UNIT 7: NUMBER THEORETIC FUNCTIONS-I

UNIT STRUCTURE

7.1 Learning Objective
7.2 Introduction
7.3 The function ζ and σ : Definitions and Example
7.4 Properties of ζ and σ functions
7.5 Euler's ϕ function : Definition and Example
7.6 Properties of Euler's ϕ function
7.7 The Mobius function: Definition and Example
7.8 Properties of Mobius function
7.9 The Greatest integer function : Definition and Example
7.10 Some Properties of greatest integer function
7.11 Let Us Sum Up
7.12 Answers to check your progress
7.13 Further Reading
7.14 Model Questions

7.1 LEARNING OBJECTIVE

After reading this unit learner will gain ability to

- define and analyze key withmetic functions such as the divisor function, Euler's ϕ-function, greatest integer function and Mobius function,
- compute values of number theoretic functions and apply their properties in problem- solving.
- explore concepts like multiplicative functions and their role in simplifying complex arithmetic expressions.

7.2 INTRODUCTION

Number theoretic functions, also known as arithmetic functions, are fundamental tools in number theory that assign values to positive integers based on specific arithmetic properties. These functions are widely used to analyze the structure and behaviour of integers, particularly in relation to divisibility, prime factorization and other number-theoretic operations. They serve as the building blocks for many results and applications in pure and applied mathematics, including cryptography, digital security and algorithm design.

A number theoretic function is typically defined as a function $f:\mathbb{N}\to\mathbb{C}$ where $\mathbb{N}$ is the set of positive integers and $\mathbb{C}$ is the set of complex numbers. In most cases, the

function values are real or integer-valued. The study of these functions reveals deep properties about the distribution and relationships among integers. Some of the most commonly studied number theoretic functions are divisor function ζ (n), sum of divisors function σ (n),Euler's ϕ-function and Mobius function μ (n). These functions can be classified as multiplicative or completely multiplicative. A function f (n) is multiplicative if f (ab) = f(a) f(b) whenever a and b are coprime. For instance both ϕ (n) and μ (n) are multiplicative functions.

The properties of number theoretic functions often reflect deeper mathematical patterns and used to derive powerful results such as Chinese Remainder Theorem, Fermat's Little Theorem and Euler's Theorem. Additionally, they play a crucial role in understanding the distribution of prime numbers and in algorithms for primality testing and integer factorization.

7.3 THE FUNCTION ζ AND σ : DEFINITIONS AND EXAMPLE

Definition 7.3.1 Given a positive integer n. Lot ζ (n) denoted the number of positive divisor of n and σ (n) denote the sum of these divisors is $\zeta : \mathbb{N} \to \mathbb{N}$ is a function such that

$$\zeta(n) \Rightarrow \sum_{\substack{d \mid n \\ d \geq 1}} d$$

Example 1 : Find ζ (15), ζ (20, σ (15) and σ (20).

Solution : The divisors of 15 are 1, 3, 5, 15

Therefore ζ (15) = 4 and σ (15) = 1 + 3 + 5 + 15

= 24

The divisors of 20 are 1, 2, 4, 5, 10, 20

Therefore ζ (20) = 6 and σ (20) = 1 + 2 + 4 + 5 + 10 + 20

= 42

Example 2. Find ζ (36) and σ (36)

Solution : The divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36

Therefore ζ (36)

and σ (36) = 1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 + 36

= 91

Example 3. If p is a prime, then find ζ (p) and σ (p)

Solution : Since the prime number p has only two factors 1 and p itself, therefore,

ζ (2) = and σ (p) = 1 + p

7.4 Properties of ζ and σ functions

Lemma 7.4.1. If $n = p_1^{k1}.p_2^{k2}.....p_r^{kr}$ is the prime factorization of n>1, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a1}\ p_2^{a2}.....p_r^{ar}$$

Proof : Since d = 1 is a factor of $n = p_1^{k1}.p_2^{k2}.....p_r^{kr}$ and we can write $1 = p_1^0.\ p_2^0.....p_r^0$. Suppose that d divides n nontrivially; say, n = dd', where d>1, d'>1. Express both d and d' as product of (not necessarily distinct) prime :

$$d = q_1.q_2.....q_s,\quad d' = t_1.t_2.....t_u$$

Then $n = p_1^{k1}.p_2^{k2}.....p_r^{kr} = q_1.q_2.....q_s,\quad d'.\ t_1.t_2.....t_u$ are two prime factorizations of the positive integer n. By uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1.q_2.....q_s = p_1^{a1}\ p_2^{a2}.....p_r^{ar}$$

when the possibility that $a_i = 0$ is allowed.

Conversely, every $d = p_1^{a1}\ p_2^{a2}.....p_r^{ar}\ \ (p \le a_i \le k_i)$ turns out to be a divisor of n. Then we can write

$$n = p_1^{k1}.p_2^{k2}.....p_r^{kr}$$

$$\left(p_1^{a1}\ p_2^{a2}.....p_r^{ar}\right)\left(p_1^{k1-a1}.p_2^{k2-a2}.....p_r^{kr-ar}\right)$$

$$= dd'$$

with $d' = p_1^{k1-a1}.p_2^{k2-a2}.....p_r^{kr-ar}$ and $k_i \ge a_i \ge 0$ for each i. Then d'> 0 and d|n.

Theorem 7.4.2. If $n = p_1^{s1}.p_2^{s2}.....p_r^{sr}$, where the Pi's are distinct primes and $s_i \geq 1$ are integers, then for each $r \geq 1$ the following holds.

(i) $\zeta(n) = (s_1 + 1)(s_2 + 1).....(s_r + 1)$

(ii) $\sigma(n) = \frac{p_1^{s1+1} - 1}{p_1 - 1}.\frac{p_2^{s2+1} - 1}{p_2 - 1}.....\frac{p_r^{sr+1} - 1}{p_r - 1}$

Proof : The proof is done by induction on r. Let r = 1. Then $n = p^s$ for $s \geq 1$. The positive divisor of n are 1, p, p^2, p^3, ….. p^s are i.e. (s + 1) in number. Therefore

$$\zeta(n) = s + 1$$

and $$\sigma(n) = 1 + p + p^2 + ... + p^s$$

$$= \frac{p^{s+1} - 1}{p - 1}$$

Therefore, the result is true for r = 1. We assume the result is true for n' which has r – 1 distinct prime factors (r > 2). Let n > 1 be an integer which has r distinct prime factors. Let

$n = p_1^{s1}.p_2^{s2}.....p_r^{sr}$, where P's are distinct prime factors and $s_i \geq 1$ are integers. Let

$$n' = p_1^{s1}.p_2^{s2}.....p_{r-1}^{sr-1}$$

Also $(n' = n'.p_r^{sr}) = 1$ because the P_i's are distinct primes. Since any divisor of n' is a divisor of n, therefore any divisor of n is of the form $d'p_r^k$ where $0 \leq k \leq s_r$, $d' \geq 1$ and d'|n' . Thus

$$\zeta(n) = \sum_{\substack{d'|n' \\ d' \geq 1}} 1 + \sum_{d'p_r|n} 1 + \sum_{d'p_r^2|n} 1 + \sum_{d'p_r^3|n} 1| + ... + \sum_{d'p_r^{sr}|n} 1$$

$$= \zeta(n') + \zeta(n') + \zeta(n') + ... + \zeta(n')$$
$$= \zeta(n').(s_r + 1)$$
$$= (s_1 + 1)(s_2 + 1)....(s_{r-1} + 1)(s_r + 1)$$

Also $$\sigma(n) = \sum d$$

$$\sum_{d|n} d$$

$$d \geq 1$$

$$= \sum_{\substack{d'|n' \\ d' \geq 1}} d' + \sum_{\substack{d'|n' \\ d' \geq 1}} d' p_r + \sum_{\substack{d'|n' \\ d' \geq 1}} d' p_r^2 + \sum_{\substack{d'|n' \\ d' \geq 1}} d' p_r^{sr}$$

$$= \sum_{\substack{d'|n' \\ d' \geq 1}} d' \left(1 + p_r + p_r^2 + ... + p_r^{sr}\right)$$

$$= \sigma(n') \frac{p_r^{s_r+1} - 1}{p_r - 1}$$

By induction hypothesis,

$$\sigma(n') = \frac{p_1^{s1+1} - 1}{p_1 - 1} . \frac{p_2^{s2+1} - 1}{p_2 - 1} ..... \frac{p_{r-1}^{s_{r-1}+1} - 1}{p_{r-1} - 1}$$

