiv 0 \pmod{p}$

further $x_2 \equiv x_1 \equiv p - x_1 \pmod{p}$

or $x_2 \equiv x_1 \pmod{p}$

So (I) has exactly two solutions (mod p)

Thus x and p – x are two solutions of (1) (mod p) since x is a solutions of (1) (mod p)

Further $x \neq p - x$

$\because$ p is odd

So (I) has exactly two solutions (mod p)

Let us take y_1 in S such that $y_1 \neq x$ & $y_1 \neq (p - x)$

Now consider the set y_1 S. Then y_1 S is also a reduced residue system (mod p). So $\exists$ y_2 in S such that

$$y_1 y_2 \equiv a \pmod{p}$$

and further y_1 y_2 since otherwise y_1 will also be a solution of (1). Thus for $y_1 \neq x$, $y_1 \neq p - x$, the remaining $(p - 3)$ elements in S can be divided into $\frac{p-3}{2}$ pairs (y_1, y_2) such that

$$y_1 y_2 \equiv a \pmod{p}$$

so

1.2.3 ……$(p - 1) = x.(p - x)(y_1, y_2)$

$$\equiv x^2 . a^{\frac{p-3}{2}} \pmod{p}$$

$$\equiv a^{\frac{1}{2}(p-1)} \pmod{p} \quad (\therefore x2 \equiv a \pmod{p})$$

$$\equiv \left(\frac{a}{p}\right) a^{\frac{1}{2}(p-1)} \pmod{p} \quad \left(\therefore \left(\frac{a}{p}\right) = 1\right)$$

Case II: $\left(\frac{a}{p}\right) = -1$

Then the congruence (1) has no solutions. So if we take $y_1 \in S$, we know $\exists$ y_2 $\in S$ such that

$$y_1 y_2 \equiv a \pmod{p} \text{ amd } y_1 \neq y_2$$

Thus we divide S into (p - 1)/2 pairs (y_1, y_2) such that $y_1 y_2$ $\equiv a \pmod{p}$

$$(p-1)! \equiv a^{\frac{p-1}{2}} \text{ (mod p)} \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \text{ (mod p)} \left(\therefore \left(\frac{a}{p}\right) - 1\right)$$

Thus theorem is proved completely.

4.8 Theorem: 7- Wilson's Theorem

If p is any prime, then$(p-1)! \equiv -1$ (mod p)

Proof :- If p = 2 or p = 3; theorem is clearly true.

So let p ≡ 5. Taking a = 1 in the last theorem we note $\left(\frac{1}{p}\right) = 1$ for all prime p.

Then we get

$$(p-1)! \equiv -1 \text{ (mod p)}$$

Converse of Wilson's Theorem: - The converse of Wilson‟s theorem is also

true. Given that$(n-1)! \equiv -1$ (mod p), they must be a prime.

Proof:- If possible, suppose n is not a prime. Then there exists a divisor d of n such that

1 < d < n, then d| $(n-1)!$

$\therefore$ $(n-1)! \equiv 0$ (mod d)

On the other hand

$(n-1)! \equiv -1 \pmod{n}$

$(n-1)! \equiv -1 \pmod{d}$

$-1 \equiv 0 \pmod{d} \Rightarrow d \mid 1$ which contradicts that $d > 1$

So n must be a prime number.

4.9 Theorem: 8- (Euler's Criterion)

Let p be an odd prime and let gcd (a, p) ≡ 1 Then

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

Proof :- We know

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

We also know $(p-1)! \equiv -1 \pmod{p}$

$\Rightarrow \quad -1 \equiv \left(\frac{a}{p}\right) a^{\frac{1}{2}(p-1)} \pmod{p}$

Multiplying by $\left(\frac{a}{p}\right)$ we get

$$\left(\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right)^2 a^{\frac{1}{2}(p-1)} \equiv a^{\frac{1}{2}(p-1)} \text{ (mod p)}$$

Theorem:9- -1 is a quad reside of primes of the form 4k + 1 & a quad non- residue of primes of the form 4 k + 3.

Proof :- By Euler‟s Criterion

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \text{ (mod p)}$$

$$\Rightarrow \quad p \left| \left[\left(\frac{-1}{p}\right) - (-1)^{\frac{1}{2}(p-1)}\right] \right.$$

The value of the quantity in brackets is either 0 or -2. But p is an odd prime and it divides the quantity in brackets, so we must have

$$\left(\frac{-1}{p}\right) - (-1)^{\frac{1}{2}(p-1)} = 0$$

$$\Rightarrow \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$$

When p = 4k + 1, $\left(\frac{-1}{p}\right) = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$

And when p = 4k + 3,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1$$

Theorem:10- Let a & b be integers such that gcd (ab, p) =1, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof :- By Eule's criterian

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{1}{2}(p-1)} = (a)^{\frac{1}{2}(p-1)}(b)^{\frac{1}{2}(p-1)} \quad \ldots\ldots\ldots\ldots (1)$$

But gcd (ab, p) = 1 ⇒ p∤ (a b)

⇒ b ∤ a and p ∤ b.

⇒ g c d (a, p) = 1 = gcd (b, p)

By Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \text{ (mod p)} \qquad \ldots\ldots\ldots\ldots (2)$$

and $$\left(\frac{b}{p}\right) \equiv b^{\frac{1}{2}(p-1)} \text{ (mod p)} \qquad \ldots\ldots\ldots\ldots (3)$$

From (2), (3), we get

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \text{ (mod p)}$$

$\Rightarrow \quad p \left| \left(\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \right) \right.$ (∵ p is an odd prime)

Corollary :- The product of two quadratic residues (mod p) or two quadratic non-residues (mod p) is a quadratic residues (mod p) where as the product of a quadratic residue (mod p) and a quadratic non-residue (mod p) is quadratic non-residue (mod p)

Theorem :11- Let p be an odd prime and let p does not divide product ab where a & b are integers. Then $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof:- Since p ł ab ⇒ p ł a & p ł b

⇒ p ł b^2,

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)$$

$$= \left(\frac{a}{p}\right)$$

[∵ $(\pm 1)^2 = 1$]

Theorem:12- Given any odd prime p, there are $\frac{1}{2}(p-1)$ quadratic residue & $\frac{1}{2}(p-1)$ quadratic non-residues.

Proof :- Let a be any quadratic residue then ∃ x (1 ≤ x ≤ p – 1) such that

$x^2 \equiv a \pmod{p}$

But $x^2 \equiv (p - x)^2 \pmod{p}$

Therefore $1^2 \equiv (p - 1)^2 \pmod{p}$

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

…….

…….

$\left(\frac{p-1}{2}\right)^2 \equiv \left(p - \frac{p-1}{2}\right)^2 = \left(\frac{p+1}{2}\right)^2 \pmod{p}$

Thus there are a maximum of $\frac{p-1}{2}$ quadratic residue (mod p)

But for $1 \le i, j \le \frac{p-1}{2}$, $i \neq j$

$i^2 \equiv j^2 \pmod{p}$

since if $i^2 \equiv j^2 \pmod{p} \Rightarrow p|(i^2 - j^2)$

$\Rightarrow$ $p|(i + j)(i - j) \Longrightarrow p|(i + j)\ or\ p|(i - j)$

Which is not possible under the given condition. So there are exactly $\frac{1}{2}(p-1)$ quadratic residues.

The remaining $\frac{p-1}{2}$ numbers must be quadratic non-residues.

Theorem 13:- Given any prime p of the for 4k + 1, ∃ x and on integers m such that

$$1 + x^2 = mp \text{ where } 1 \leq m < p$$

Proof:- Since -1 is a quadratic residue of primes of the form 4k + 1, ∃ x such that

$$x^2 = -1 \pmod{p}$$

∴ W.L.O.G, we can assume $1 \leq x \leq \frac{p-1}{2}$

Then ∃ an integer m such that

$$mp = x^2 + 1 \leq x \leq \left(\frac{p-1}{2}\right)^2 < p^2$$

⇒ $m < p$

Clearly $m > o$

⇒ $1 \leq m \leq p$

Theorem 14:- Given any prime p, there exist $x \geq 0$, $y \geq 0$ and $m(1 \leq m < p)$ such that $1 + x^2 + y^2 = mp$

Proof:- If p = 2, theorem is trivially true

$\because \quad 1 + 1^2 = 2 = 1 \cdot 2$

So let p be an odd prime.

Consider S = $\left\{-x^2; x = 0,1,2, \ldots \ldots, \frac{p-1}{2}\right\}$

T = $\left\{1 + y^2; y = 0,1,2, \ldots \ldots, \frac{p-1}{2}\right\}$

Here elements of S are mutually incongruent (mod p)

Similarly elements of T are mutually incongruent. S contains $\frac{p+1}{2}$ elements and T also contain $\frac{p+1}{2}$ elements.

$\therefore$ SUT contains p + 1 district element. But there are only p residue classes (mod p)

Therefore at least two elements of SUT must be congruent to each other (mod p). However, no element of S is congruent to another element of S and no element of T is congruent to another element of T. So at least one element of S must be congruent to an element of T i.e.,

$\exists$ x, y such that $0 \le x \le p - \frac{1}{2}$ and $0 \le y \le p - \frac{1}{2}$ such that

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

Or $$1 + x^2 + y^2 = 0 \pmod{p}$$

So, $\exists$ an integer m such that

$$1 + x^2 + y^2 = mp$$

Clearly $m > p$

Now $$mp = 1 + x^2 + y^2 \le 1 + \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2$$

$$< 1 + \frac{p^2}{4} + \frac{p^2}{4} < p^2$$

$\Rightarrow$ $m < p$ and so $1 \le m < p$ which proves the theorem.

Definition:- Let $m \ge 2$ be any given integer and let gcd (a, m) = 1 for some integer a. They by Euler fermat theorem,

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

Now take $S = \{n \in N; a^n \equiv 1 \pmod{m}\}$

Then S ≠ Ø since Ø(m)∈S. so by L.W.O., S has a smallest element say 'd'. Then we say d is the order of a (mod m) and we write d = ord_m^a (order a mod m)

Theorem 16: Let ord_m^a = d then

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

⇒ d | n. In particular d | Ø(m)

Proof:- Since $a^{\emptyset} = 1 \pmod{m}$, so if d | n, then

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

Now let $a^n = 1 \pmod{m}$. By division algorithm theorem, write

$$n = dq + r,\ 0 \le r < d$$

then

$$1 \equiv a^n = a^{dq+r} = a^{d/q} - a^r$$

$$= (a^d)q.a^r$$

$$= a^r \pmod{m} \qquad (\because a^d \equiv 1 \pmod{m})$$

So if r ≠ 0, then we get a number r < d such that $a^r \equiv 1 \pmod{m}$ which contradicts the definition of d

⇒ r = 0 ⇒ d| n

Theorem 17 : Let ord_m^a = d. Then for any positive integer k,

$$ord_m^{a^k} = \frac{d}{\gcd(d,k)}$$

Proof:- Let gcd(d, k) = g and $ord_m^{a^k} = r$

Then $1 = (a^k)^r \equiv a^{kr} \pmod m$

⇒ d| kr

⇒ $\frac{d}{g} \left| \left(\frac{k}{g}\right) r \right.$

But $gcd\left(\frac{d}{g}.\frac{k}{g}\right) = 1$

⇒ $\frac{d}{q} | r \quad \Rightarrow \frac{d}{q} \leq r$. Now since gcd(d, k) = q

⇒ q| d, q| k

Let k = qk_1

Now $(a^k)^{\frac{d}{q}} = (a^{qk_1})^{\frac{d}{q}} = (a^{k_1 d}) = (a^d)^{k_1}$

$\equiv 1 \pmod m$

$\Rightarrow \quad r \leq \frac{d}{g}$ [by definition of order]

So $\frac{d}{g} = r$

Or $r = \frac{d}{q}$

Hence the theorem.

