Dr. N. PARANJOTHI
Assr. Prof. Statistics
PAC – Cuddalore

Unit - 2 Elementary Number Theory

Prime numbers – Composite Number – Decomposition of a Composite number as a product of primes uniquely (without proof) – Divisors of a positive integer – Congruence modulo n – Euler Function (without proof) – Highest power of a Prime number p Contained in n! – Fermat's and Wilson's Theorem (without Proof)

Prime number

An integer bigger than one whose only factors are 1 and the number itself.

Example: 2, 3, 5, 7, 11, 13 ...

Composite number

A number that has more than two factors is called Composite number.

Example: 4, 6, 8, 9 ...

Factors of 4 are : 1, 2, 4
Factors of 6 are : 1, 2, 3, 6
Factors of 8 are : 1, 2, 4, 8
Factors of 9 are : 1, 3, 9

Twin prime numbers

If the difference between the two prime numbers is only 2 then the prime numbers are called twin prime numbers.

Example: We know that 2, 3, 5, 7, 11, 13, 17, 19, 23 ... are called prime numbers

The pairs (3,5), (5,7) (11,13) (17,19) ... are Twin Prime because the diff

7 - 5 = 2
13 - 11 = 2 (difference) 2
19 - 17 = 2 (difference) 2
5 - 3 = 2 (difference) 2

Perfect Number

A number is called a perfect number if the sum of its divisors excluding the number is equal to the number.

Example:

The divisor of 28 are, 1, 2, 4, 7, 14 and 28

Sum of the divisors excluding the given number is

$$1+2+4+7+14 = 28$$

$$1+2+4+7+14 = \text{given number}$$

$\therefore$ 28 is a perfect number.

Theorem: Every Composite number can be resolved into prime factors and this can be done in only one way.

Divisors of a given number N

Let $N = p^a q^b r^c \ldots$

where $p, q, r \ldots$ be primes

and $a, b, c \ldots$ be all ~~integers~~ natural

Consider the Product

$$(1+p+p^2+\ldots+p^a)(1+q+q^2+\ldots+q^b)(1+r+r^2+\ldots+r^c)\ldots$$

Every term in the expansion of this product is a divisor of N.

The number of terms in the expansion of this product

$$(a+1)(b+1)(c+1)\ldots$$

SUM OF THE DIVISORS

$\therefore$ The number of divisors of $N = (a+1)(b+1)(c+1)\ldots$

Sum of the divisors is equal to Sum of all the divisors in this expansion

$$(1+p+p^2+\ldots+p^a)(1+q+q^2+\ldots+q^b)(1+r+r^2+\ldots+r^c)\ldots$$

$$= \left(\frac{p^{a+1}-1}{p-1}\right)\left(\frac{q^{b+1}-1}{q-1}\right)\left(\frac{r^{c+1}-1}{r-1}\right)\ldots$$

PRODUCT OF THE DIVISORS

Let x be a divisor of N.

Then $\frac{N}{x}$ is also a divisor of N

But the number of all the divisors $= (a+1)(b+1)(c+1)\cdots$

Hence there are $\frac{(a+1)(b+1)(c+1)\cdots}{2}$ pairs of divisors

Such that the product of each pair is N.

$\therefore$ The product of all the divisors = Product of all the pairs

$= N \cdot N \cdot N \cdots \frac{1}{2}(a+1)(b+1)(c+1)$ times

$= N^{\frac{1}{2}(a+1)(b+1)(c+1)}$

EULER'S FUNCTION

Example: Find the number of divisors of the number 48.