Therefore

$$\sigma(n) = \frac{p_1^{s1+1} - 1}{p_1 - 1} . \frac{p_2^{s2+1} - 1}{p_2 - 1} ..... \frac{p_{r-1}^{s_{r-1}+1} - 1}{p_{r-1} - 1} . \frac{p_r^{s_r+1} - 1}{p_r - 1}$$

Example 1. If n =7056, find $\zeta(n)$ and $\sigma(n)$

Solution : We have n = 7056

$$= 2^4 . 3^2 . 7^2$$

Therefore $\zeta(n)$ = (4 + 1) (2 + 1) (2 + 1) = 45

And $$\sigma(n) = \frac{2^{4+1} - 1}{2 - 1} . \frac{3^{2+1} - 1}{3 - 1} . \frac{7^{2+1} - 1}{7 - 1}$$

$$= 31. 13. 57$$

$$= 204321$$

Definition 7.4.3. A number theoretic function f is said to be multiplicative if f (mn) = f(m) f(n) whenever ged (m, n) = 1.

Theorem 7.4.4. The function ζ and σ are multiplicative.

Proof : Let (m, n) = 1, $m, n \in \mathbb{N}$

If m = 1, then ζ (m) = 1 and σ (n) = 1. In this case

$\zeta(m.n) = \zeta(1.n) = \zeta(n) = 1.\ \zeta(n) = \zeta(m)\ \zeta(n)$

$\sigma(m.n) = \sigma(1.n) = \sigma(n) = 1.\ \sigma(n) = \sigma(m).\ \sigma(n)$

Similarly, if n = 1, we get

$$\zeta(mn) = \zeta(m)\ \zeta(n) \text{ and } \sigma(mn) = \sigma(m)\ \sigma(n)$$

Next, let m > 1, n > 1. Then by unique factorization theorem,

$$m = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k} \text{ and } n = q_1^{\beta_1}.q_2^{\beta_2}.....p_t^{\beta_t}$$

Since (m, n) = 1, so $\left(p_i^{\alpha_i}, q_i^{\beta_i}\right)$ for all I = 1, 2, ….. k; j = 1, 2, ….., t

Then $mn = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}.q_1^{\beta_1}.q_2^{\beta_2}.....q_t^{\beta_t}$

Therefore $\zeta(mn) = (\alpha_1+1)\ (\alpha_2+1).....(\alpha_k+1)\ (\beta_1+1)\ (\beta_2+1).....(\beta_t+1)$

$$= \zeta(m)\ \zeta(n)$$

and $$\sigma(mn) = \frac{p_1^{\alpha_1+1}}{p_1-1}.\frac{p_2^{\alpha_2+1}}{p_2-1}.....\frac{p_{k-1}^{\alpha_k+1}}{p_1-1}.\frac{q_{1-1}^{\beta_1+1}}{q_1-1}.\frac{q_{2-1}^{\beta_1+1}}{q_2-1}.....\frac{q_{t-1}^{\beta_1+1}}{q_t-1}$$

$$= \sigma(m)\ .\ \sigma(n)$$

Hence the functions ζ and σ are multiplicative.

Theorem 7.4.5. If f I multiplicative, F (n) = $\sum f(d)$ is multiplicative.

Proof : Let a and b be two positive integers such that (a, b) = 1. We have to prove F (a. b) = F (a). F (b)

Now $$F(ab) = \sum_{d|ab} f(ab)$$

Since (a, b) = 1, so d is the product of a divisor d' of a and a divisor d'' of b. Thus

$$F(ab) = \sum_{\substack{d'|a \\ d''|b}} f(d'dd'')$$

$$= \sum_{\substack{d'|a \\ d''|b}} f(d')\, f(d'') \qquad [\because f \text{ is multiplicative}]$$

$$= \sum_{d'|a} f(d') \sum_{d''|b} f(d'')$$

$$= F(a)\, F(b)$$

Hence F is multiplicative.

W CHECK YOUR PROGRESS

Q.1. Find ζ (180) and σ (180)

Q.2. Prove that ζ (n) is odd iff in is a perfect square.

Q.3. If σ (n) is odd, then n is of the form k^2 or $2k^2$.

Q.4. Show that $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ for every positive integer n.

Q.5. If n is a square free integer, prove that ζ (n)=2^r, where r is the number of prime divisors of n.

Q.6. Show that there are no positive integers n satisfying σ (n) = 10.

7.5 EULER'S ϕ FUNCTION

Definition 7.5.1 For $n \geq 1$, the Euler's ϕ-function is defined as ϕ (1) = 1 and for n > 1, ϕ (n) = the number of positive integers not exceeding n that are relatively prime to n.

For example, $\phi(20) = 8$ and ϕ (13) = 12

In general, if p is a prime number, then ϕ (p) = p – 1.

7.6 PROPERTIES OF EULER'S ϕ FUNCTION

Theorem 7.6.1 If p is prime and k is any positive integer, then

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

Proof : If k = 1, then the integers which are less than p and relatively prime to p are 1, 2, 3 ……, p – 1 and therefore

$$\phi(p) = p - 1$$

Let $k > 1$. Then among the integers 1, 2, 3, ….., p^k those which are not prime to p^k are p, 2p, 3p, ….. p^{k-1}, p^k and no more, i.e. p^{k-1} numbers are loss than p^k and not coprime to p^k . Hence the number of integers which are less than p^k and coprime to p^k is

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

Thus $\phi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right)$

Lemma 7.6.2 Given integers a, b, c, ged (a, bc) = 1 if and only if ged (a, b) = 1 and ged (a, c) = 1

Theorem 7.6.3. The function ϕ is a multiplicative function.

Proof : Let m and n be two integers such that (m, n) = 1. The result obviously holds if either m or n equals 1. We assume m > 1 and n > 1. Arrange the integers from 1 to mn in m columns of n integers each, as follows :

1	2	…… r	…….. m
m+1	m+2	..... m + r	…… 2m
2m+1	2m+2	.....2m + r	…… 3m
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
(n–1) m+1	(n–1)m+2	.....(n–1) m + r	…… mn

We know that ϕ (mn) is equal to the number of entries in this array that are relatively prime to mn; by virtue of the Lemma 7.6.2, this is the same as the number of integers that are relatively prime to both m and n.

Since ged (qm + r, m) = ged (r, m), therefore the numbers in the r^{th} column are relatively prime to m if and only if r itself relatively prime to m. Therefore only ϕ (m) columns contains integers relatively prime to m and every entry in the colum will be relatively prime to m.

Now the entires in the r^{th} column (where it is assumed the ged (r, m = 1) are

r, m + r, 2m + r , ……, (n – 1) m + r

There are n integers in this sequence and no two are congruent modulo n. If possible, let

$$km + r = jm + r \pmod n, \text{ where } 0 \le k < j < n$$

$$\Rightarrow km \equiv jm \pmod n$$

$$\Rightarrow k \equiv j \pmod n \qquad \text{as } (m, n) = 1.$$

Which is a contradiction as $0 \le k < j < n$. This, the numbers in the r^{th} column are congruent modulo n to 0, 1, 2, ……, n – 1, in some order. But if $s \equiv t \pmod n$, then ged (s, m) = 1 $\Leftrightarrow$ ged (t, n) = 1. The implication is that the r^{th} column contains as many integers that are relatively prime to n as does the set { 0, 1, 2, ….., n – 1}, namely, ϕ (n) integers. Therefore, the total number of entries in the aray that are relatively prime to both m and n is ϕ (m) ϕ (n). Thus ϕ (mn) = ϕ (m) ϕ (n)

Theorem 7.6.4 If the integer n > 1 has the prime factorizaation $n = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right).....\left(p_r^{k_r} - p_r^{k_r-1}\right)$ then

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_1^{k_2-1}\right).....\left(p_r^{k_r} - p_r^{k_r-1}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_n}\right)$$

Proof : Since the primes p_1, p_2, …… p_r are pairwise coprime and ϕ is a multiplication function, so

$$\phi(n) = \phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right).....\phi\left(p_r^{k_r}\right)$$

$$= \phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right).....\phi\left(p_r^{k_r}\right)$$

$$= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right).....\left(p_r^{k_r} - p_r^{k_r-1}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_r}\right)$$

Example 1. Find (i) ϕ (23^4) (ii) ϕ (324)

Solution : (i) ϕ (23^4) = $23^4\left(1-\frac{1}{23}\right)$

$$= 23^4 \left(\frac{22}{23}\right)$$

$$= 23^3 \times 22$$

$$= 267674$$

(ii) $\phi(324) = \phi(2^2 \cdot 3^4)$

$$= 2^2.3^4 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$$

$$= 2^2 \times 3^4 \times \frac{1}{2} \times \frac{2}{3}$$

$$= 108$$

Theorem 7.6.5. For $n > 2$, $\phi(n)$ is even.