Theorem:18 (Euler's Criterion):-

Let p be an odd prime and let a ∈ N such that gcd (a, p) = 1, then, a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Proof:- Suppose a is quadratic residue modulo p. Hence, by definition, the quadratic equivalence $x^2 \equiv a \pmod{p}$ has a solution, say x_0, As gcd (a, p) = 1. We get gcd(x, p) = 1. Therefore, by fermat's little theorem, we have

$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv (x_0)^{p-1} \equiv 1 \pmod{p}$.

Conversely, assume that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

As p is an odd prime, so up is cyclic and hence there exists r ∈ N such that r is a primitive root modulo p.

As gcd (a, p) = 1, there exists a, k, $1 \leq k \leq p - 1$

Such that $a \equiv r^k \pmod{p}$

Thus, we see that

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

And hence p – 1 = ord p (r) divides $k\,\frac{p-1}{2}$.

Therefore k = 2j, for some j and hence r^j is a solution of the quadratic equivalence $x^2 \equiv a \pmod{p}$ as $(r^j)^2 = r^{2j} = r^k = a \pmod{p}$

Even powers of a primitive root are quadratic residues:- The proof of above theorem suggests that, if r is a primitive root of an off prime p then, the set of quadratic residues modulo p is the set $\{r^2, r^4, r^6, \ldots\ldots r^{p-1}\}$

And the set of all quadratic non-residues modulo p is given by the set $\{r^1, r^3, r^5, \ldots\ldots r^{p-2}\}$

Further, one can check that

$$r^{2j},\ r^{2k} = r^{2(j+k)},\ 1 = r^{p-1} \text{ and } (r^{2j})^{-1} = r^{p-2j-1}$$

and hence, the set of all quadratic residues modulo p forms a multiplicative abelian group.

r^{2j+1}, $r^{2k+1} = r^{2(j+k+1)}$ and hence, the product of two quadratic non-residues modulo p is a quadratic residue modulo p.

r^{2j}, $r^{2k+1} = r^{2(j+k)+1}$ and hence, the product of a quadratic residue modulo p and a quadratic non-residue modulo p is a quadratic non-residue modulo p.

Example:-2: Let p be an odd prime and let r be a primitive root modulo p. Then

The product of quadratic residues is congruent modulo p to r $\frac{p-1}{2}$.

The product of quadratic non-residues is congruent modulo p to r $\frac{(p-1)^2}{2}$.

Solution:- By the above observation

{r^2, r^4, r^6, .,……. r^{p-1}} is the set of all quadratic residues modulo p. Hence,

r^2, r^4, r^6, ……. $r^{p-1} = r^{2+4+6+\ldots.+p+1}$

$$= r^{2(1+2+3+\ldots\ldots\frac{p-1}{2})}$$

$$= r^{2.\frac{1}{2}.\frac{p-1}{2}.\frac{p+1}{2}}$$

$$= r^{\frac{p^2-1}{4}}$$

As $\{r^1, r^3, r^5, \ldots\ldots\ldots\ldots r^{p-2}\}$ is the set of all quadratic non-residues modulo p. we have

$$r^1, r^3, r^5, \ldots\ldots\ldots\ldots r^{p-2} = r^{1+3+5+\cdots..+2\frac{p-1}{2}-1}$$

$$= r^{\frac{(p-1)^2}{4}}$$

4.10 Summary

In this Unit, we defined the quadratic residue (and non residues) and established some of their basic properties. We demonstrate which integers have primitive roots. We start by showing that every power of an odd prime has a primitive root and to do this we start by showing that every square of an odd prime has a primitive root. We defined the Legendre symbols which allow us to detect quadratic residues and non residues. We proved the Euler's criterion, which provides a method for calculating Legendre symbols efficiently.

4.11 Terminal Questions

1. Find a primitive root (mod 23).

……

……

……..

2. Find a primitive root of (mod 43).

……

……

……..

3. If p is a prime of the form 4t + 1, show that a is a primitive root (mod p) if and only if $-a$ is a primitive root (mod p).

……

……

……..

4. Find the following Legendre symbols: (a) $\left(\frac{19}{41}\right)$ (b) $\left(\frac{3}{7}\right)$ (c) $\left(\frac{5}{11}\right)$ (d) $\left(\frac{6}{11}\right)$

……

……

……..

5. Compute the following Legendre symbols: (a) $\left(\frac{109}{337}\right)$ (b) $\left(\frac{41}{61}\right)$ (c) $\left(\frac{73}{191}\right)$ (d) $\left(\frac{34}{71}\right)$

……

……

……..

6. Describe the primes p for which $x^2 - 7$ splits into linear factors modulo p.

……

……

……..

7. If $p = 2^{2^k} + 1$, for some $k \geq 1$ is a prime, so that 3 is a primitive root for $U(Z_p)$.

……

……

……..

8. For g = 2,3,5,7,11 determine a prime number p > g such that g is a primitive root mod p.

……

……

……..

9. The set {1,5,7,11} is a reduced residue system modulo 12..

……

……

……..

10. Check whether the Quadratic residue $(\boldsymbol{i})\left(\frac{10}{13}\right)$ $(\boldsymbol{ii})\left(\frac{7}{13}\right)$

……

……

……..

Unit 5 Gauss's lemma and Quadratic residues

Structure

5.1. INTRODUCTION

This unit introduces Gauss's lemma in number theory gives a condition for an integer to be a quadratic residue. It made its first appearance in Carl Friedrich Gauss's third proof (1808) of quadratic reciprocity and he proved it again in his fifth proof (1818). Gauss's lemma plays an important role in the study of unique factorization. Gauss reciprocity law **A relation connecting the values of the Legendre symbols for different odd prime numbers and** Quadratic reciprocity law. In addition to the principal reciprocity law of Gauss for quadratic residues, which may be expressed as the relation.

Let p and q be two distinct odd primes. Then, the quadratic reciprocity law relates the numbers (p=q) and (q=p). In particular, it gives us an algorithm to find whether p is a quadratic residue modulo q or not, depending on whether q is a quadratic residue modulo p or not. Gauss gave many different proofs of this law, some of which led to completely new areas of number theory.

5.2. Objectives

After studying this unit we should be able to:

· Statement and Proof Gauss lemma

· Application of Gauss lemma

· Define Gauss reciprocity theorem

· Gauss criterion for quadratic residues

· Check the Quadratic residues for prime-power moduli

· Define the Quadratic residues for arbitrary moduli

· Finding all primes p such that 2 is a quadratic residue modulo p

---

5.3 Gauss's Lemma:

Statement: Let p be an odd prime and let gcd (a, p) = 1

Let $S = \left\{1, 2, \ldots., \frac{p-1}{2}\right\}$

Let μ be the number of elements in the set S such that least positive residue of a

S > p/2

Then $\left(\frac{a}{p}\right) = (-1)^{\mu}$

Proof:- Consider any integer n where gcd(n, p) = 1. Apply division algorithm to n & p, ∃ q & r such that n = qp + r where $0 \leq r \leq (p - 1)$. Since gcd (n ,p) = 1

$\Rightarrow$ $p \nmid n \Rightarrow r \neq 0$

$\Rightarrow$ $1 \leq r \leq p - 1$

Since p is odd p/2 is not an integer. So either $r < p/2$ or $r > p/2$. If $r < p/2$, we leave it as it is if $r > p/2$, write $r = p - r'$ where $1 \leq r' < p/2$,

Thus $n = qp + (p-r') = (q+1)p-r' \equiv -r' \pmod{m}$.

Now we consider least positive residues of every element of aS. We are given that μ of those elements have least positive residues > p/2. Let k be the elements of as with least positive residues < p/2.

Then $k + \mu = \frac{p-1}{2}$

If the least positive residues <p/2 are $r_1, r_2, \ldots\ldots r_k$ and the least positive residues >p/2 are $-r_1, -r_2, \ldots\ldots -r_\mu$ such that $1 \leq r_\mu \leq \frac{p-1}{2}$ then

$$r_1, \ldots\ldots r_k, -r_1, -r_2 \ldots\ldots, -r_\mu$$

are the residues of elements of aS in some order such that

$$1 \leq r \leq \frac{p-1}{2} \text{ or } 1 \leq r' \leq \frac{p-1}{2}$$

Since S is a subset of a reduced residue set {1, 2, ……, p-1} and gcd(1, p)=1, so {a, 2a, …..,(p-1)a} is also a reduced residue set. Then first of all

$$r_i \neq r_j \text{ for } i \neq j$$

If possible, let $r_i = r_j$ for some pair (i, j)

Then $\exists\ x_i \in S$ and $x_j \in S$ such that

$$ax_i \equiv r_i \pmod{p} \ \& \ ax_j \equiv -r_j \pmod{p}$$

But $r_i = r_j$

$\Rightarrow$ $ax_i \equiv ax_j \pmod{p}$

This means $a(x_i + x_j) \equiv 0 \pmod{p}$

$\Rightarrow$ $p \mid a(x_i + x_j)$

But $\gcd(a, p) = 1$

$\Rightarrow$ $p \mid a(x_i + x_j)$

But $1 < x_i \leq \frac{p-1}{2}$

And $1 \leq x_j \leq \frac{p-1}{2}$

$\Rightarrow \quad 2 \leq x_i + x_j \leq p - 1$

$\Rightarrow \quad p \nmid (x_i + x_j)$

Which is a contradiction and so $\{r_1, r_2, \ldots..r_k, r_1', r_2', \ldots..r_\mu'\}$ are all distinct.