Solution:

$N = 48$ (Given)

The prime factors of 48 are

$48 = 2 \times 2 \times 2 \times 2 \times 3$

$48 = 2^4 \times 3^1$

Prime factorization of 48

2	48
2	24
2	12
2	6
3	3
	1

Number of divisors of 48:

$d = (a+1)(b+1)$

$= (4+1)(1+1)$

$= 5 \times 2$

$\boxed{d = 10}$

If $N = p^a q^b r^c$,

Number of divisors of N

$= (a+1)(b+1)(c+1)$

Justification:

Divisor of 48 can be obtained by combining 2's and 3's

Here we have 4 number of 2's and one number of 3's

The number of ways of Combining the available prime factors are

$\{2^0 \text{ or } 2^1 \text{ or } 2^2 \text{ or } 2^3 \text{ or } 2^4\}$ and $\{3^0 \text{ or } 3^1\}$

$\Rightarrow \{2^0 + 2^1 + 2^2 + 2^3 + 2^4\} \cdot \{3^0 + 3^1\}$

$\Rightarrow \{5 \text{ terms}\} \cdot \{2 \text{ terms}\}$ $\{\because$ No. of divisors = No. of terms in the expansion $\}$

$\Rightarrow (a+1) \cdot (b+1)$

$\Rightarrow (4+1)(1+1)$

$\Rightarrow 5 \cdot 2$

$\Rightarrow \underline{10}$ divisors.

#

Euler's function $\phi(N)$

The number of integers less than N and coprime to N is called Euler's function and it is denoted by $\phi(N)$ unity is considered as a divisor of every integer N.

Definition

Euler's function $\phi(n)$ for all positive integers n is defined by $\phi(n) = 1$ for $n = 1$

and $\phi(n)$ = number of positive integers less than n and coprime to n

Remark: $\phi(1) = 1$

Illustration:

(i) $\phi(2)$ means number of positive integers less than 2, that are coprime to 2

$\therefore \phi(2) = 1$

(ii) $\phi(3)$ means number of positive integers less than 3, that are coprime to 3.

integers less than 3 are, 1 and 2

The numbers coprime to 3 are 1 and 2

$\therefore \phi(3) = 2$

(iii) $\phi(4)$ means numbers of positive integers less than 4, that are coprime to 4.

integers less than 4 are 1, 2 and 3

among these three coprime to 4 are 1 and 3

$\therefore \phi(4) = 2$

(iv) $\phi(5)$

The positive integers less than 5 are 1, 2, 3 and 4

among these four numbers, the numbers coprime to 5 are 1, 2, 3 and 4

$\therefore \phi(5) = 4$

(v) $\phi(6)$

Positive integers less than 6 are 1, 2, 3, 4, 5

Composite to 6 are, 1, 4, 5

$\therefore$ ~~$\phi(6) = 3$~~

Prime factors of 6 $= 2 \times 3$

$\phi(6) = \phi(2 \times 3)$

$= \phi(2) \cdot \phi(3)$

$= (2-1)(3-1)$

$= 1 \cdot 2$

$= 2$

(vi) $\phi(7)$: 1, 2, 3, 4, 5, 6

Coprime to 7 are, 1, 2, 3, 4, 5, 6

$\phi(7) = 6$

Properties of Euler's function

Let p be a prime number

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

(2) $\phi(p^e) = p^e - p^{e-1}$

(3) If $m \neq n$, $\phi(m \times n) = \phi(m) \cdot \phi(n)$ (where m, n Prime number)

(4) $\phi(1) =$

Property (1) If $N = p^e$ where p is a prime number then $\phi(p^e) = p^e\left(1 - \frac{1}{p}\right)$

Property (2) let $N = ab$ where a and b are prime to each other then $\phi(ab) = \phi(a) \cdot \phi(b)$

Proof let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}$

where, $p_1, p_2 \ldots q_1, q_2 \ldots$ are prime numbers

Then

$\phi(a) = \phi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right)$

$= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$

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

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

Similarly $\phi(a) = a \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

$\phi(b) = b \cdot \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right)$

$\phi(a) \cdot \phi(b) = ab \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right)$

$$= N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_k}\right)$$

$$= \phi(N)$$

$$\boxed{\phi(a)\cdot\phi(b) = \phi(ab)}$$

∴

Remark: $\phi(a_1 a_2 \ldots a_k) = \phi(a_1)\cdot\phi(a_2)\cdots\phi(a_k)$

Property (3) Show that $\phi(N)$ is even and the sum of all N and prime to it is $\frac{N}{2}\phi(N)$.