Proof : Case (I). Let $n = 2^k$, $k \geq 2$. Then

$\phi(n) = \phi\left(2^k\right) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1}$, which is even.

Case (II). Let $n = p^k.m$ where $p\ (\neq 2)$ is a prime and $(p^k, m) = 1$. Then

$$\phi(n) = \phi\left(p^k.m\right) = \phi\left(p^k\right).\phi(m)$$

$$= \left(p^k - p^{k-1}\right)\phi(m)$$

$$= p^{k-1}(p-1)\,\phi(m)$$

We have $2 \mid p - 1$

$\Rightarrow 2 \mid p^{k-1}(p-1)\,\phi(m)$

$\Rightarrow 2 \mid \phi(n)$

$\Rightarrow \phi(n)$ is even.

Theorem 7.6.6 (Gauss Theorem). (i) $n \geq 1$, $n = \sum_{d \mid n} \phi(d)$

$$\sum k = \frac{1}{2} n\ \phi(n)$$

(ii) For $n > 1$, $(n,k) = 1$
$k \le n$

Proof : (i) The prove is done by induction on the number of distinct prime divisors of n. First let $n = p^{\alpha}$, $\alpha \in \mathbb{N}$ and p is prime. Then a divisor d of n is of the form p^r, $0 \le r \le \alpha$. Thus 1, p, p^r, …..p^{α} are the divisors of n. So

$$\sum_{d \mid n} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^{\alpha})$$

$$= 1 + (p-1) + (p^2 - P) + ... + \left(p^{\alpha} - p^{\alpha-1}\right)$$

$$= p^{\alpha}$$

$$= n$$

i.e. the result is true when n is a power of a prime.

We assume now that the result is true for all integers n'>1 that contains r – 1 distinct prime factors, i.e., if $n' = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_{r-}^{\alpha_{r-1}}$ where p_i's are distinct primes and the $\alpha_i \ge 1$ are integers, then $n' = \sum_{d|n'} \phi(d)$.

Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_{r-1}^{\alpha_{r-1}}.p_r^{\alpha_r}$, where p_i's are distinct primes and $\alpha_i \ge 1$ are integers. Then

$$n = n' p_r^{\alpha_r} \quad \text{where} \quad \left(n' p_r^{\alpha_r}\right) = 1$$

Therefore any divisor d of n is of the form $d' p_r^t$ where $d' \mid n'$ and $0 \le t \le \alpha_r$

If $d_1, d_2, \ldots\ldots d_s$ are all the divisors of n', then $d_1\ d_2, ... d_s$; $p_r^1 d_1, p_r d_2, ..., p_r d_s$; $p_r^2 d_2, ...p_r^2 ds$; …….; $p_r^{\alpha_r} d_1, p_r^{\alpha_r} d_2, ..., p_r^{\alpha_r} ds$ are all the divisors of n. So

$$\sum_{d|n} \phi(d) = \sum_{i=1}^{s} \phi(di) + \sum_{i=1}^{s} \phi(p_r d_i) + \sum_{i=1}^{s} \phi\left(p_r^2\, di\right) + ... + \sum_{i=1}^{s} \phi\left(p_r^{\alpha_r} di\right)$$

$$= \sum_{i=1}^{s} \phi(di) + \sum_{i=1}^{s} \phi(p_r)\, \phi(di) + \sum_{i=1}^{s} \phi\left(p_r^2\right) \phi(di) + ... + \sum_{i=1}^{s} \phi\left(p_r^{\alpha_r}\right) \phi(di)$$

$$= \sum_{i=1}^{s} \phi(di)\left[1+\phi(p_r)+\phi(p_r^2)+.....+\phi(p_r^{\alpha_r})\right]$$

$$= n'\left[1+(p_r-1)+(p_r^2-p_r)+(p_r^{\alpha_r}-p_r^{\alpha_r-1})\right]$$

$$= n'\, p_r^{\alpha_r}$$

$$= n$$

(ii) Let $a_1, a_2, ...a_{\phi(n)}$ be the positive integers not exceeding n and relatively prime to n and

$$S = a_1 + a_2 + ...a_{\phi(n)}$$

Now $(k, n) = 1, \quad 1 \le k \le n$

$$\Rightarrow (n-k, n) = 1, \quad 1 \le n-k < n$$

So, the set of integers $\{n-\alpha_1, n-\alpha_2, ..., n-\alpha_{\phi(n)}\}$ is the same set of integers $\{\alpha_1, \alpha_2, ..., \alpha_{\phi(n)}\}$ and

$$s = (n-\alpha_1)+(n-\alpha_2)+.....+(n-\alpha_{\phi(n)})$$

$$\Rightarrow s = n\,\phi(n)-(\alpha_1+\alpha_2+\alpha_{\phi(n)})$$

$$\Rightarrow s = n\,\phi(n)-s$$

$$\Rightarrow 2s = n\,\phi(n)$$

$$\Rightarrow s = \frac{1}{2} n\,\phi(n)$$

$$\Rightarrow \sum k = \frac{1}{2} n\,\phi(n)$$

$(n, k) = 1$

$1 \le k \le n$

Example 2. Find the sum of integers less than 360 and relatively prime to 360.

Solution : $360 = 2^3 . 3^2 . 5^1$

$$\therefore \phi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 96$$

Thus $\sum k = \frac{1}{2} \times 360 \times \phi(360)$

$(360, k) = 1$

$1 \le k \le 360$

$$= \frac{1}{2} \times 360 \times 96$$

$$= 17280$$

Lemma 7.6.7 Let n > 1 and ged (a, n) = 1. If are positive $a_1, a_2, ...a_{\phi(n)}$ are positive integers less than n and relatively prime to n, then $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, ...a_{\phi(n)}$ in some order.

Theorem 7.6.8 If $n \ge 1$ and ged (a, n) = 1, then $a^{\phi(n)} = 1 (\mathrm{mod}\, n)$

Proof : Let n > 1 be an integer and $a_1, a_2, ...a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n.

Since (a, n) = 1, so by Lemma 7,6,7, the integers $aa_1, aa_2, ..., aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, ...a_{\phi(n)}$ in some order, i.e.

$aa_1 \equiv a_1' (\mathrm{mod} n)$

$aa_2 \equiv a_2' \ (\mathrm{mod} n)$

……

……

$aa_{\phi(n)} \equiv a_{\phi(n)}' \ (\mathrm{mod} n)$ where $a_1', a_2', a_{\phi(n)}'$ are just the integers in some order.

On taking the product of these $\phi(n)$ congruence get

$$(aa_1)(aa_2).....(aa_{\phi(n)}) \equiv a_1', a_2', ... a_{\phi(n)}' (\mathrm{mod}\, n)$$

$$\Rightarrow a^{\phi(n)}\left(a_1\ a_2.....a_{\phi(n)}\right)\equiv a_1\ a_2.....a_{\phi(n)}\ (\text{mod } n)$$

Since for each i, $(a_i, n) = 1$, so $\left(a_1\ a_2.....a_{\phi(n)}, n\right)=1$

Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1, a_2,.....a_{\phi(n)}$, leaving us with $a^{\phi(n)}\equiv 1(\text{mod}n)$

Note : The Theorem 7.6.8 is known as Euler's Theorem.

Example 3. Find the last two digits in the decimal representation of 3^{100}.

Solution : The given problem is equivalent to find the smallest non-negative integer to which 3^{100} is congruent modulo 100.