But $\quad \mu + k = \frac{p-1}{2}$

So there are $\frac{p-1}{2}$ distinct numbers lying between 1 & $\frac{p-1}{2}$

So $\quad r_1. \ldots\ldots.r_k, r_1'\ldots\ldots.r_\mu'$

Are the natural numbers 1 to $\frac{p-1}{2}$ in some order. Therefore

$$\left\lfloor \frac{p-1}{2} \right\rfloor = r_1. \ldots\ldots.r_k, r_1'\ldots\ldots.r_\mu' \pmod p$$

Then by definition of $r_1. \ldots\ldots.r_k, r_1'\ldots\ldots.r_\mu'$

$$\left\lfloor \frac{p-1}{2} \right\rfloor \equiv a.2a \ldots\ldots \frac{p-1}{2}.a(-1)^\mu \pmod p$$

$$= (-1)^\mu \left(\left\lfloor \frac{p-1}{2} \right\rfloor \right) a^{\frac{p-1}{2}} \pmod p$$

But $\quad \gcd\left(\left\lfloor \frac{p-1}{2} \right\rfloor, p \right) = 1$

$\Rightarrow \quad (-1)^{\mu} a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

But by Euler's criterion,

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

$\Rightarrow \quad (-1)^{\mu} \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$

$\Rightarrow \quad \left(\frac{a}{p}\right) \equiv (-1)^{\mu} \pmod{p}$

But the value of $\left(\frac{a}{p}\right) - (-1)^{\mu}$ is either 2 or 0 or -2 and p is an odd prime

$\Rightarrow \quad \left(\frac{a}{p}\right) = (-1)^{\mu}$

Example: $x^2 \equiv 5(mod\ 61)$

Solution: $x^2 \equiv 5(mod\ 61)$

According to Euler's Criterion, the equation

$x^2 \equiv 5(mod\ 61)$ has solutions since.$5^{30} \equiv 1(mod\ 61)$ To find the solutions, we keep adding the modulus to $a = 5$ until we get a perfect square.

$$x^2 \equiv 5 \equiv 5 + 61 \equiv 5 + 2(61) \equiv \cdots \equiv 5 + 20(61) = 1225$$

$$= 35^2 (mod\ 61)$$

So we have $x^2 \equiv 35^2 (mod\ 61)$ which gives $x = 35$ and $x = -35$. The solutions are $x^2 \equiv -35 \equiv 26\ (mod\ 61)$and $x \equiv 35 (mod\ 61)$

Example: $x^2 \equiv 899 (mod\ 50261)$

Solution: $x^2 \equiv 899 (mod\ 50261)$

Since,$899^{25130} \equiv 1 (mod\ 50261)$ the equation has solutions. We then add the modulus repeatedly to 899 until we get a perfect square. So we have $x^2 \equiv 14696^2 (mod\ 50261)$which gives $x = 14696$and $x = -14696$. The solutions

are $x = 14696\ (mod 50261)$and $x = -14696 \equiv 35565 (mod\ 50261)$

Example: Let a = 7 and p = 17.

Then {7 · 1 (mod 17), 7 · 2 (mod 17), 7 · 3 (mod 17),

7 · 4(mod 17), 7·5 (mod 17), 7·6 (mod 17), 7·7 (mod 17), 7·8 (mod 17)}

= {7, 14, 4, 11, 1, 8, 15, 5}.

Since 17/2 = 8.5, hence three numbers 14, 11, 15 are greater than p/2.

Thus $(7/17) = (-1)^3 = -1$.

Where as if choose a = 17, p = 7, then

$\{17 \cdot 1 (\text{mod } 7), 17 \cdot 2 (\text{mod } 7), 17 \cdot 3 \quad (\text{mod } 7)\} = \{3, 6, 2\}$

Hence $(17/7) = (-1)^1 = -1$

Theorem. If p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \; if \; p \equiv 1 \pmod 8 \; or \; p \equiv 7 \pmod 8 \\ -1 \; if \; p \equiv 3 \pmod 8 \; or \; p \equiv 5 \pmod 8 \end{cases}$$

Proof. Since p is an odd prime, gcd(2, p) = 1. Thus, one can apply Gauss lemma (see Theorem 1), for a = 2 to get S = {2, 4, . . . , p − 1}. Let us now compute n for different values of the prime p.

Case p = 4k + 1: Then, the numbers $2k + 2 = \frac{p+3}{2}, \frac{p+7}{2}. . . , p - 1$ are elements of S that exceed $p/2$. Thus, in this case n = p−1 and hence, $(2/p) = (-1)^{\frac{p-1}{4}} = (-1)^k$.

Therefore, we see that (2/p) = 1 whenever k is even (corresponds to the case p ≡ 1 (mod 8))

and (2/p) = −1 whenever k is odd (corresponds to the case p ≡ 5 (mod 8)).

Case p = 4k + 3: In this case, the numbers 2k + 2 = $\frac{p+1}{2}$, $\frac{p+5}{2}$, . . . , p − 1 are elements of S that exceed p/2. Thus, in this case n = $\frac{p+1}{4}$ and hence, (2/p) = $(-1)^{\frac{p+1}{4}} = (-1)^{k+1}$

Therefore, as above, (2/p) = 1 whenever k is odd (corresponds to the case p ≡ 7 (mod 8)) and (2/p) = −1 whenever k is even (corresponds to the case p ≡ 3 (mod 8).

We state a corollary of the above theorem which follows from the fact that $\frac{p^2-1}{8}$ is even if and only if either p ≡ 1 (mod 8) or p ≡ 7 (mod 8) and hence we omit the proof.

Corollary 4. Let p be an odd prime. Then, (2/p) = $(-1)^{\frac{p^2-1}{8}}$.

Example: Let p be a prime of the form p ≡ 7 (mod 8). Then prove that p divides $2^{\frac{p-1}{2}} - 1$.

Solution: Using Theorem 3, we know that (2/p) = 1 whenever p ≡ 7 (mod 8). Therefore, using

Theorem 8.3 of Module 2 of Chapter 4, we have $1 = (2/p) \equiv 2^{\frac{p-1}{2}} \pmod{p}$.

Hence, p divides $2^{\frac{p-1}{2}} - 1$.

Example: If $n \in \{11, 23, 83, 131, 179, 183, 239, 251\}$ then, $2n - 1$ is composite.

Solution: Let $n \in \{11, 23, 83, 131, 179, 183, 239, 251\}$. Then,

$$2n + 1 \in \{23, 47, 167, 263, 359, 367, 479, 503\}.$$

This set contains primes of the form $8k + 7$ and therefore, from the above problem, we see that $2n + 1 | 2^n - 1$ as $n = \frac{p-1}{2}$. Thus, the required result follows.

5.4 Application of Gauss's Lemma"-

Theorem : for every odd prime p,

$$\left(\frac{2}{p}\right) = (-1)^{1/4(p+1)}$$

When [x] means greatest integer

Proof:- Let $S = \left\{1,2, \ldots \ldots \frac{p-1}{2}\right\}$

Then $2S = \{2, 4, \ldots\ldots p - 1\}$

Let $x \in S$, then the number of elements of 2S with least positive value $< \frac{p}{2}$ is $x < \frac{p}{2}$

But x is an integer $\Rightarrow x = [p/4]$

$\therefore$ The number of elements of 2S with least positive value > p/2 is $\frac{p-1}{2} - \left[\frac{p}{4}\right]$

(i) If p is of the form 4k + 1, then

$$\mu = \left(\frac{p-1}{2}\right) - \left[\frac{p}{4}\right]$$

$$= 2k - k = k = \left[\frac{p-1}{4}\right] = \left[\frac{p+1}{4}\right]$$

(ii) If p is of the form, 4k + 3 then

$$\mu = \left(\frac{p-1}{2}\right) - \left[\frac{p}{4}\right] = \frac{4k+3-1}{2} - \left[\frac{4k+3}{4}\right]$$

$= 2k + 1 - k = k + 1 = \left[\frac{k+1}{4}\right]$

Thus in both cases, $\mu = \left(\frac{p+1}{4}\right)$

So by Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\left[\frac{1}{4}(p+1)\right]}$$

Corollary:- 2 is a quadratic residue of primes of the form 8k ± 1 and quadratic non residues of primes of the form 8k ±3

Proof:- Let p = 8k ± 1

Then $\left[\frac{1}{4}(k+1)\right] = \left[\frac{1}{4}(8k \mp 1 + 1)\right] = 2k$

Therefore, in these two cases

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{1}{4}(p+1)\right]} = (-1)^{2k} = 1$$

Let p = 8k ±3

Then $\left[\frac{1}{4}(p+1)\right] = \left[\frac{1}{4}(8k+4)\right] = 2k+1$

And if p = 8k – 3

Then $\left[\frac{1}{4}(p+1)\right] = \left[\frac{1}{4}(8k-3+1)\right]$

$$= \left[\frac{1}{4}(8k-2)\right] = 2k+1$$

Therefore in these two cases

$$\left(\frac{2}{p}\right) = -1$$

Therefore 2 is a quadratic non-residue.

Corollary:- For every odd prime p

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$$

Proof:- We know 2 is a quadratic residue of primes of the form 8k ± 1 & a quadratic non residue of primes of the form 8k ± 3.

Let p = 8k ± 1

Then $\frac{p^2-1}{8} = \frac{(8k\mp1)^2-1}{8} = \frac{64k^2\mp16k+1-1}{8}$

$= 8k^2 \mp 2k$

= an even number

$\Rightarrow \quad (-1)^{\frac{p^2-1}{8}} = 1 = \left(\frac{2}{p}\right)$

Let p = 8k ± 3

Then $\frac{p^2-1}{8} = \frac{(8k\mp3)^2-1}{8}$

$= \frac{64k^2\mp48k+9-1}{8}$

$$= \frac{64k^2 \mp 48k + 8}{8}$$

$$= 8k^2 \mp 6k + 1$$

= An odd number

Therefore $(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$

Thus in all cases

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

5.5 Quadratic Law of Reciprocity:-

For Legendre Symbols

Statement:- Let p & q be distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{p'q'}$$

Where $p' = \frac{p-1}{2}, \quad q' = \frac{q-1}{2}$

Alternative statements: -

(i) Let p or q be a prime of the form 4k + 1. Then either p' is even or q'

is even

$\Rightarrow$ p'q' is even

$\therefore$ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \Longrightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(ii) If both p & q are of the form 4k + 3 then both p' & q' are odd

Therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$

$\Rightarrow$ $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

So sometimes quadratic law of reciprocity is also asked in the following form.

