Chapter - IV

(10) **Prime number :—** Any integer $p > 1$ which has no divisor except 1 and the number itself is called a prime number. It is denoted by p. Also the nth prime is denoted by p_n.

(11) **Composite number :—** Any integer greater than 1 which is not prime is called composite number.

Theorem 1 : The least divisor other than 1 of a composite number is a prime.

Proof :— Let if possible the least divisor $q\ (>0)$ of an integer a, is not prime, then it has a divisor q_1, $1 < q_1 < q$. Clearly, q_1 is a divisor of a, which contradicts the fact that q is the least divisor, since if a is not prime, then its least positive divisor is a prime divisor.

Theorem-2 If a is a composite divisor and q is its least positive divisor then

$$q \leq \sqrt{a}$$

Proof :— Given that q is divisor of a i.e q/a then we have

$$a = q a_1$$

$$\Rightarrow a_1 \geq q$$

Hence $a \geq q^2$ i.e $q \leq \sqrt{a}$

—x—

Scanned with CamScanner

Theorem – 3

If p is prime and a is any integer, then either $(a,p) = 1$ or a is multiple of p.

Proof :→ Given that p is prime, then it has two divisor 1 and p. Therefore

$(a,p) = 1$ or $(a,p) = p$

in case of $(a,p) = 1$ result is obvious.

if $(a,p) = p$ then by definition of g.c.d a is multiple of p.

Theorem – 4 (Euclid's theorem)

The number of prime is infinite i.e There is no end to the sequence of primes.

Proof :→ Let p be any prime and Q is prime divisor of $a = LA + 1$.

Now since $Q \nmid p$, $Q > p$.

Therefore, for any given prime number, there is a greater prime number, and hence there are infinitely many prime.

Theorem 5

The number of primes of the form $(4n-1)$ is infinite.

Proof :→ Let $4n_1 - 1, 4n_2 - 1, \ldots, 4n_k - 1$ be all the primes not greater than $4n-1$ with same form 1 Then

$a = 4(4n_1 - 1) \cdots (4n_k - 1) - 1$

has a prime divisor different from $4n_1 - 1$. clearly the prime divisor of a

Scanned with CamScanner

is an odd number. Since an odd number can be written as $4n+1$ or $4n-1$ and $(4m+1)(4l+1) = 4(4lm+l+m)+1$ the prime divisor of a can not be all of the form $4n+1$ and therefore among them, there exists an integer of the form $4n-1$.

Theorem 6

If p is prime and p/ab then either p/a or p/b.

Proof: If p/a then $(a,p)=1$ then theorem is proved.

Now suppose that

$p \nmid a$. Then

only divisors p are 1 and p, therefore

$(p,a) = p$

or $(p,a) = 1$

Therefore, there exists integers x and y such that $1 = bx + py$

Multiplying by b, we get

$$b = abx + bpy$$

Since, by hypotheses p divides ab and since obviously p divides p, it follows that p divides b.

Scanned with CamScanner

(Fundamental theorem of Arithmetic)

Statement :— Every positive integer greater than 1 can be expressed uniquely as a product of primes, up to the order of the factors. More precisely, any positive integer a can be expressed as

$a = p_1 p_2 \cdots p_r$ all p_i being primes.

Further, if a is also given by

$a = q_1 q_2 \cdots q_s$ all q_j being primes.

then $r = s$ and

$p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots q_s$ differ only in their orders.

Proof :— Let $a > 1$ be an integer. If a is prime then result is obvious. If n is composite number, then $\exists$ a prime p_1 such that

$a = p_1 a_1$ for some integer a_1

If a_1 is prime, then a can be expressed as the product of prime factors. But if a_1 is a composite number then $\exists$ a prime p_2 such that $a = p_1 a_1 = p_1 p_2 q_2$ for some integer a_2.

If a_2 is prime, then again it can be expressed as the product of prime factors. If a_2 is a composite number then we proceed continuously as above.

Now since $a > a_1 > a_2 \cdots$

the process can not continue infinitely,

Thus, after a finite number of steps, we get

$a = p_1 p_2 \cdots p_k$

Scanned with CamScanner

where all p_i's are prime.

Now we shall show the uniqueness of factorisation. Let if possible a can be represented as a product of primes in two ways, as follows

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad r \le s \qquad \text{——— (1)}$$

where p_i and q_i are primes in the non decreasing order. i.e.

$$p_1 \le p_2 \le p_3 \cdots \le p_r \text{ and } q_1 \le q_2 \le q_3 \cdots \le q_s$$

since $p_1 / q_1 q_2 \cdots q_n$,

There exists some q_i such that p_1 / q_k.

But p_1 and q_k are both primes. Thus $p_1 = q_k$

Rearrange q_i's such that $p_1 = q_1$.

on Cancelling p_1 and q_1 in (1) we get

$$p_2 \cdot p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

We Continue this process till all p_i's are exhausted. Now since $r < s$, we get

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

Which is not possible because q_i's are primes.

Therefore, r can not be less than s.

Similarly we can show that s can not be less than r.

Hence $r = s$ and

$$p_i = q_i \quad \forall i$$

$\Rightarrow$ factorization is unique

Scanned with CamScanner