Since $(3,100) = 1$,

$$3^{\phi(100)} \equiv 1\ (\text{mod } 10)$$

$$\Rightarrow 3^{40} \equiv 1\ (\text{mod } 100)\ \text{ since } \phi(100)=\phi\left(2^2.5^2\right)=40$$

Now $3^{100} \equiv 3^{40\times2+20}$

$$\equiv \left(3^{40}\right)^2.\ 3^{20}$$

$$\equiv 1^2.3^{20}\ (\text{mod } 100)$$

$$\equiv \left(3^5\right)^4\ (\text{mod } 100)$$

$$\equiv (43)^4\ (\text{mod } 100)$$

$$\equiv \left(43^2\right)^2\ (\text{mod } 100)$$

$$\equiv (49)^2\ \ (\text{mod } 100)$$

$$= 01\ (\text{mod } 100)$$

Therefore the last two digits in the decimal representation of 3^{100} are 01.

W CHECK YOUR PROGRESS

Q.7. If n is an odd positive integer, then prove that $\phi(2n) = \phi(n)$

Q.8. If n is an even integer, prove that $\phi(2n) = 2\phi(n)$

Q.9. If $n = p_1^{k1}.p_2^{k2}.....p_r^{kr}$ derive the following inequalities

a) $\sigma(n)\phi(n) \geq n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right).....\left(1-\frac{1}{p_r^2}\right)$

b) $\zeta(n)\,\phi(2n) \geq n$

Q.10. Find the last two digits in the decimal representation of 3^{256}.

Q.11. If p and p + 2 are both primes, then show that

$$\phi(p+2) = \phi(p) + 2$$

Q.12. Use Euler's Theorem, to prove $a^{37} \equiv a \pmod{1729}$ for any integer a.

Q.13. Show that if ged (a, n) ; ged (a – 1, n) = 1, then

$$1 + a + a^2 + ... + a^{\phi(n)} \equiv 0 \pmod{n}$$

Q.14. If m and n are relatively prime positive integers, prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

7.7 THE MOBIUS FUNCTION : DEFINITION AND EXAMPLES

Definition 7.7.1. For a positive integer n, the Mobius function μ is defined as

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } p^2 \mid n \text{ for some prime } p \end{cases}$$

$(-1)^r$, if $n = p_1.p_2 \ldots\ldots\ldots p_r$ where p'$_i$s are distinct primes.

For example,

$$\mu(6) = \mu(2.3) = (-1)^2 = 1$$

$$\mu(8) = \mu(2.2.2) = 0$$

$$\mu(20) = \mu(2^2.5) = 0$$

$$\mu(30) = \mu(2.3.5) = (-1)^3 = -1$$

$$\mu(2) = (-1)^1 = -1$$

$$\mu(3) = (-1)^1 = -1$$

Remark : If p is a prime number, it is clear that $\mu(p) = -1$; in addition, $\mu(p^k) = 0$ for $k \geq 2$.

7.8 PROPERTIES OF MOBIUS FUNCTION

Theorem 7.8.1 The function μ is a multiplicative function.

Proof : We want to prove that $\mu(mn) = \mu(m)\mu(n)$, whenever (m, n) = 1. If either $p^2|m$ or $p^2|n$ for some prime p, then $p^2|mn$, hence $\mu(mn) = 0 = \mu(m).\mu(n)$

If both m and n are square free integers, i.e. $m = p_1, p_2 \ldots\ldots p_r$ and $n = q_1\ q_2\ \ldots\ldots\ q_s$ with all the primes p_i and p_j being distinct, then

$$\mu(mn) = \mu(p_1\ p_2 \ldots . p_r\ \ q_1\ q_2 \ldots . q_s)$$

$$= (-1)^{r+s}$$

$$= (-1)^r.(-1)^s$$

$$= \mu(m)\ \mu(n)$$

Lemma 7.8.2. If f_1 and f_2 are multiplicative functions $f_1\ \ f_2$ is multiplicative.

Theorem 7.8. For each positive integer $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n = 0 \end{cases}$$

Proof : For n = 1, $\sum_{d|n} \mu(d) = \mu(1) = 1$

Let n > 1 and $n = p_1^{\alpha 1}.\ p_2^{\alpha 2} \ldots\ldots\ldots p_k^{\alpha k}$ be the prime decompositive of n. Let $F(n) = \sum_{d|n} \mu(d)$.

We know from Theorem 7.8.1. that μ is a multiplicative function. Therefore F is also a multiplicative function and $F(n) = F\left(p_1^{\alpha 1}.\ p_2^{\alpha 2} \ldots\ldots\ldots p_k^{\alpha k}\right)$

$$= F\left(p_1^{\alpha 1}\right).\ F\left(p_2^{\alpha 2}\right).\ F\left(p_k^{\alpha k}\right)$$

Now $F\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}|} \mu(d)$

$= \mu(1) + \mu(p_1) + \mu\left(p_1^2\right) + ...\mu\left(p_1^{\alpha_1}\right)$

$= 1 + (-1)^1 + 0 + ... + 0$

$= 0$

Similarly, $F\left(p_i^{\alpha_i}\right) = 0$ for $i = 2, 3, ..., k$

Thus $F(n) = F\left(p_1^{\alpha_1}\right).F\left(p_2^{\alpha_2}\right).....F\left(p_k^{\alpha_k}\right)$

$= 0.\ 0\ ……..\ 0$

$= 0$

Hence $F(n) = \sum_{d|n} \mu(d) = 0$ for all $n \geq 1$

Example 1. Show that $\sum_{d|10} \mu(d) = 0$

Solution : $\sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$

$= 1 + (-1)^1 + (-1)^1 + (-1)^2$

$= 0$

Example 2. Show that $\sum_{d|n} \mu(d)\,\zeta(d) = (-1)^k$ where k denotes the number of distinct prime factors of n.

Solution : Let $n = p_1^{\alpha_1} . p_2^{\alpha_2} . p_k^{\alpha_k}$ where p_i's $(1 \leq i \leq k)$ are the distinct prime factors of n and

$$F(n) = \sum_{d|n} \mu(d)\,\zeta(d)$$

We know that μ and ζ are multiplicative functions.

$\Rightarrow \mu\zeta$ is also a multiplicative function.

$\Rightarrow F$

Therefore $F(n) = F\left(p_1^{\alpha_1} . p_2^{\alpha_2} . p_k^{\alpha_k}\right)$

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

Now $F\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}} \mu(d)\,\zeta(d)$

$= \mu(1)\,\zeta(1) + \mu(p_1)\,\zeta(p_1) + \mu\left(p_1^{2}\right)\zeta\left(p_1^{2}\right) + ... + \mu\left(p_1^{\alpha_1}\right)\zeta\left(p_1^{\alpha_1}\right)$

$= 1.1 + (-1)^1 . 2 + 0 + ... + 0$

$= —1$

Similarly $F\left(p_i^{\alpha_i}\right) = -1$ for i = 2, 3, ……, k.

Therefore $F(n) = F\left(p_1^{\alpha_1} . p_2^{\alpha_2} . p_k^{\alpha_k}\right)$

$= F\left(p_1^{\alpha_1}\right) . F\left(p_2^{\alpha_2}\right) . F\left(p_k^{\alpha k}\right)$

$= (—1) . (—1) \ldots\ldots (—1)$

$= (-1)^k$

Thus $\sum_{d|n} \mu(d)\,\zeta(d) = (-1)^k$, where k denotes the number of distinct prime factor of n.

Example 3. Show that $\sum_{d|n} \mu(d)\,\sigma(d) = (-1)^k\ p_1\ p_2\ p_k$; where $n = p_1^{\alpha_1} . p_2^{\alpha_2} . p_k^{\alpha_k}$

Solution. Let $F(n) = \sum_{d|n} \mu(d)\,\sigma(d)$

We know that μ and σ are multiplicative functions.

$\Rightarrow \mu\sigma$ is also a multiplicative function.

$\Rightarrow$ F is a multiplicative function.