Theorem: Let p & q be two distinct odd primes. Then

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if either of p & q is of the form 4k + 1

And $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if both of p & q are of the form 4k + 3

Proof:- By Gauss's Lemma

$\left(\frac{p}{q}\right) = (-1)^v$

Where v is the number of integers x $\left(1 \leq x \leq \frac{p-1}{2}\right)$ such that

$$qx = py + r \text{ where } -\frac{p}{q} < r < 0$$

Since q > 0, x > 0 and r < 0

$\Rightarrow$ $(p\ y) > 0 \Rightarrow y \geq 1$

Further

$$P\ y = qx - r < \frac{p-1}{2}q + \frac{p}{2} < \frac{p}{2}(q+1)$$

$\Rightarrow$ $y < \frac{q+1}{2}$

$\Rightarrow$ $y \leq \frac{q-1}{2}$

Similarly, $\left(\frac{p}{q}\right) = (-1)^{\mu}$ where μ is the number of integers y$\left(1 \leq y \leq \frac{q-1}{2}\right)$

such that

$Py = qx + s$ where $-\frac{q}{2} < s < 0$

Therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+v}$ ..... (1)

Where μ + v is the number of pairs of integers (x, y) such that $1 \leq x \leq \frac{p-1}{2}$

$$1 \leq y \leq \frac{q-1}{2}$$

And $$-\frac{p}{2} < r = qx - py = -s < \frac{q}{2}$$

Note, let us consider the following sets of pairs of integers (x, y)

$$S = \left\{(x, y): 1 \leq x \leq \frac{p-1}{2}; 1 \leq y \leq \frac{q-1}{2}\right\}$$

$$S_1 = \left\{(x, y) \in S; qx - py \leq -\frac{p}{2}\right\}$$

$$S2 = \left\{(x, y) \in S; \frac{p}{2} < qx - py < \frac{q}{2}\right\}$$

$$S_1 = \left\{(x, y) \in S; qx - py \geq \frac{q}{2}\right\}$$

Then $\#(S) = \#(S_1) + \#(S_2) + \#(s'_1)$ …….. (II)

Consider a mapping θ from S defined by

$$\theta(x, y) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

Since $$1 \leq x \leq \frac{p+1}{2} \quad \& \quad 1 \leq y \leq \frac{q-1}{2}$$

⇒ $$1 \leq \frac{q+1}{2} - y \leq \frac{q-1}{2}$$

So that θ is a mapping from S to S. Now let (x, y) ∈ S_1

Then, by definition

$$\theta\,(x, y) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right) = (x', y')(say)$$

Now $qx' - py' = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right)$

$$= \frac{q}{2} - \frac{p}{2} - (qx - py)$$

$$\geq \frac{q}{2} - \frac{p}{2} - \left(-\frac{p}{2}\right) \qquad (\because (x, y) \in S_1)$$

$$= q/2$$

$$\Rightarrow \qquad (x', y') \in S_1'$$

This means

$$\#(S_1) \leq \#(S'_1) \qquad \text{…….. (III)}$$

Then $qx' - py' = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right)$

$$= \frac{q}{2} - \frac{p}{2} - (qx - py)$$

$$\geq \frac{q}{2} - \frac{p}{2} - \left(-\frac{q}{2}\right) \qquad (\because (x, y) \in S'_1)$$

=-p/2

⇒ $(x', y') \in S_1$

This means

$\#(S'_1) \leq \#(S_1)$ …….. (IV)

From (III) & (IV)

$\#(S_1) = \#(S'_1)$ …….. (V)

Therefore from (II) & (V) we get

$\#(S) \equiv \#(S_2) \pmod p$

But $\#(S) = p'.q'$

⇒ $\#(S_2) = \mu + v$

$= p'q' \pmod 2$

∴ From (I); $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{pq}$

Example: Evaluate $\left(\frac{202}{257}\right)$

Or Determine whether 202 is quadratic residue of 257 or not? Or Determine

$X^2 \equiv 202 \pmod{257}$ is solvable or not

Solution:- we have $202 = 2 \times 101$

$$\left(\frac{202}{257}\right) = \left(\frac{2}{257}\right)\left(\frac{101}{257}\right)$$

$\left(\frac{2}{257}\right) = 1$ since

$257 = 1 \pmod 8$

$$\therefore \quad \left(\frac{202}{257}\right) = \left(\frac{101}{257}\right) = \left(\frac{257}{101}\right)$$

$\left| \because \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\right.$

$$= \left(\frac{55}{101}\right)$$

$$= \left(\frac{5}{101}\right)\left(\frac{11}{101}\right)$$

But $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$

And $\left(\frac{11}{101}\right) = \left(\frac{101}{11}\right)$

By reciprocity law

$$= \left(\frac{2}{11}\right)$$

$$= -1$$

$$\therefore \quad \left(\frac{202}{257}\right) = -1$$

Alternative $\left(\frac{202}{257}\right) = \left(\frac{-55}{257}\right)$

$$= \left(\frac{-1}{257}\right)\left(\frac{5}{257}\right)\left(\frac{11}{257}\right)$$

$$\Rightarrow \quad \left(\frac{-1}{257}\right) = 1\left(\frac{5}{257}\right) = \left(\frac{257}{5}\right) - \left(\frac{2}{5}\right) = -1\left(\frac{11}{257}\right) = \left(\frac{257}{11}\right) = \left(\frac{4}{11}\right) = 1$$

$$\therefore \quad \left(\frac{202}{257}\right) = (1)(-1)(1) = -1$$

Example: Evaluate $\left(\frac{650}{401}\right) = \left(\frac{26}{401}\right)\left(\frac{25}{401}\right)$

$$= \left(\frac{25}{401}\right)\left(\frac{2}{401}\right)\left(\frac{13}{401}\right)$$

$$= \left(\frac{13}{401}\right)$$

$$= \left(\frac{401}{12}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$$

$$= \left(\frac{2}{11}\right) = -1$$

Theorem: If p is an odd prime & gcd (a, 2p) = 1

Then $\left(\frac{a}{p}\right) = (-1)^t$

Where $t = \sum_{j=1}^{p=1} \left[\frac{ja}{p}\right]$

Also $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof:- Let S = $\left[1, 2, \ldots., \frac{p-1}{2}\right]$

Let $r_1, \ldots.., r_\lambda$ and $r'_1, \ldots..r'_\mu$

Be the least positive remainders of the elements of the set aS, which are <p/2 and >p/2 respectively.

Then as shown in the proof of Gauss's Lemma

$r_1, \ldots\ldots r_\lambda, p - r'_1, \ldots..p - \mu$

are all distinct

Since $\lambda + \mu = \frac{p-1}{2}$. Therefore $r_1, \ldots\ldots r_\lambda$, $p - r'_1, \ldots.. p - _\mu$ are the integers

$1, 2, \ldots., \frac{p-1}{2}$ in some order so that

$$\sum_{j=1}^{\frac{p-1}{2}} j = r_1 + r_2 + \cdots \ldots + r_\lambda + \sum_{s=1}^{\mu} \left(p - r_j'\right)$$

$$= \mu p + \sum_{i=1}^{\lambda} r_1 - \sum_{j=1}^{\mu} r_j' \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(I)}$$

Further by definition of $r_1, \ldots.., r_\lambda$, $r'_1, \ldots..r'_\mu$

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} j \left[\frac{ja}{p}\right] + \sum_{i=1}^{\lambda} r_1 + \sum_{j=1}^{\mu} r_j' \qquad \ldots\ldots\ldots \text{(II)}$$

Subtracting (I) from (II), we get

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = pt + 2\sum_{j=1}^{\mu} r_j' - \mu p \text{ where } t = \sum_{j=1}^{\frac{p-1}{2}} j \left[\frac{ja}{p}\right] \ldots. \text{(III)}$$

But $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$

$$\therefore \qquad (a-1)\left[\frac{p^2-1}{8}\right] = p(t-\mu) + 2\sum_{j=1}^{\mu} r_j' \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(IV)}$$

Since g.c.d. (a, 2p) = 1

$\Rightarrow$ a is odd.

⇒ (a – 1) is even. Also $\frac{p^2-1}{8}$ is an integers as p is odd

∴ From (IV), we get

$t - \mu \equiv 0 \pmod 2$ as p is odd

⇒ $\mu \equiv t \ (mod\ 2)$

By Gauss's Lemma

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

Therefore $\left(\frac{a}{p}\right) = (-1)^{t}$

Now set a = 2 in (II) since for j = 1, 2, …, $\frac{p-1}{2}$

$\left[\frac{ij}{p}\right] = 0$ for all j ⇒ t = 0

∴ From (III); e get $\sum_{j=1}^{\frac{p-1}{2}} j + \mu p = 2\sum_{j=1}^{\mu} ij$

∴ $\sum_{j=1}^{\frac{p-1}{2}} j \equiv -\mu p \pmod 2$ 2\RHS ∴ 2\LHS

But p ≡ -1 (mod 2)

$\therefore \qquad \mu = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8} \pmod 2$

$\therefore$ By Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p^2-1}{2}}$$

The Jacobi Symbol: - Let Q > 1 be an odd integer and Q = $q_1, q_2, \ldots q_s$ its prime factorization where $q_1, q_2, \ldots, q_s$ are odd primes, not necessarily distinct.

Then the Jacobi symbol, denoted by $\left(\frac{P}{Q}\right)$, is defined as:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_i}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right) \ldots \ldots \left(\frac{P}{q_s}\right)$$

Where $\left(\frac{P}{j}\right)$ is the Legendre symbol.

Remark 1, If Q itself is an odd prime then the Jacob symbol and Legendre symbol are same

(2) If gcd (P,Q) > 1, then $\left(\frac{P}{Q}\right) = 0$

For, gcd(P, Q) > 1 $\Rightarrow q_i \mid p$ for some $(1 \leq i \leq j)$

The corresponding Legendre symbol $\left(\frac{P}{q_i}\right) = 0$ and hence $\left(\frac{P}{Q}\right) = 0$

(3) if gcd(P, Q) = 1, then $\left(\frac{P}{Q}\right) = \pm 1$

(4) If P is a quadratic residue mod Q, then P is a quadratic residue mod each prime qj dividing Q, so that $\left(\frac{P}{q_j}\right) = 1$ for each j and hence $\left(\frac{P}{Q}\right) = 1$. However $\left(\frac{P}{Q}\right) = 1$ does not imply that P is a quadratic residue of Q.

Theorem: Let Q and Q' be odd and positive, then

(1)$\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$

(2)$\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$

(3)If gcd (P, Q) = 1, then $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$

(4)If gcd (PP', QQ') = 1, then $\left(\frac{P^1P^2}{Q^1Q^2}\right) = \left(\frac{P'}{Q'}\right)$

(5)P' ≡ P (mod Q) ⇒ $\left(\frac{P'}{Q}\right) = \left(\frac{P}{Q}\right)$

Theorem (Eisenstein's lemma): Let p be an odd prime and let a be an odd integer with gcd(a, p) = 1. Then, (a/p) = $(-1)^{T(a,p)}$, where T (a, p) = $\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] and\ [x]$ is the largest integer (box) function.

Proof: Recall that the numbers $v_1, v_2, \ldots, v_m, p - u_1, p - u_2, \ldots, p - u_n$ in the proof of Theorem 1 were are all positive, distinct and less than or equal to $\frac{p-1}{2}$. Moreover, u_i's and v_j's were obtained as remainders when ka, for $1 \leq k \leq \frac{p-1}{2}$, was divided by p.