Proof:

Let x be any number prime to N and less than N. Then $N-x$ is also less than N and prime to N.

∴ for any number x (less than N) there corresponds another number $N-x$ such that both of are prime to N. and also their sum is N.

Hence the number of numbers less than N and prime to N is even.

∴ $\phi(N)$ can be grouped into $\frac{\phi(N)}{2}$ pairs such that the sum of each pair is N.

∴ The sum of all the numbers less than N and prime to it is $N\frac{\phi(N)}{2}$

Example (1) Find the number of integers less than 600 and Prime to it.

Solution

$600 = 2^3 \times 3^1 \times 5^2$

$\phi(600) = 600 \times (1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})$

$= 600 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$

$\boxed{\phi(600) = 160}$

Prime factorization of 600

2	600
2	300
2	150
3	75
5	25
5	5
	1

If $N = p_1^a p_2^b p_3^c$

then $\phi(N) = N(1-\frac{1}{p_1})(1-\frac{1}{p_2})(1-\frac{1}{p_3})$

Example (2)

Find the Sum of all the positive integers which are less than 600 and Prime to it.

Solution: WKT Sum of all the integers less than N and Prime to $N = \frac{N\,\phi(N)}{2}$

$\boxed{\phi(600) = 160}$

$= \frac{600 \times 160}{2}$

$= 600 \times 80$

$= 48000$

Theorem If $d_1, d_2 \dots d_r$ are all the divisors of any number N then $\phi(d_1) + \phi(d_2) + \dots + \phi(d_r) = N$

Proof: Let $N = p^a q^b \dots k^r$

$\therefore$ any divisor of N is of the form

$p^\alpha q^\beta \dots k^\theta$ where $0 \le \alpha \le a,\ 0 \le \beta \le b, \dots 0 \le \theta \le r$

Consider the product

$$\left[1 + \phi(p) + \phi(p^2) + \dots + \phi(p^a)\right] \cdot \left[1 + \phi(q) + \phi(q^2) + \dots + \phi(q^b)\right]$$
$$\dots \cdot \left[1 + \phi(k) + \phi(k^2) + \dots + \phi(k^r)\right] \longrightarrow (1)$$

Consider a term of this Product say,

$$\phi(p^\alpha)\ \phi(q^\beta) \dots \phi(k^\theta) = \phi(p^\alpha q^\beta \dots k^\theta)$$
$$= \phi(d) \quad \text{where } d \text{ is the divisor of } N.$$

Each term of the Product (1) is of the form $\phi(d)$

$$\Sigma \phi(d) = \left[1 + \phi(p) + \phi(p^2) + \dots + \phi(p^a)\right]$$
$$\cdot \left[1 + \phi(q) + \phi(q^2) + \dots + \phi(q^b)\right] \dots$$
$$\dots \left[1 + \phi(k) + \phi(k^2) + \dots + \phi(k^r)\right]$$
$$= \left[1 + (p-1) + (p^2 - p) + \dots + (p^a - p^{a-1})\right]$$
$$\cdot \left[1 + (q-1) + (q^2 - q) + \dots + (q^b - q^{b-1})\right] \dots$$
$$\cdot 1 + (k-1) + (k^2 - k) + \dots + (k^r - k^{r-1})\Big]$$
$$= p^a \cdot q^b \dots k^r$$

$$\therefore \Sigma \phi(d) = N$$

Integral Part of a real number

The integral part of a real number 'n' is denoted by $[n]$

ie $[n] = I + f$ where I is an integer and $0 < f < 1$

Example: (1) $\frac{5}{4} = 1.25$

$\frac{5}{4} = 1 + 0.25$ ($I + f$ form)