Therefore $F(n) = F\left(p_1^{\alpha_1} . p_2^{\alpha_2} .....p_k^{\alpha_k}\right)$

$= F\left(p_1^{\alpha_1}\right) . F\left(p_2^{\alpha_2}\right) . F\left(p_k^{\alpha k}\right)$

Now $F\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}} \mu(d)\,\sigma(d)$

$= \mu(1)\,\sigma(1) + \mu(p_1)\,\sigma(p_1) + \mu\left(p_1^2\right)\sigma(p_1^2) + \mu\left(p_1^{\alpha_1}\right)\sigma(p_1^{\alpha_1})$

$= 1.1 + (-1)^1\,(1+p_1) + 0 \ldots\ldots + 0$

$= -p_1$

Similarly $F\left(p_i^{\alpha_i}\right) = -p_i$ for $i = 2,\ 3,\ \ldots\ldots,\ k$

Therefore $F(n) = (-p_1)(-p_2)\ldots\ldots(-p_k)$

$= (-1)^k\ p_1 .. p_2 \ldots\ldots p_k$

$\Rightarrow \sum_{d|n} \mu(d)\,\sigma(d) = (-1)^k\ p_1\ p_2\ p_3 \ldots\ldots p_k$

Check Your Progress

Q.15. Show that $\sum_{d|n} \mu(d)\,\phi(d) = 0(-1)^k$ for any even integer n.

Q.16. For $n = p_1^{\alpha_1} . p_2^{\alpha_2} . p_k^{\alpha_k}$ where $p_1\ p_2\ p_k$ are distinct primes and $\alpha_i \geq 1$ are integers, show that

(i) $\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\ldots\left(1 - \frac{1}{p_k}\right)$

(ii) $\sum_{d|n} \mu(d)\,d = 2^k$

(iii) $\sum_{d|n} |\mu(d)| = 2^k$

(iv) $\sum_{d|n} \mu(d)\,f(d) = (1 - f(p_1))\,(1 - f(p_2))\ldots\ldots(1 - f(p_k))$

(v) $\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$

7.9. THE GREATEST INTEGER FUNCTION : DEFINITION AND EXAMPLE.

Definition 7.9.1. For an arbitrary real number x, we denoted by [x] the largest integer less than or equal to x; that [a] is the unique integer satisfying $x - 1 < [x] \leq x$.

Examples : $\left[-\frac{3}{2}\right] = -2, \left[\sqrt{2}\right] = 1, \left[\frac{1}{3}\right] = 0, [\pi] = 3, [-\pi] = -4$

Remarks : (i) $[x] = x$ if any only if x is an integer.

(ii) For any real x, $x = [x] + \theta$, for a suitable choice of θ, with $0 \leq \theta < 1$.

7.10. THE PROPERTIES OF GREATEST INTEGER FUNCTION

Theorem 7.10.1 For any real numbers x and y,

(i) $[x] \leq x < [x] + 1$

(ii) $[x + n] = [x] + n$, if n is an integer.

(iii) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$

(iv) $[x] + [-x] = \begin{cases} 0, & \text{if } x \text{ is an integer} \\ -1, & \text{otherwise} \end{cases}$

(iv) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$, if n is an positive integer

Proof : For any real number x, we have

$x = [x] + \theta$ Where $0 \leq \theta < 1$ ------- (1)

(i) From (1) if is ckar that

$[x] \leq x$ ------- (2)

Also $[x] + 1 - x = [x] + 1 - ([x] + \theta)$

$= 1 - \theta > 0$ as $\theta < 1$

$\Rightarrow [x] + 1 > x$

$\Rightarrow x < [x] + 1$ -------- (3)

From (2) and (3), we get

$$[x] \le x < [x] + 1$$

(ii) From (1),

$$x = [x] + \theta \quad \text{Where} \quad 0 \le \theta < 1$$

$$\Rightarrow x + n = [x] + n + \theta, \quad \text{where n is an integer.}$$

$$\Rightarrow x + n = [x] + n \quad [\because [x] + n \text{ is an integer}]$$

(iii) Let $x = [x] + \theta_1$ where $0 \le \theta_1 < 1$

$$y = [y] + \theta_2 \text{ where } 0 \le \theta_2 < 1$$

Therefore $x + y = [x] + [y] + \theta_1 + \theta_2$

$$\Rightarrow [x + y] = \begin{cases} [x] + [y], & \text{if } \theta_1 + \theta_2 < 1 \\ [x] + [y] + 1, & \text{if } \theta_1 + \theta_2 \ge 1 \end{cases}$$

Thus $[x + y] = [x] + [y] + 1$

(iv) If x is an integer, then

$$[x] = x \text{ and } [-x] = -x$$

Therefore $[x] + [-x] = 0$

If x is not an integer, then

$$x = [x] + \theta \quad \text{Where} \quad 0 \le \theta < 1$$

$$\Rightarrow -x = -([x] + \theta)$$

$$\Rightarrow [-x] = [-([x] + \theta)]$$

$$= -[x] - 1$$

$$\Rightarrow [x] + [-x] = -1$$

Thus $[x] + [-x] = \begin{cases} 0, & \text{if } \propto \text{ is an integer} \\ -1, & \text{otherwise} \end{cases}$

(v) By division algorithm, we have

$$\lfloor x \rfloor = nq + r, \text{ where } 0 \le r < n$$

Also, we have $x = \lfloor x \rfloor + \theta$, where $0 \le \theta < 1$

Therefore $$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + \theta}{n} \right\rfloor$$

$$= \left\lfloor \frac{nq + r + \theta}{n} \right\rfloor$$

$$= \left\lfloor q + \frac{r + \theta}{n} \right\rfloor$$

$= q$ [$\because r < n \Rightarrow r \le n - 1 \Rightarrow r + \theta \le n - 1 + \theta$

$\Rightarrow r + \theta \le n + (\theta - 1)$

$\Rightarrow r + \theta < n$]

Also $$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{nq + r}{n} \right\rfloor$$

$$= \left\lfloor q + \frac{r}{n} \right\rfloor$$

$= q$ as $r < n$

Thus $$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$$

Lemma 7.10.2. The number of integers in s = { 1, 2, 3, ……, n} divisible by a positive integer a is $\left\lfloor \frac{n}{a} \right\rfloor$

Theorem 7.10.2 The highest power of a prime p which divides n! is $\sum_{i=1}^{k} \left\lfloor \frac{n}{p^k} \right\rfloor$

where $p^k \le n < p^{k+1}$

Proof : Let s = { 1, 2, 3, ……, n } and p is a prime.

Then s has $\left\lfloor \frac{n}{p} \right\rfloor$ integers divisible by p …….. (1)

$\left[\frac{n}{p^2}\right]$ integers divisible by p^2 …… (2)

$\left[\frac{n}{p^3}\right]$ integers divisible by p^3 …… (3)

……

……

$\left[\frac{n}{p^k}\right]$ integers divisible by p^k …… (k)

Since $p^k \le n < p^{k+1}$, so there will be integer in S divisible by higher powers of p than p^k. Moreover, p is a prime, therefore there will be no more integers in S the product of which is divisible by p. Therefore, the total number of factors p in n! will be

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^k}\right] = \sum_{i=1}^{k}\left[\frac{n}{pi}\right]$$

Corollary 7.10.4. The highest power of a prime p dividing n! is $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$, where $p^k \le n < p^{k+1}$

Proof : Since $p^{k+1} > n$ therefore $\left[\frac{n}{p^{k+r}}\right] = 0$ for $r > 0$ and the highest power of a p dividing n! is

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

Example 1. Find the highest power of 3 contained in 40 !

Solution : The highest power of a prime p dividing n! is given by

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^k}\right]$$

where $p^k \le n < p^{k+1}$

We have $3^3 < 40 < 3^4$. Therefore, the highest power of 3 dividing 40! Will be

$$\left[\frac{40}{3}\right]+\left[\frac{40}{3^2}\right]+\left[\frac{40}{3^3}\right]=13+4+1$$

Theorem 7.10.4 If f and F be number theoretic functions such that $F(n)=\sum_{d|n} f(d)$, then for any positive integer N, $\sum_{n=1}^{N} F(n)=\sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$

Proof : Let f and F be two number-theoretic function such that $F(n)=\sum_{d|n} f(d)$

$$\Rightarrow \sum_{n=1}^{N} F(n)=\sum_{n=1}^{N}\ \sum_{d|n} f(d)$$

For a fixed positive integer $k \le N$, the term f(k) appears in $\sum_{d|n} f(d)$ if and only if k is a divisor of n.