Also, by division algorithm, for each k, $1 \leq k \leq \frac{p-1}{2}$, we obtain integers q_k and t_k such that $ka = q_k p + t_k$ with $1 \leq t_k \leq p - 1$. Consequently $q_k = [q_k + t_k/p] = [ka/p]$. Thus, $ka = \left[\frac{ka}{p}\right] p + t_k$ with $1 \leq t_k \leq p - 1$. We further see that

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] p + \sum_{i=1}^{n} u_i + \sum_{j=1}^{n} v_j \qquad (3)$$

From the proof of Theorem 1, we also recall that the numbers $v_1, v_2, \ldots, v_m, p - u_1, p - u_2, \ldots, p - u_n$ were a re-arrangement of the numbers $1, 2, \ldots, \frac{p-1}{2}$. Hence

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{n}(p-u_i) + \sum_{j=1}^{m} v_j = pn + \sum_{j=1}^{m} v_j - \sum_{i=1}^{n} u_i$$

……(4)

Now, subtracting Equation (4) from Equation (3), we get

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] - n\right) + 2\sum_{i=1}^{n} u_i$$

(5)

But, we know that p_a_1 (mod 2) and hence Equation (5) gives $0 \equiv \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] - n$ (mod 2). Or equivalently, n = $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$ (mod 2). In other words, n and $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$ have the same parity and hence,

(a/p) = (-1)n = $(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]}$.

Example. Find (7/11).

Solution: (7/11) = $(-1)^{\sum_{k=1}^{\frac{11-1}{2}}\left[\frac{k7}{11}\right]}$ = $(-1)^{\left[\frac{11}{7}\right]+\left[\frac{2.7}{11}\right]+\left[\frac{3.7}{11}\right]+\left[\frac{4.7}{11}\right]+\left[\frac{5.7}{11}\right]}$ = $(-1)^{0+1+1+2+3} = -1$.

Example. Find (11/7).

Solution: $(7/11) = (-1)^{\sum_{k=1}^{\frac{7-1}{2}}\left[\frac{k11}{7}\right]} = (-1)^{\left[\frac{11}{7}\right]+\left[\frac{2.11}{7}\right]+\left[\frac{3.11}{7}\right]} = (-1)^{1+3+4} = 1$

Theorem: Let p be an odd prime and let a, k ∈ N such that gcd(a, p) = gcd(k, p) = 1. Then, (a/p) = 1, whenever the equation $x^2 - ay^2 = kp$ admits a solution.

Proof. Let (r, s) be a solution of $x^2 - ay^2 = kp$. Then, $r^2 - as^2 = kp$. Thus, $r^2 \equiv as^2 \pmod p$ and hence $r^2s^2p^{-4} \equiv as^2s^2p^{-4} \equiv a(s^{p-1})^2 \pmod p$. As gcd(k, p) = gcd(a, p) = 1, we have gcd(s, p) = 1 and hence, $s^{p-1} \equiv 1 \pmod p$. Therefore,

$$(rs^{p-2})^2 \equiv r^2s^2p^{-4} \equiv a(s^{p-1})^2 \equiv a \pmod p.$$

Thus, (a/p) = 1.

But converse of this result is not true. That is, we can find a prime p and integers a, k such that gcd(a, p) = gcd(k, p) = 1 and (a/p) = 1 but the equation $x^2 - ay^2 = kp$ has no solution. For example, take p = 7, a = 4 and k = 1. Then, it can be easily verified that gcd(a, p) = gcd(k, p) = 1 and (a/p) = 1 as (4/7) = 1. But, it can be checked (using modulo 4 congruence) that the equation $x^2 - 4y^2 = 7$ does not have any integer solution as $x^2 \equiv 0$ or $1 \pmod 4$.

Theorem: Let $p \equiv \pm 3 \pmod 8$ then, the equation $x^2 - 2y^2 = p$ has no solution.

Proof. If $x^2 - 2y^2 = p$ has a solution then, $x^2 \equiv 2y^2 \pmod p$ and hence $(2/p) = 1$. A contradiction to Theorem 3, where it has been shown $(2/p) = -1$ whenever $p \equiv \pm 3 \pmod 8$.

Theorem: Let p and 2p + 1 are odd primes. Then show that $(-1)^{\frac{p-1}{2}} 2$ is primitive root of 2p + 1.

Proof. Let q = 2p + 1. Since p is odd prime, hence $q \geq 7$ and $ord_q(2)$, $ord_q(-2) \in \{1, 2, p, 2p\}$ as $\phi(q) = 2p$. Further it is easy see that $ord_q(2)$, $ord_q(-2) \notin \{1, 2\}$ As if $ord_q(2) = 2$ or $ord_q(-2) = 2$, then $q|3$. Hence we have $ord_q(2), ord_q(-2) \in \{p, 2p\}$. Now it is sufficient to prove that $ord_q (-1)^{\frac{p-1}{2}} 2 \neq p$. We show this in the following two cases.

$p \equiv 1 \pmod 4$ In this case $q \equiv 3 \bmod 8$, $(-1)^{\frac{p-1}{2}} 2 = 2$ and $\left(\frac{2}{q}\right) = -1$. Or equivalently $2^p = -1$.

Hence

$$ord_q(2) = 2p = \emptyset(q).$$

p ≡ 3 (mod 4) In this case q ≡ 7 mod 8, $(-1)^{\frac{p-1}{2}}2 = -2$ and $\left(\frac{2}{q}\right) = 1$. Hence

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\frac{2}{q} = \left(\frac{-1}{q}\right) = -1$$

Hence $ord_q(-2) = 2p = \emptyset(q)$.

Theorem: There are infinite number of primes of the 8k − 1.

Proof: Let $p_1, p_2, \ldots, p_k$ be finite number of primes of the form 8k −1. Consider $P = (4p_1 p_2 \ldots p_k)^2 - 2$. Then it is easy to see that P is for the 16k − 2. Let p be any prime divisor of P. Then $(4p_1 p_2 \ldots p_k)^2 - 2$. (mod p) or equivalently $\left(\frac{2}{p}\right) = 1$. Hence p is of the form 8a + 1 or 8a – 1.

If every odd prime divisor of P is of the 8a + 1 then P is of the 16k + 2 as 2|P. Hence there exists a prime divisor q of P of the from 8a − 1. Which is different from $p_1, p_2, \ldots, p_k$.

5.6 Quadratic residues for prime-power moduli

Theorem: Let p be an odd prime, let $e \geq 1$, and let $a \in Z$. then $a \in Q_{p^e}$ if and only if $a \in Q_P$.

Proof: we know that there is a primitive root $g\ (mod\ p^e)$, so with $n = p^e$ we see that Q_{p^e} consists of the even powers of g. Now g, regarded as an element of $U_{p,}$ is also a primitive root (mod p),and with $n = p$, we know that $Q_{P.}$also consists of the even powers of g. Thus $a \in Q_{p^e}$ if and only if $a \in Q_{p^e}$ .this completes the proof.

Note: for odd primes p, we can find square roots in $U_{p^e}\ for\ e \geq 2$ by applying the iterative method to the polynomial $f(x) = x^2 - a$:we use a square root of a mod (p^i) to find the square roots mod (p^{i+1}). suppose that $a \in Q_{P,}$are r is a square root of a mod (p^i) for some $i \geq 1$; thus $r^2 \equiv a\ mod\ (p^i)$, say $r^2 \equiv a + p^i q$. If we put $s = r + p^i k$, where k is as yet unknown, then $s^2 = r^2 + 2rp^i k + p^{2i}k^2 \equiv a + (q + 2rk) mod\ (p^{i+1})$, Since $2i \geq i + 1$. Now $\gcd(2r, p) = 1$,

So we can choose k to satisfy the linear congruence $q + 2rk \equiv 0\ (mod\ p)$, giving $s^2 \equiv a(mod\ p^{i+1})$ as required. An element $a \in Q_{P^{i+1}}$ has just two square roots in $U_{P^{i+1}}$ for odd p, so these must be $\pm s$. It follows that if we have a square root for a in U_p, then we can iterate this process to find its square roots in U_{p^e} for all e.

Example: Let us take $a = 6$ and $p^e = 5^2$. in U_5 we have $a = 1 = 1^2$, so we can take $r = 1$ as a square root (mod 5). Then $r^2 = 1 = 6 + 5.(-1), so\ q = -1$ and we need to solve the linear congruence $-1 + 2k = 0(mod\ 5)$. this has solution $k \equiv 3\ (mod\ 5)$,

So we take $s = r + p^i k = 1 + 5.3 = 16$, and the square roots of 6 in Z_{5^2} are given by ± 16, or equivalently $\pm 9\ (mod\ 5^2)$. If we want the square root $(mod\ 5^2)$, with $r^2 = 81 = 6 + 5^2.3$,

$so\ q = 3$; Solving $3 + 18k = 0(mod\ 5)$ we have $k \equiv -1, so\ s = 9 + 5^2.(-1) = -16$, giving square roots $\pm 16\ (mod\ 5^3)$.

Theorem: Let a be an odd integer, then

(a) $a \in Q_2$;

(b) $a \in Q_4$ if and only if $a \equiv 1(mod\ 4)$;

(c) $if\ \ e \geq 3, then\ a \in Q_{2^e}$ if and only if $a \equiv 1(mod\ 8)$.

Proof: Part (a) and (b) are obvious: squaring the elements of $U_2 = \{1\} \subset Z_2$ and of $U_4 = \{1,3\} \subset Z_{4,}$ we see that $Q_2 = \{1\} and\ Q_4 = \{1\}$. for part (c) we use the theorem which states that the elements of U_{2^e} all have the form $\pm 5^i$ for some i; squaring, we see that the quadratic residues are the even powers

of 5. Since $5^2 \equiv 1(mod\ 8)$,these are all represented by integers $a \equiv 1(mod\ 8)$.

Now both the even powers of 5 and the elements $a \equiv 1(mod\ 8)$ account for exactly one quarter of the classes in Q_{2^e} ; since the first set is contained in the second, these two sets are equal.

Example: $\mathrm{Q}_8 = \{1\}, \mathrm{Q}_{16} = \{1,9\}, \mathrm{Q}_{32} = \{1,9,17,25\}$, and so on.

Note: One can find square roots in Q_{2^e} by adapting the iterative algorithm given earlier for odd prime-powers. Suppose that $a \in Q_{2^i}$ for some $i \geq 3$, say $r^2 = a + 2^i q$. If we put $s = r + 2^{i-1}k$, then $s^2 = r^2 + 2^i rk + 2^{2(i-1)}k^2 \equiv a + (q + rk)2^i (mod\ 2^{i+1})$,

$since\ 2(i-1) \geq i+1$. Now r is odd, so we can choose $k = 0\ or\ 1$ to make $q + rk$ even, giving $s^2 \equiv a(mod\ 2^{i+1})$. Thus s is a square root of a in$U_{2^{i+1}}$. There are four square roots of a in $U_{2^{i+1}}$, and these have the form $t = sx$, where $x = \pm 1\ or\ 2^i \pm 1$ is a square root of 1.