$\therefore$ The integral part of $\frac{5}{4}$ is

$$\boxed{\left[\frac{5}{4}\right] = 1}$$

(2) $\frac{11}{4} = 2.75$

$\frac{11}{4} = 2 + 0.75$

$\therefore$ The integral part of $\left[\frac{11}{4}\right] = 2$

(3) $\frac{3}{4} = 0.75$

$\frac{3}{4} = 0 + 0.75$

$\therefore$ The integral part of $\left[\frac{3}{4}\right] = 0$

Theorem: If $x = a_1 + a_2 + \cdots + a_r$

then $[x] \geq [a_1] + [a_2] + \cdots + [a_r]$ $0 < f_1 < 1$

Let $\frac{a_1}{n} = I_1 + f_1$

$\frac{a_2}{n} = I_2 + f_2$

$\vdots$

$\frac{a_r}{n} = I_r + f_r$

$$\therefore \frac{a_1}{n} + \frac{a_2}{n} + \cdots + \frac{a_r}{n} = I_1 + f_1 + I_2 + f_2 + \cdots + I_r + f_r$$

$$= (I_1 + I_2 + \cdots + I_r) + (f_1 + f_2 + \cdots + f_r)$$

We have $x = a_1 + a_2 + \cdots + a_r$

$$\frac{x}{n} = \frac{a_1}{n} + \frac{a_2}{n} + \cdots + \frac{a_r}{n}$$

$$= (I_1 + I_2 + \cdots + I_r) + (f_1 + f_2 + \cdots + f_r)$$

$$= I + f \quad \text{(say)}$$

Here f can be less than 1 or greater than or equal to 1.

If $f < 1$, then $\left[\frac{x}{n}\right] = I$

If $f \geq 1$ then $\left[\frac{x}{n}\right] = I + 1 > I$

$$\therefore \left[\frac{x}{n}\right] \geq I$$

$$= I_1 + I_2 + \cdots + I_r$$

$$\boxed{\left[\frac{x}{n}\right] \geq \left[\frac{a_1}{n}\right] + \left[\frac{a_2}{n}\right] + \cdots + \left[\frac{a_r}{n}\right]}$$

Theorem: The highest power of a prime p contained in $\lfloor n$ is zero or

$$\lfloor n = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^{k-1}}\right]$$

where $\left[\frac{n}{p^k}\right] = 0$ according as $n < p$ or $n \geq p$.

Proof:

Case(i) If $n < p$ then no integer in $\lfloor n$ is divisible by p and therefore the highest power of p in $\lfloor n$ is zero.

Case (ii) If $n \geq p$ then the numbers $1p, 2p, 3p \cdots \left[\frac{n}{p}\right] p$ are divisible by p.

Hence the highest Power of p in $\underline{n}$ = the highest Power of p in the product $p^{\left[\frac{n}{p}\right]} \cdot 1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right]$

Example: Find the highest power of 2 in $\lfloor 10$

Solution

we know that,

the highest Power of a prime number p in $\lfloor n$ is

$$= \begin{cases} 0 & \text{when } n < p \\ \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^{k-1}}\right] & \text{when } n \geq p. \end{cases}$$

In the given problem, $p=2$ and $n=10$

Here $n > 10$

$\therefore$ The highest Power of 2 in $\lfloor 10$ is

$$= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^{k-1}}\right]$$

$$= \left[\frac{10}{2}\right] + \left[\frac{10}{2^2}\right] + \left[\frac{10}{2^3}\right] + \left[\frac{10}{2^4}\right] + \left[\frac{10}{2^5}\right] + \cdots$$

$$= [5] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] + \left[\frac{10}{16}\right] + \left[\frac{10}{32}\right] + \cdots$$

$$= [5.0] + [2.5] + [1.25] + [0.625] + [0.3125] + \cdots$$

$$= 5 + 2 + 1 + 0 + 0 \cdots$$

$$= 5 + 2 + 1$$

$$= 8$$

$\therefore$ The highest Power of 2 in $\lfloor 10$ is 8.

Justification

$$\lfloor 10 = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$$

$$= (2^1 \times 5) \times 9 \times (2^3) \times 7 \times (2 \times 3) \times 5 \times (2^2) \times 3 \times 2^1 \times 1$$

$$= 2^8 \times 5 \times 9 \times 7 \times 5 \times 3 \times 1$$

$$\lfloor 10 = 2^8 \times 5^2 \times 3^3 \times 7 \times 1$$

Here the highest Power of 2 is 8