Now, to calculate the number of sum $\sum_{d|n} f(d)$ in which f(k) occurs as a term, if is sufficient to find the number of integers among 1, 2, 3, ……, N, which are divisible by k. There are exactly $\left[\frac{N}{k}\right]$ of them :

$$k,\ 2k,\ 3k,\ .....\left[\frac{N}{k}\right]k$$

Thus, for each k such that $1 \le k \le N$, f(k) is a term of the sum $\sum_{d|n} f(d)$ for $\left[\frac{N}{k}\right]$ different positive integers less than or equal to N. Thus we can write the double sum as

$$\sum_{n=1}^{N} F(n)=\sum_{n=1}^{N}\ \sum_{d|n} f(d)$$

$$=\sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Corollary 7.10.5. If N is a positive integer, then

$$\sum_{n=1}^{N}\zeta(n)=\sum_{n=1}^{N}\left[\frac{N}{n}\right]$$

Corollary 7.10.6. If N is a positive integer, then

$$\sum_{n=1}^{N}\sigma(n)=\sum_{n=1}^{N} n\left[\frac{N}{n}\right]$$

Example 2. Find $\sum_{n=1}^{6}\zeta(n)$ and $\sum_{n=1}^{6}\sigma(n)$

Solution : We have $\sum_{n=1}^{6}\zeta(n)=\sum_{n=1}^{6}\left[\frac{6}{n}\right]$

$$=[6]+[3]+[2]+\left[\frac{3}{2}\right]+\left[\frac{6}{5}\right]+[1]$$

$$=6+3+2+1+1+1$$

$$=14$$

and $\sum_{n=1}^{6}\sigma(n)=\sum_{n=1}^{6} n\left[\frac{6}{n}\right]$

$$=1.[6]+2.[3]+3.[2]+4.\left[\frac{3}{2}\right]+5.\left[\frac{6}{5}\right]+6.[1]$$

$$=1.6+2.3+3.2+4.1+5.1+6.1$$

$$=33$$

W CHECK YOUR PROGRESS

Q.17. Find the highest power of 13 contained in 20000 !

Q.18. Find the hight power of 18 contained in 500 !

27.11. LET US SUM UP

- ζ **and** σ **functions :** Given a positive integer n. Let ζ (n) denote the number of positive of n and σ (n) denote the sum of these divisors, i.e., $\zeta : \mathbb{N} \to \mathbb{N}$ is a function such that

$$\zeta(n) = \sum_{\substack{d|n \\ d\geq 1}} 1$$

and $\sigma : \mathbb{N} \to \mathbb{N}$ is a function such that

$$\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} 1$$

- If $n = p_1^{s1} . p_2^{s2} . p_r^{sr}$, where p_i's are distinct primes and $s_i \geq 1$ are integers, then for each $r \geq 1$, the following holds :

  (i) $\zeta(n) = (s_1 + 1)\ (s_2 + 1)\ (s_r + 1)$

  (ii) $\sigma(n) = \frac{p_1^{s1+1} - 1}{p_1 - 1} . \frac{p_2^{s2+1} - 1}{p_2 - 1} ..... \frac{p_r^{sr+1} - 1}{p_r - 1}$

- A number-theoretic function f is said to be multiplicative if f(mn) = f(m). f(n) whenever (m, n) =1.
- The function ζ and σ are multiplicative.
- If f is multiplicative, then $F(n) = \sum_{d|n} f(d)$ is multiplicative.
- **Euler's ϕ - function :** For $n \geq 1$, the Euler's function is defined as $\phi(1) = 1$ and for n > 1, $\phi(n)$= the number of positive integers not exceeding n that are relatively prime to n.
- If p is prime and k is any positive integer, then $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.
- The Euler's ϕ - function is multiplicative.
- If the integer n > 1 has the prime factorization then $n = p_1^{k1} . p_2^{k2} . p_r^{kr}$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_r}\right)$$

- For n > 2, is $\phi(n)$ even.
- Gauss Theorem : (i) For $n \geq 1$, $n = \sum_{d|n} \phi(d)$

  (ii) For n > 1, $\sum_{\substack{(n,k)=1 \\ k\leq n}} k = \frac{1}{2} n\ \phi(n)$

- **Euler's Theorem :** If $n \geq 1$ and ged (a, n) = 1, then
- **The Mobius function :** For a positive integer n, the Mobius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as

$$\mu(n) = \begin{cases} 1, \text{ if } n = 1 \\ 0, \text{ if } p^2 \mid n \text{ for some prime } p \\ (-1)^p \text{ if } n = p_1\ p_2\ \ldots\ldots p_r \text{ where } p_i\text{'s are distinct primes} \end{cases}$$

- The Mobius function μ is a multiplicative function.
- For each positive integer $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \text{ if } n = 1 \\ 0, \text{ if } n > 1 \end{cases}$$

- **The Greatest integer function :** For an arbitrary real number x, we denoted by [x] the largest integer less than or equal to x, i.e. [x] is the unique integer satisfying $x - 1 < [x] \leq x$.
- **Properties of Greatest integer function :** For any real numbers x and y.

(i) $[x] \leq x < [x] + 1$

(ii) $[x + n] = [x] + n$, if n is an integer.

(iii) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$

(iv) $[x] + [-x] = \begin{cases} 0, & \text{if } x \text{ is an integer} \\ -1, & \text{otherwise} \end{cases}$

(v) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$, if n is an positive integer

K 7.12. ANSWERS TO CHECK YOUR PROGRESS

Ans to Q.1 We can write $180 = 2^2 . 3^2 . 5^1$

Therefore $\zeta(180) = (2 + 1)\ (2 + 1)\ (1 + 1)$

$$= 180$$

and $$\sigma(180) = \frac{2^{2+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1}$$

$$= \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4}$$

$= 7.\ 13.\ 6$

$= 546$

Ans. to Q.2 Suppose $n = p_1^{\alpha_1} . p_2^{\alpha_2} ..... p_k^{\alpha_k}$. Then

$$\zeta(n) = (\alpha_1 + 1)(\alpha_2 + 1) ..... (\alpha_k + 1)$$

Now $\zeta(n)$ is odd $\Leftrightarrow$ $(\alpha_1 + 1)(\alpha_2 + 1) ..... (\alpha_k + 1)$ is odd for each i.

i.e. $\zeta(n)$ is odd $\Leftrightarrow$ α_i is even for each i.

$\Leftrightarrow \alpha_i = 2m_i$ for each i.

Therefore $n = p_1^{2m_1} . p_2^{2m_2} ..... p_k^{2m_k}$

$$= \left(p_1^{m_1} . p_2^{m_2} . p_k^{m_k}\right)^2$$

$= m^2$ where $m = p_1^{m_1} . p_2^{m_2} . p_k^{m_k}$

Hence $\zeta(n)$ is odd $\Leftrightarrow$ n is a perfect square.

Ans to Q 3. Let $\sigma(n)$ is odd. We have to prove that n is of the form k^2 or $2k^2$ for some integer k. Let $n = 2^a p^\ell q^m$, $a \in \{o\} \cup \mathbb{N}$, $l, m \in \mathbb{N}$; p, q are odd primes.

$$\therefore \sigma(n) = \sigma\left(2^a p^\ell q^m\right)$$

$$= \sigma\left(2^a\right).\sigma\left(p^\ell\right).\sigma\left(q^m\right)$$

Now $\sigma\left(2^a\right) = \dfrac{2^{a+1} - 1}{2 - 1} = 2^{a+1} - 1$ is always odd and

$\sigma\left(p^\ell\right) = \dfrac{p^{\ell+1} - 1}{p - 1} = 1 + p + p^2 + ... + p^\ell$ is odd iff $p + p^2 + ... + p^\ell$ is even $\Leftrightarrow \ell$ is even, i.e. $\ell = 2k_1$ for some $k_1 \in \mathbb{N}$.

Similarly, $\sigma\left(q^m\right)$ is odd $\Leftrightarrow$ m is even, i.e. $m = 2k_2$ for some $k_2 \in \mathbb{N}$.