Since $a \equiv 1(mod\ 8)$, we can start with a square root $r = 1$ for a in U_{2^3}, and then by iterating this process we can find the square roots of a U_{2^e} for any e.

Example: Let us find the square roots of $a = 17(mod\ 2^5)$; these exist since $17 \equiv 1(mod\ 8)$. First we find a square root $(mod\ 2^4). Taking\ r = 1$ we have $r^2 = 1 = 17 + 2^3.(-2)$,

$so\ q = -2;\ taking\ k = 0\ makes\ q + rk = -2\ even, so\ s = r + 2^2k = 1$ is square root of $17(mod\ 2^4)$. Now we repeat this process, using $r = 1$ as a square root $(mod\ 2^4)$ to find a square root $s\ (mod\ 2^5)$. We have $r^2 = 1 = 17 + 2^4.(-1), so\ now\ q = -1; taking\ k = 1\ makes\ q + rk = 0\ even, so\ s = r + 2^3k = 9$ is a square root of $17(mod\ 2^5)$. The remaining square roots t are found by multiplying $s = 9\ by\ 2^4 \pm 1 = \pm 15$, so we have $\pm 7, \pm 9$ as the complete set of square roots of $17(mod\ 2^5)$.

5.7 Quadratic residues for arbitrary moduli:

Theorem: Let $n = n_1n_2n_3 \ldots\ldots\ldots n_k$, where the integers n_i are mutually coprime. Then $a \in Q_n$ if and only if $a \in Q_{n_i}$ for each i.

Proof: If $a \in Q_n$ then $a \equiv s^2(mod\ n)$ for some $s \in U_n$. Clearly $a \equiv s^2(mod\ n_i)$ for each i, with s coprime to n_i, so $a \in Q_{n_i}$. Conversely, if $a \in Q_{n_i}$ for each i then there exist elements $s_i \in Q_{n_i}$ such that $a \equiv$

$s_i{}^2 (mod\ n_i)$. By the Chinese Remainder Theorem there is an element $s \in Z_n$ such that $s \equiv s_i (mod\ n_i)$ for all $i. then\ s^2 \equiv s_i{}^2 (mod\ n_i)$ for all i, and hence $s^2 \equiv a (mod\ n)$ since the moduli n_i are coprime, so $a \in Q_n$.

We can now answer the question of whether $a \in Q_n$ for arbitrary moduli n:

Theorem: Let $a \in U_n$. Then $a \in Q_n$ if and only if

(a) $a \in Q_p$ for each odd prime p dividing n, and

(b) $a \equiv 1 (mod\ 4)$ if $2^2 | n, and\ a \equiv 1 (mod\ 8) if\ 2^3 | n.$

(Note the condition (b) is relevant only when n is divisible by 4; in all other cases we can ignore it.)

Proof: By Theorem above, $a \in Q_n$ if and only if $a \in Q_{P^e}$ for each prime power p^e in the factorization of n. For odd primes p this is equivalent to $a \in Q_{p,}$ by giving condition (a); for $p = 2$ it is equivalent to condition (b), by theorem.

Example: Let $n = 144 = 2^4 . 3^2$. An element $a \in U_{144}$ is a quadratic residue if and only if $a \in Q_3\ and\ a \equiv 1 (mod\ 8)$; since $Q_3 = \{1\} \subset Z_3$, this is equivalent to $a \equiv 1 (mod\ 24)$, so $Q_{144} = \{1,25,49,73,97,121\} \subset U_{144}$. any $a \in Q_{144}$ must have $N = 8$ square roots. To find these, we first find its four

square roots $(mod\ 2^4)$ and its two square roots $(mod\ 3^2)$ by the methods described earlier, and then we use the Chinese Remainder Theorem to covert each of these eight pairs of roots into a square root $(mod\ 144)$. For instance, let $a = 73; then\ a \equiv 9\ (mod\ 2^4)$, with square roots $s \equiv \pm 3, \pm 5\ (mod\ 2^4)$, and similarly $a \equiv 1(mod\ 3^2)$, with square roots $s \equiv \pm 1\ (mod\ 3^2)$; solving these eight pairs of simultaneous congruence's for s, we get the square roots $s \equiv \pm 19, \pm 35, \pm 37, \pm 53\ (mod\ 144)$.

5.8. Summary

We study the Gauss's Lemma is needed to prove the quadratic reciprocity theorem, that for odd primes p and q, (p/q) = (q/p) unless p ≡ q ≡ 3 (mod 4), in which case (p/q) = - (q/p), and it also asserts that the product of two primitive polynomials is primitive (a polynomial with integer coefficients is primitive if it has 1 as a greatest common divisor of its coefficients).

In this Unit, we have discussed the several applications of quadratic reciprocity:

▪ Defined and given examples Gauss's Lemma.

▪ Characterizing the primes p for which a is a quadratic residue modulo p.

▪ Characterizing primes dividing values of a quadratic polynomial.

▪ Quadratic residues for prime-power moduli and arbitrary moduli.

5.9. Terminal Questions

1.Using Gauss's lemma, find $\left(\frac{2}{p}\right) and \ \left(\frac{3}{p}\right)$.

2. Determine whether 112 is a quadratic residue or nonresidue modulo 675.

3. Evaluate (4661/9901).

4. Evaluate (24 /31).

5. Characterize all prime numbers $p > 11$ for which $x^2 \equiv 11(mod\ p)$ has a solution.

6. Find all prime numbers p for which $\left(\frac{5}{p}\right) = -1$.

7. Evaluate $\left(-\frac{42}{61}\right)$.

UNIT-6 Arithmetic Functions & Application

Structure

6.1. INTRODUCTION

This unit introduces the concept of functions such as $F(a)$ of that are defined for all positive integers a are called arithmetic functions. The Mobius Function is an arithmetic function of a natural number argument n with $\mu(1) = 1, \mu(n) = 0$ if n is divisible by the square of a prime number.

August Ferdinand Mobius (1790-1868) is perhaps most well known for the one-sided Mobius Strip and, can be seen in the important technique of Mobius Inversion, which utilizes the important Mobius Function, finally, we'll use Mobius Inversion to solve a problem concerning Euler's totient function.

6.2. Objectives

After studying this unit you should be able to

- To understand the Introduction to arithmetic functions.
- To understand the definition of Arithmetic functions and multiplicative functions.
- To understand the mobius function and mobius inversion formula.

- To understand the Properties of few well known multiplicative functions.
- To understand the definition of Perfect numbers.
- An arithmetic function takes positive integers as inputs and produces real or complex numbers as outputs.

6.3 Arithmetical Functions:

Definition: A function F(a) whose domain is a set of positive integers is called an arithmetical function, or a numerical function or a function of Number Theory.

e.g. F(a) = a, F(a) = sin a, F(a) = $\frac{1}{a+2}$ F(a) = e^{ia}, etc.

6.4 Multiplicative Functions:

Definition: "An arithmetical function F(a) is said to be multiplicative or factorable if for every pair of positive integers a and b where (a, b) = 1, we have F(ab) = F(a)F(b)"

We now describe some important number theoretic functions.

(1) The number of all positive divisors of a given number a. we denote this by the symbol T(a)

Let $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ be the canonical resolution of a as the product of powers of distinct primes p1 < p2 < ……pn. Then any divisor of the number a is of the form $d = p_1^{l_1} p_2^{l_2} \ldots\ldots\ldots p_k^{l_k}$ where for each i = 1, 2, …..n, we have $0 \leq l \leq \alpha$. Thus there are (α_i+1) choices for each l. ∴ The number of divisors d of a is the same as the number of distinct ways of choosing the set (l_1, l_2, …..l_n), subject to the above restrictions. But the number of these selections is obviously.

$(1 + \alpha_1)(1 + \alpha_2)\ldots\ldots\ldots\ldots(1 + \alpha_n)$.

∴ $T(a) = (1 + \alpha_1)(1 + \alpha_2)\ldots\ldots\ldots\ldots(1 + \alpha_n)$.

(2) The sum of all positive divisors of a given number a. We denote it by the symbol S(a).

Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ be the canonical prime power resolution of a. Then every term in the product.

P = (1 + p_1 + p_1^2 + …….$p_1^{\alpha^1}$) (1 + p_2 + p_2^2 + …….$p_2^{\alpha^2}$)…….. (1 + p_n + p_n^2 + …….$p_n^{\alpha^x}$) is of the form d = $p_1^l, p_2^{l_2}$ … … …. . $p_n^{l_n}$ where $0 \leq l_i \leq \alpha_i$ for each I = 1, 2, ….., n.

But the numbers such as d exhaust all the divisors of a when the indices l, and the suffixed I are given the full range of variation, already specified. And this is provided for in the product P. ∴ P represents the sum S(a).

Thus S(a) = $\left(\frac{p_1^{\alpha_1+1}}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}}{p_2-1}\right)$ … … …. $\left(\frac{p_n^{\alpha_n+1}}{p_n-1}\right)$

After summing up each geometric progression in the expression for p.

Example: (1) Find T(768).

Solution: Now 768 = 2^8.31

∴ T (768) = (1 + 8)(1 + 1) = 9 x 2 = 18

Example: (2) Find S(960).

Solution: Now 960 = $2^6.3^1.5^1$

∴ S (960) = $\frac{2^7-1}{2-1}.\frac{3^2-1}{3-1}.\frac{5^2-1}{5-1} = \frac{127}{1}.\frac{8}{2}.\frac{24}{4} = 3048$

It is easy to prove that both T(a) and S(a) are multiplicative functions, for (a, b) = 1 where a =$p_1^{\alpha_1}p_2^{\alpha_2}$ … … …. $p_k^{\alpha_k}$ and b = $q_1^{\beta_1}q_2^{\beta_2}$ … … …. $q_k^{\beta_k}$.

Where none of the q's is a p. then the product ab =

$p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k} . q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots\ldots q_t^{\beta_t}$, we find that all the primes are distinct. Hence we find

(I) $T(ab) = (1 + \alpha_1)\ldots\ldots\ldots(1 + \alpha_k)(1 + \beta_1)\ldots\ldots(1 + \beta_t) = T(a.T(b)$

(II) $S(ab) = \left(\frac{p_1^{\alpha_1+1}}{p_1-1}\right) \ldots\ldots\ldots \left(\frac{p_k^{\alpha q+1}}{p_1-1}\right)\left(\frac{q_1^{\beta_1+1}}{q_1-1}\right) \ldots\ldots \left(\frac{q_t^{\beta_t+1}}{q_t-1}\right)$

We shall now prove some general results concerning multiplicative functions.