Case (1). If a is even, say a = 2m, then

$$n = 2^a p^\ell q^m = 2^{2m} p^{2k_1} q^{2k_2}$$

$$= \left(2^m \; p^{k_1} \; q^{k_2}\right)^2$$

$$= k^2 \text{ where } k = 2^m \; p^{k_1} \; q^{k_2}$$

Case (II). If a = 0, then $n = 2^0 . p^{2k_1} q^{2k_2}$

$$= \left(p^{k_1} \; q^{k_2}\right)^2$$

$$= k^2, \text{ where } k = p^{k_1} q^{k_2}$$

Case (III). If a is odd, say $a = 2k_0 + 1$, then

$$n = 2^1 \; p^{\ell} \; q^m = 2^{2k_0+1} . \; p^{2k_1} q^{2k_2}$$

$$= 2.\left(2^{k_0} \; p^{k_1} \; q^{2k_2}\right)$$

$$= 2k^2, \text{ where } k = 2^{k_0} p^{k_1} \; q^{k_2}$$

Hence $\sigma(n)$ is odd if n is of the form k^2 or $2k^2$

Ans to Q.4 Note that d is a divisor of n if and only if $\frac{n}{d}$ is a divisor of n. Therefore the set of divisors of n = { d_1, d_2, …… d_k } can also be written as $\left\{ \frac{n}{d_1}, \frac{n}{d_2}, \frac{n}{d_k} \right\}$. Thus

$$\sigma(n) = d_1 + d_2 + ... + d_k$$

$$= \frac{n}{d_1} + \frac{n}{d_2} + ... + \frac{n}{d_k}$$

$$= n\left(\frac{1}{d_1} + \frac{1}{d2} + ... + \frac{1}{d_k} \right)$$

$$\Rightarrow \frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$$

Ans. to Q.5 Let n is square free. Then $n = p_1 \; p_2 \; .....p_r$ where each p_i is distinct and of exponent power 1. Thus

$$\zeta(n) = \underbrace{(1+1)(1+1).....(1+1)}_{\text{r times}}$$

Ans to Q.6 Left as an exercise.

Ans to Q.7 Since n is odd, so (2, n) = 1 and

$$\phi(2n)=\phi(2)\,\phi(n) \text{ as } \phi \text{ is multiplicative.}$$

$$\Rightarrow \phi(2n)=1.\phi(n)$$

$$\Rightarrow \phi(2n)=\phi(n)$$

Ans to Q. 9

Case (I). If $n = 2^k.\ p$ where p is an odd positive integer,

$$\text{then } \phi(n)=\phi\left(2^k.p\right)=\phi\left(2^k\right)\phi(p)=2^k\left(1-\frac{1}{2}\right)\phi(p)=2^{k-1}\phi(p)$$

$$\text{and } \phi(2n)=\phi\left(2.2^k p\right)=\phi\left(2^{k+1}.p\right)=\phi\left(2^{k+1}\right)\phi(p)$$

$$=2^k\phi(p)$$

$$=2.2^{k-1}\ \phi(p)$$

$$=2\phi(n)$$

Case (II). If $n = 2^k$, then

$$\phi(n)=\phi\left(2^k\right)=2^k\left(1-\frac{1}{2}\right)=2^{k-1}$$

and $$\phi(2n)=\phi\left(2.2^k\right)$$

$$=\phi\left(2^{k+1}\right)$$

$$=2^k$$

$$=2.2^{k-1}$$

$$=2\phi(n)$$

Ans. to Q.9

(a) We have $n = p_1^{k1}.\ p_2^{k2}.....p_r^{kr}$. Then

$$\sigma(n)=\frac{p_1^{k_1+1}-1}{p_1-1}\cdot\frac{p_2^{k_2+1}-1}{p_2-1}\cdot\frac{p_r^{k_r+1}-1}{p_r-1}$$

and $$\sigma(n)=\left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right).....\left(p_r^{k_r}-p_r^{k_r-1}\right)$$

$$=p_1^{k_1-1}(p_1-1)\,p_2^{k_2-1}(p_2-1).....p_r^{k_r-1}(p_r-1)$$

$$\therefore \sigma(n)\,\phi(n)=\left(p_1^{k_1+1}-1\right)p_1^{k_1-1}\left(p_2^{k_2+1}-1\right)p_2^{k_2-1}.....\left(p_r^{k_r+1}-1\right)p_r^{k_r-1}$$

$$=\left(p_1^{2k_1}-p_1^{k_1-1}\right)\left(p_2^{2k_2}-p_2^{k_2-1}\right).....\left(p_r^{2k_r}-p_r^{k_r-1}\right)$$

But $p_i^{2k_i}-p_i^{k_i-1}=p_i^{2k_i}\left(1-\frac{p_i^{k_i-1}}{p_i^{2k_i}}\right)=\left(p_i^{k_i}\right)^2\left(1-\frac{1}{p_i^{k_i+1}}\right)$

For $k_i\geq 1,\ p_i^{k_i+1}\geq p_i^2 \Rightarrow \frac{1}{p_i^2}\geq\frac{1}{p_i^{k_i+1}}$

$$\Rightarrow -\frac{1}{p_i^2}\leq -\frac{1}{p_i^{k_i+1}}$$

$$\Rightarrow 1-\frac{1}{p_i^2}\leq 1-\frac{1}{p_i^{k_i+1}}$$

Therefore $p_i^{2k_i}-p_i^{k_i-1}\geq\left(p_i^{k_i}\right)^2\left(1-\frac{1}{p_i^2}\right)$

Thus $\sigma(n)\,\phi(n)\geq\left(p_i^{k_1}\right)^2\left(1-\frac{1}{p_1^2}\right)\left(p_2^{k_2}\right)\left(1-\frac{1}{p_2^2}\right).....\left(p_r^{k_r}\right)^2\left(1-\frac{1}{p_r^2}\right)$

$$=\left(p_1^{k_1}\ p_2^{k_2}.....p_r^{k_r}\right)^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right).....\left(1-\frac{1}{p_r^2}\right)$$

$$=n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right).....\left(1-\frac{1}{p_r^2}\right)$$

b) Left as an exercise

Ans to Q. 10 Left as an exercise

Ans to Q. 11 Left as an exercise

Ans to Q. 12 We have $1729 = 7.13.19$ and $\phi(7) = 6,\ \phi(13) = 12,\ \phi(19) = 18$.

By Euler's Theorem,

$$a^{\phi(7)} \equiv 1(\mathrm{mod}\,7),\ a^{\phi(13)} \equiv 1(\mathrm{mod}\,13),\ a^{\phi(19)} \equiv 1(\mathrm{mod}\,19)$$

$$\Rightarrow a^{6} \equiv 1(\mathrm{mod}\,7),\ a^{12} \equiv 1(\mathrm{mod}\,13),\ a^{18} \equiv 1(\mathrm{mod}\,19)$$

$$\Rightarrow \left(a^{6}\right)^{6} \equiv 1^{6}(\mathrm{mod}\,7),\ \left(a^{12}\right)^{13} \equiv 1^{3}(\mathrm{mod}\,13),\ \left(a^{18}\right)^{2} \equiv 1^{2}(\mathrm{mod}\,19)$$

$$\Rightarrow a^{36} \equiv 1(\mathrm{mod}\,7),\ a^{36} \equiv 1(\mathrm{mod}\,13),\ a^{36} \equiv 1(\mathrm{mod}\,19)$$

$$\Rightarrow a^{36} \equiv 1(\mathrm{mod}\,7.13.19)$$

$$\Rightarrow a^{36}.a \equiv 1.a\,(\mathrm{mod}1729)$$

$$\Rightarrow a^{37} \equiv a\,(\mathrm{mod}1729)$$

Ans. to Q.13 Let ged (a, n) = ged (a — 1, n) = 1. Then by Euler's Theorem,

$$a^{\phi(n)} \equiv 1(\mathrm{mod}\,n)$$

$$\Rightarrow a^{\phi(n)} - 1 \equiv 0(\mathrm{mod}\,n)$$

$$\Rightarrow (a-1)\left(a^{\phi(n)-1} + \ldots\ldots + a^{2} + a + 1\right) \equiv 0(\mathrm{mod}\,n)$$

$$\Rightarrow (a-1)\left(a^{\phi(n)-1} + \ldots\ldots + a^{2} + a + 1\right) \equiv 0.(n-1)(\mathrm{mod}\,n)$$

$$\Rightarrow \left(a^{\phi(n)-1} + \ldots\ldots + a^{2} + a + 1\right) \equiv 0(\mathrm{mod}\,n)\ \left[\because \mathrm{ged}(a-1, n) = 1\right]$$

Ans. to Q. 14 Let ged (m, n) =1. Then by Euler's Theorem,

$$m^{\phi(n)} \equiv 1(\mathrm{mod}\,n) \text{ and } n^{\phi(m)} \equiv 1(\mathrm{mod}\,m)$$

But $n^{\phi(m)} \equiv 0(\mathrm{mod}\,n)$ and $m^{\phi(n)} \equiv 0(\mathrm{mod}\,m)$

Therefore $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\,n)$ and $n^{\phi(m)} + m^{\phi(n)} \equiv 1(\mathrm{mod}\,m)$

$$\Rightarrow m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\,mn)$$

Ans. to Q. 15

Case (I). If $n = 2^k$, $k \geq 1$, then

$$\sum_{d|n} \mu(d)\,\phi(d) = \mu(1)\,\phi(1) + \mu(2)\,\phi(2) + \mu(2^2)\,\phi(2^2) + \ldots\ldots\ldots \mu(2^k)\,\phi(2^k)$$

$$= 1.1 + (-1)^1.1 + 0 + \ldots\ldots + 0$$

$$= 0$$

Case (II). If $n = 2^k.p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots p_m^{\alpha_m}$, where $k \geq 1$ and p_i's are primes such that $(p_i^{\alpha_i},\ p_j^{\alpha_j}) = 1$ for $i \neq j$.

Let $F(n) = \sum_{d|n} \mu(d)\,\phi(d)$

We have μ and ϕ are multiplicative functions.

$\Rightarrow \mu\,\phi$ is also a multiplicative function.

$\Rightarrow F$ is a multiplicative function.

Therefore $F(n) = F(2^k.p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots p_m^{\alpha_m})$

$$= F(2^k).\,F(p_1^{\alpha_1}).F(p_2^{\alpha_2})\ldots\ldots F(p_m^{\alpha_m})$$

$= 0$ as $F(2^k) = \sum_{d|2^k} \mu(d)\,\phi(d) = 0$

Thus $\sum_{d|n} \mu(d)\,\phi(d) = 0$, for an even integer n.

Ans. to Q. 16

(i) Let $F(n) = \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \frac{\mu(d)}{f(d)}$

Where f (d) = d is a multiplicative function.

We have μ and f are multiplicative functions.

$\Rightarrow \frac{\mu}{f}$ is also multiplicative function.

$\Rightarrow F$ is a multiplicative function.

Therefore $F(n) = F\left(p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}\right)$

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

Now $F\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}} \frac{\mu(d)}{d}$

$$= \frac{\mu(1)}{1} + \frac{\mu(p_1)}{p_1} + \frac{\mu\left(p_1^2\right)}{p_1^2} + ... + \frac{\mu\left(p_1^{\alpha_1}\right)}{p_1^{\alpha_1}}$$

$$= 1 + \frac{(-1)^1}{p_1} + 0 + ... + 0$$

$$= 1 - \frac{1}{p_1}$$

Similarly $F\left(p_1^{\alpha_1}\right) = 1 - \frac{1}{p_i}$ for i = 2, 3, ….., k

Therefore $F(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)..... \left(1 - \frac{1}{p_k}\right)$

$$\Rightarrow \sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)..... \left(1 - \frac{1}{p_k}\right)$$

(ii) Left as an exercise.

(iii) Let $F(n) = \sum_{d|n} |\mu(d)|$

We have μ is a multiplicative function.

$\Rightarrow |\mu|$ is also a multiplicative function

$\Rightarrow$ F is a multiplicative function.

Therefore $F(n) = F\left(p_1^{\alpha_1}.p_2^{\alpha_2}.p_k^{\alpha_k}\right)$

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

Now $F\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}} |\mu(d)|$

$= |\mu(1)| + |\mu(p_1)| + |\mu(p_1^2)| + ... + |\mu(p_1^{\alpha_1})|$

$= 1 + 1 + 0 + ... + 0$

$= 2$

Similarly $F = (p_i^{\alpha_i}) = 2$ for all i = 2, 3, ..., k

Thus $F(n) = \underbrace{2.2.....2}_{r \text{ times}}$

$= 2^r$

(iv) Left as an exercise.

(v) Let $G(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$

We have μ and ϕ are multiplicative functions.

$\Rightarrow \frac{\mu^2}{\phi}$ is also multiplicative function.

$\Rightarrow$ G is a multiplicative function.

Therefore $G(n) = G\left(p_1^{\alpha_1}.p_2^{\alpha_2}.p_k^{\alpha_k}\right)$

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

Now $G\left(p_1^{\alpha_1}\right) = \sum_{d|p_1^{\alpha_1}} \frac{\mu^2(d)}{\phi(d)}$

$= \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p_1)}{\phi(p_1)} + \frac{\mu^2(p_1^2)}{\phi(p_1^2)} + ... + \frac{\mu^2(p_1^{\alpha_1})}{\phi(p_1^{\alpha_1})}$

$= 1 + \frac{(-1)^2}{p_1 - 1}$

$$= \frac{p_1}{p_1 - 1}$$

$$= \frac{p_1}{p_1\left(1 - \frac{1}{p_1}\right)}$$

$$= \frac{1}{1 - \frac{1}{p_1}}$$

Similarly, $G\left(p_i^{\alpha_i}\right) = \frac{1}{1 - \frac{1}{p_i}}$ for all i = 2, 3, ….., k

Therefore $G(n) = \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdot ..... \frac{1}{1 - \frac{1}{p_k}}$

$$= \frac{n}{n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_k}\right)}$$

Thus $\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$

Ans. to Q. 17 Here n = 20000. We have $13^3 < 20000 < 13^4$. Therefore highest power of 13 contained in 20000! Will be

$$\left[\frac{20000}{13}\right] + \left[\frac{20000}{13^2}\right] + \left[\frac{20000}{13^3}\right]$$

$$= 1538 + 118 + 9$$

$$= 1665$$

Ans. to Q. 18 Left as an exercise.

O 7.13 FURTHER READING

1. David M. Burton, Elementary Number Theory (7th Edn.), McGraw Hill Education (India) Private Limited, Chennai – 600116, 2018.

2. S.B. Malik, Basic Number Theory (2nd Edn.) Vikash Publishing House Private Limited, Noida-201301, 2017

3. H. Kishan, Number Theory, Krishna Prakashan Media (P) Limited, Meerut – 250001 (UP), India, 2017

M 7.14 MODEL QUESTIONS

1. If $n = p_1^{k1} . p_2^{k2} . p_r^{kr}$ is the prime factorization of n > 1, prove that

$$1 > \frac{n}{\sigma(n)} > \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_r}\right)$$

2. For any positive integer n, prove that

$$\frac{\sigma(n!)}{n!} \geq 1+\frac{1}{2}+\frac{1}{3}+.....+\frac{1}{n}$$

3. Given a positive integer k > 1. Show that there are infinitely many integers n for which $\zeta(n) = k$, but at most finitely many n with $\sigma(n) = k$

4. Find the form of all positive integers n satisfying $\sigma(n) = 10$. What is the smallest positive integer for which this is true?

5. For a fixed integer k, show that the function defined by f (n) = n^k is multiplicative.

6. Prove that if f and g are multiplicative functions, then so is their product fg and $\frac{f}{g}$ (whenever $\frac{f}{g}$ is defined)

7. Find the highest power of 10 that divideds 50! .

8. Given integers a and b > 0, show that there exists a unique integer r with $o \leq r < b$ satisfying $a = \left[\frac{a}{b}\right] b + r$.

9. Find the highest power of 5 dividing 1000 !

10. Find ϕ (5040) and ϕ (360000).

11. Show that there are infinitely many integers n of which ϕ (n) is a perfect square.

12. For any positive integer n, verify

$$\frac{1}{2}\sqrt{n} \le \phi(n) \le n$$

13. If the integer n > 1 has r distinct prime factors, then verify $\phi(n) \ge \frac{n}{2^n}$.

14. If the integer n has r distinct odd prime factors, then prove $2^r \mid \phi(n)$.

*** *** ***