Theorem 1: If θ is a multiplicative function, then (θ, 1) = 1

Proof:- We have θ(a.b) = θ(a).θ(b) whenever (a, b) = 1

Let a be such that θ(a) ≥ 0 $\quad \therefore \theta(a.1) = \theta(a).\theta(1)$

i.e. θ(a) = θ(a).θ(1) $\quad \therefore \theta(1) = 1, \because \theta(a) \neq 0$

Theorem 2: Let θ_1 and θ_2 be two multiplicative functions, and define $\theta = \theta_1\theta_2$ as $\theta_1\theta_2(x) = \theta_1(x).\theta_2(x)$ for all positive integers x. Then θ is also multiplicative.

Proof.:- $\theta(ab) = \theta_1\theta_2(ab) = \theta_1(ab).\theta_2(ab)$, for all a, b.

If now (a, b) = 1, since θ_1, and θ_2 are multiplicative, we get

$\theta(ab) = \theta_1(a).\theta_2(b) = \theta_2(a).\theta_2(b),$

$= \theta_1(a).\theta(b) = \theta_1(b).\theta_2(b),$

$= \theta_1\theta_2(a).\ \theta_1\theta_2(b)$

$= \theta(a).\theta(b)$

Theorem 3: Let θ(a) be a multiplicative function, and let a = $p_1^{\alpha_1}p_2^{\alpha_2}$ ... ... $p_k^{\alpha_k}$ be the canonical prime power resolution of a. Then, denoting by the symbol d/a summation extended over all the positive divisors of a, we have the formula,

$$\sum_{d/a} \theta(d) = \left\{1 + \theta(p_1) + \theta(p_1^2) + \cdots \ldots \ldots \ldots . \theta\left(p_1^{\alpha_1}\right)\right\}$$

$$\times \left\{1 + \theta(p_2) + \theta(p_2^2) + \cdots \ldots \ldots \ldots . \theta\left(p_2^{\alpha_2}\right)\right\}$$

……

$$\times \left\{1 + \theta(p_k) + \theta(p_k^2) + \cdots \ldots \ldots \ldots . \theta\left(p_k^{\alpha_k}\right)\right\}$$

Proof:- Any term in the product on the right side is of the form $\theta(p_1^{l1}) + \theta(p_2^{l2}) + \cdots \ldots \ldots \ldots . \theta\left(p_k^{lk}\right)$ where for each i = 1, 2, ……k, $0 \leq t_i \leq \alpha_i$.

But $\theta(p_1^{l1}) + \theta(p_2^{l2}) + \cdots \ldots \ldots \ldots . \theta\left(p_k^{lk}\right).\theta\left(p_1^{l1}.p_2^{l2} \ldots . p_k^{lk}\right)$

Here $p_1^{l1}.p_2^{l2}\ldots.p_k^{lk}$ is any divisor of a and when the powers and suffixes are given the full range of variation already specified, these numbers exhaust all the divisors of a.

∴ R.H.S. of the given formula $\sum_{d/a}\theta(d)$.

Corollory 1: Taking θ(d) = d, for all d, we find that

$\sum_{d/a}\theta(d)$ = the sum of the sth powers of all the divisors of a

$$= (1 + p_1^{s1} + p_2^{s2} + \cdots . + p_k^{a1s}) \ldots\ldots\ldots (1 + p_k^s + p_c^{s2} + \cdots . + p_k^{aks})$$

$$= \left(\frac{(p_1^s)^{\alpha_1+1}-1}{(p_1^s-1)}\right)\left(\frac{(p_2^s)^{\alpha_2+1}-1}{(p_2^s-1)}\right) \ldots\ldots\ldots \left(\frac{(p_k^s)^{\alpha_k+1}-1}{(p_k^s-1)}\right)$$

Corollory 2: The case s = 1 gives the expression for S(a), already determined.

6.5 Properties of Multiplicative Function:

A Multiplicative Function is completely determined by its values at the powers of prime numbers, a consequence of the fundamental of arithmetic. Thus, if n is product of powers of distinct primes, say $n = p^a q^b \ldots$,

Then $f(n) = f(p^a)f(q^b)$ ....this property of multiplicative functions significantly reduces the need for computation, as in the following examples for $n = 144 = 2^4 3^2$

6.6 The Mobius Function:

The number theoretic function μ(a), the Mobius function, is defined by the equations:

$$\mu(a) = \begin{cases} 1 \; for \; a = 1 \\ (-1) \; if \; a \; is \; the \; product \; r \; different \; primes, \\ 0 \; if \; a \; is \; divisible \; by \; the \; square \; of \; a \; prime \end{cases}$$

Thus we have

μ(1) = 1	μ(5) = -1	μ(9) = 0
μ(2) = -1	μ(6) = 1	μ(10) = 1
μ(3) = -1	μ(7) = -1	μ(11) = -1
μ(4) = 0	μ(8) = 0	μ(12) = 0
		etc

In fact for any prime p, μ(p) = -1

Theorem 5: μ(a) is a multiplicative function.

Proof:- (1) If at least one of a and b is not square free i.e. divisible by the square 0 at least one prime, than ab is not square free ∴ μ(ab) = 0 and one at least of μ(a) and μ(b) = 0

∴ μ(ab) = μ(a) μ(b)

(2) If a is the product of r distinct primes, and b that of s other distinct primes, then as is the product of r + s distinct primes.

∴ $\mu(ab) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(a).\ \mu(b)$

Theorem 6: Let θ(a) be a multiplicative function, and let $p_1^{\alpha_1}p_2^{\alpha_2}$ ... ... $p_k^{\alpha_k}$ be the canonical prime power resolution of the number a, then

$\sum_{d/a}\mu(d)\theta(d) = [1-\theta p_1]$ ... ... $[1-\theta p_k]$ if a > 1

= 1 ..... If a = 1

Proof:- Putting $\psi(x) = \mu(x).\theta(x), \forall x$, we see that on using theorem 2.12

$$\sum_{d/a}\psi(d) = [1+\psi(p_1)+\psi(p_1^2)+\cdots \dots \dots \dots \dots +\psi(p_1^{\alpha_1})]$$

$$\times [1+\psi(p_2)+\psi(p_2^2)+\cdots \dots \dots \dots \dots +\psi(p_2^{\alpha_2})]$$

$$\times [1+\psi(p_k)+\psi(p_k^2)+\cdots \dots \dots \dots \dots +\psi(p_k^{\alpha_k})]$$

But $\psi(p) = \mu(p).\theta(p)$ = (-1)θ(p) = -θ(p)

And $\psi(p') = \mu(p').\theta(p') = 0$ for s > 1

$\therefore \quad \sum_{d/a} \mu(d)\theta(d) = [1 - \theta p_1] \dots \dots \dots [1 - \theta p_k]$ if a > 1. While

= 1, if a = 1

Corollary 1. In particular, taking θ(a) = 1, ∀ a, we get,

$$\sum_{d/a} \mu(d) = \begin{cases} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \dots \dots \dots \left(1 - \frac{1}{p_k}\right), & if\ a > 1 \\ 1, & if\ a = 1 \end{cases}$$

Corollary 2. Taking θ(x) = $\frac{1}{x}$ ∀ x, we get

$$\sum_{d/a} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \dots \dots \dots \left(1 - \frac{1}{p_k}\right), & if\ a > 1 \\ 1, & if\ a = 1 \end{cases}$$

6.7 Properties of Mobius Function:

If $n \geq 1$, then $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, if\ n = 1 \\ 0, if\ n > 1 \end{cases}$

Where d runs over positive divisor of n, $\mu(1) = 1$

Consider $n = 12$, the positive divisors of $n = 12$ are {1,2,3,4, ,12}.

$$then \sum_{d/n} \mu(d) = \left[\frac{1}{n}\right]$$

$$\sum_{\frac{d}{12}} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$

$$\sum_{\frac{d}{12}} \mu(d) = 1 - 1 - 1 + 0 + 1 + 0 = 0$$

$$\sum_{\frac{d}{12}} \mu(d) = 0, n = 12 > 1.$$

6.8 Mobius inversion formula:

Result obtained is the following theorem is known as Mobius inversion formula.

Theorem 7: Let F(a) be any number theoretic function and define the number theoretic function G(a) as

$G(a) = \sum_{d/a} F(d)$

Then $F(a) = \sum_{d/a} \mu(d)\, G\left(\frac{a}{d}\right)$ which is called the Mobius inversion formula.

Proof:- For every positive divisor d of a.

$$G\left(\frac{a}{d}\right) = \sum_{b/\left(\frac{a}{d}\right)} F(b)$$

$\therefore \quad \mu(d)G\left(\frac{a}{d}\right) = \mu(d)\sum_{\frac{b}{\left(\frac{a}{d}\right)}} F(b) = \sum_{b/\left(\frac{a}{d}\right)} \mu(d)F(b)$

$\therefore \quad \sum_{d/a} \mu(d)\, G\left(\frac{a}{d}\right) = \sum_{d/a}\sum_{b/\left(\frac{a}{d}\right)} \mu(d)F(b) = \sum_{b/a}\sum_{b/\left(\frac{a}{d}\right)} \mu(d)F(b)$

$= \sum_{b/a} F(b)\sum_{\frac{b}{\left(\frac{a}{b}\right)}} \mu(d) = F(a)$ for

$$\sum_{\frac{b}{\left(\frac{a}{b}\right)}} \mu(d) = \begin{cases} 1, if\ \frac{a}{b} = 1 \quad i.e..a = b \\ 0 \quad if \frac{b}{a}\ and\ b < a \end{cases}$$

6.9 Application of Mobius Inversion:

There are two main uses Mobius Inversion, the first is that we can just apply the formula to immediately obtain identities which might be difficult to obtain directly.

1. By definition $\sigma(n) = \hat{n} = \sum_{d/n} d$

Mobius Inversion gives that $n = \sum_{\frac{d}{n}} \mu\left(\frac{n}{d}\right)\sigma(d)$

2. By definition $\tau(n) = \widehat{1(n)} = \sum_{d/n} 1$

Mobius Inversion gives that $1 = \sum_{\frac{d}{n}} \mu\left(\frac{n}{d}\right)\tau(d)$

Euler's ∅ Function or the totient

The number theoretic function ∅(a) called the Euler's Function, is defined as the number of positive integers less than a and relatively prime to a.

Example:- ∅(1) = 1 ∅(5) = 4

∅(2) = 1 ∅(6) = 2

∅(3) = 2 in general, if p is a prime

∅(4) = 2 ∅(p) = p – 1

Theorem 4.16. For any positive integer a, we have $\sum_{d/a} \emptyset(d) = a$

Leema: If F(x) is any number theoretic function then $\sum_{d/a} F(d) = \sum_{d/a} \emptyset(\frac{a}{d})$, for if d is a divisor of a, then b = $\frac{a}{d}$ is the complementary divisor of a. ∴ if d runs over the set of all divisors of a, then b also runs over the same set. Thus $\sum_{d/a} F(d) = \sum_{d/a} \emptyset(\frac{a}{d})$.

Proof of the theorem. Let $d_1 < d_2 < \ldots\ldots < d_s$, be all the positive divisors of a. Any d, is such that $(d, a) = d_i$, for all i = 1, 2, …..s Let $C_i = \{x \mid 0 < x \leq a_i, (x, a) = d_i\}$

Thus for an $x \in C_i$, $x = k_i d_i$ where $\left(k_i, \frac{a}{d_i}\right) = 1$.

∴ Ci has as many elements as there are ki such that $0 < k_i d_i \leq a$, and $\left(k_i, \frac{a}{d_i}\right) = 1$ ∴ $k_i \leq \frac{a}{d_i}$ and relatively prime to $\frac{a}{d_i}$. ∴ number of elements in $C_i = \emptyset\left(\frac{a}{d_i}\right)$.

If y ∈ {1, 2, 3, ….., a} then (y, a) will be one and only one of the s divisors $d_1, d_2, \ldots\ldots d_s$ of a.

∴ The classes $C_1, C_2, \ldots..C_i$ form a partition of the set S = (1, 2, 3, ……, a).

∴ if $o(C_i)$ = the number of elements in C_i,

We have $\sum_{i=1}^{s} \emptyset\left(\frac{a}{d_i}\right) = o(S)$.

∴ $\sum_{i=1}^{s} \emptyset\left(\frac{a}{d_i}\right) = \sum_{i=1}^{s} \emptyset\left(\frac{a}{d}\right) = a$

∴ $\sum_{d/a} \emptyset(d) = a$, using the lemma.

e.g. Taking a = 12 its divisors are 1, 2, 3, 4, 6, and 12.

$$\emptyset(1) + \emptyset(2) + \emptyset(3) + \emptyset(4) + \emptyset(6) + \emptyset(12) = 1 + 1 + 2 + 2 + 2 + 4$$

$$= 12$$

Theorem 4.17: If the canonical decomposition of the number a is

$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$, then

$$\emptyset(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots\ldots\left(1 - \frac{1}{p_k}\right)$$

Proof: We have Mobius inversion formula, that if

G(d) = $\sum_{d/a} F(d)$. Then F(a) =$\sum_{d/a} \mu(d) G\left(\frac{a}{d}\right)$

By taking F(x) = $\emptyset$(x), we find that

G(a) = $\sum_{d/a} \mu(d) = a$. Using theorem $\therefore G\left(\frac{a}{d}\right) = \frac{a}{d}$

$\therefore \quad \emptyset(a) = \sum_{d/a} \mu(d) \frac{a}{d} = \sum_{d/a} \frac{\mu(d)}{d}$

$= a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots\ldots\left(1 - \frac{1}{p_k}\right)$ on using theorem 4.14

Theorem 4.18 $\emptyset$(x) is a multiplicative function

Proof:- Let (a, b) = 1, a > 0, b > 0. Then, if a = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ and b = $q_1^{\beta} q_2^{\beta_2} \ldots\ldots\ldots q_t^{\beta_t}$, the p's and q's are (k + t) distinct primes, and

$\therefore$ ab = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k} . q_1^{\beta} q_2^{\beta_2} \ldots\ldots\ldots q_t^{\beta_t}$ is the complete resolution of ab into the product of powers of distinct primes.

$$\emptyset(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots\ldots\left(1 - \frac{1}{p_k}\right)$$

$$\emptyset(b) = b\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \ldots\ldots\ldots\ldots\left(1 - \frac{1}{q_t}\right)$$

And $\emptyset(ab) = ab\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\ldots\ldots\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots\ldots\ldots\ldots\left(1-\frac{1}{q_t}\right)$

$$= \left\{a\left(1-\frac{1}{p_1}\right)\ldots\ldots\ldots\ldots\left(1-\frac{1}{p_k}\right)\right\}\left\{b\left(1-\frac{1}{q_1}\right)\ldots\ldots\ldots\ldots\left(1-\frac{1}{q_t}\right)\right\}$$

$$\emptyset(ab) = \emptyset(a).\emptyset(b)$$

An alternative method of obtaining the formula for $\emptyset(a)$ will be described in pervious unit.

Example 1: Let k be a positive even number, and the canonical decomposition of a is of the form $a = p_1p_2\ldots..p_k$; let dt run through the divisions of the number a, such that $0 < d1 < a$ prove that $\sum_{d_1}\mu(d_1) = 0$

Solution: [Hints: Let d_1 be a divisor of a, where $0 < d_1 < \sqrt{a}$

Then if $a = d_1d_2$, d_2 is a divisor of a where $d_2 > \sqrt{a}$

Now $\mu(a) = \mu(d_1d_2) \therefore (-1)^k = \mu(d_1)\mu(d_2)$, where k is even

$\therefore \mu(d1) = \mu(d2) \quad \therefore 2\sum_{d_1}\mu(d_1) = \sum_{d_1}\mu(d_1) + \sum_{d_2}\mu(d_2) =$

$\sum_{d/a}\mu(d_1) = 0$

Example 2: Find for what values of m, does $\emptyset(m)/m$.

For what value of n is (1) $\emptyset(n)$ odd? (2) $\emptyset(n) = \frac{n}{2}$?

Solution: [$\emptyset(n)$ is even for all n ≥ 3. As can be seen from its value $n\left(1-\frac{1}{p_1}\right)\ldots.\left(1-\frac{1}{p_k}\right)$ let m = 2^t, $p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ldots\ldots.p_k^{\alpha_k}$, where p_1, p_2, ……p_k, are distinct odd primes.

Then $\emptyset(m)$ = m$\left(1-\frac{1}{2}\right)\left(!\,1-\frac{1}{p_1}\right)\ldots.\left(1-\frac{1}{p_k}\right) = \frac{m}{2} \Rightarrow \left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_1}\right)\ldots.\left(1-\frac{1}{p_k}\right) = \frac{1}{2}$ which is the case only when m = 2. So that α_1 = …… = α_k = 0.1

Example 3: If f(n) is a multiplicative function, and $F(n) = \sum_{d/n} f(d)$, prove that F(n) is multiplicative.

Solution: [Let (a, b) = 1, and then we have

F(ab) = $\sum_{d/ab} f(d) = \sum_{\frac{d_1}{a},\frac{d_2}{b}} f(d_1 d_2) = \sum_{\frac{d_1}{a},\frac{d_2}{b}} f(d_1)f(d_2)$

i. $= \sum_{\frac{d_1}{a}} f(d_1).\sum_{\frac{d_2}{a}} f(d_2) = F(a).F(b).]$

Example:4 Verify Mobius Inversion formula for $n = 24$

Solution: We know that Mobius Inversion formula states that for any two arithmetic functions F and f and $F(n) = \sum_{\frac{d}{n}} f(d)$,

$$then\ f(n) = \sum_{d/n} \mu(d) F(\frac{n}{d}) = \sum_{d/24} \mu(d) F(\frac{24}{d})$$

$$= \mu(1)\mathrm{F}(24) + \mu(2)\mathrm{F}(12) + \mu(3)\mathrm{F}(8) + \mu(4)\mathrm{F}(6) + \mu(6)\mathrm{F}(4) + \mu(8)\mathrm{F}(3)$$

$$+ \mu(12)\mathrm{F}(2) + \mu(24)\mathrm{F}(1)$$

$$= F(24) - F(12) - F(8) + F(4)$$

$$= \sum_{d/24} f(d) - \sum_{\frac{d}{12}} f(d) - \sum_{\frac{d}{8}} f(d) + \sum_{d/4} f(d)$$

$$= [f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)]$$

$$- [f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12)]$$

$$- [f(1) + f(2) + f(3) + f(4) + f(6) + f(8)]$$

$$+ [f(1) + f(2) + f(3) + f(4)]$$

$$= f(24)$$

$$\sum_{d/24} \mu(d) F(\frac{24}{d}) = f(n)$$

6.11 Summary:

A simple but very beautiful concept in number theory is that of an arithmetic function. An arithmetic function is just a sequence of real or complex numbers. Arithmetic functions have applications in number theory, combinatorics, counting, probability theory, and analysis, in which they arise as the coefficients of power series.

In this unit we have covered the following points.

1) The definition of Arithmetic Functions.
2) The definition of Multiplication Functions and their Properties.
3) The definition of Mobius Function and their Properties.
4) The definition of Mobius Inversion Formula and its Examples.

6.12 Terminal Questions

1. Evaluate T(a), S(a), μ(a) and ∅(a) for each of the numbers a = 1024, 1025, 1026

2. Show that the sum of positive integers less than the positive integer n and relatively prime to it is $\frac{1}{2}n\emptyset(n)$.

3. A number a is said to be a perfect number if S(a) = 2a. Verify that 6, 28, 496, 8128 are perfect.

4. Show that $2^{n-1}(2^n-1)$ is perfect if $2^n - 1$ is a prime. This is Euclid's theorem concerning even perfect numbers: Whether any odd perfect number exists is not yet known.

5. A number n is said to be a perfect number of multiplicity k if S (n) = k_n, where k ≥ 3. Show that 120 and 672 are multiplicative perfect, and find their multiplicities.

6. If t is the number, and p the product of all the divisors of a number A show that $p^2 = A^t$

7. In the notation of Ex. 6 if A^2 = P. Prove that A is the product of two primes or the cube of a prime.

8. Prove that there is an infinity of primes of the form (6n - 1).

9. If a and b are natural numbers, prove that $\emptyset(ab)\emptyset(d) = d\emptyset(a).\emptyset(b)$ where d = (a, b).

10. For all m, prove that $\emptyset(m^2) = m\emptyset(m)$

11. Let k be a positive integer, and let d run through the positive integers such that $\emptyset(d) = k$. Prove that $\sum \mu(d) = 0$

[Pair all square free numbers into pairs (x, y) such that x is an odd number d_1 and y is the even number $2d_1$. Now $\mu(2d_1) = -\mu(d_1)$.

$\therefore \mu(d_1) + \mu(2d_1)=0 \quad \therefore \mu(d) = \sum \mu(d_1) + \sum \mu(d_1) = \sum[\mu(d_1) + \mu(d_1)] = 0$

12. Show that the number of positive fractions in lowest terms between 0 and 1 and whose denominators do not exceed n is $\emptyset(2) + \emptyset(3) + \cdots .. + \emptyset(n)$.

[for each integer k < n, the various fractions in lowest terms which lie in (0, 1) are $\frac{k_1}{n}$, $\frac{k_2}{n}$ … … … … … $\frac{k_{\emptyset(k)}}{n}$. $\therefore$ their number is $\emptyset(k)$.]

(b) Prove that $\sum_{d/p^n} \emptyset(d) = p^n$ for any prime p, and natural number n.

(c) Use (a) and (b) to prove $\sum_{d/n} \emptyset(d) = n$.

13. Find the value of Mobius function $\mu(n)$ for n

(i) 15 (ii) 30 (iii) 47 (iv) 100