M.S c Mathematics –SEM 2 Number Theory CC-10 Unit 2

E-content –By Dr Abhik Singh, Guest faculty, PG Department of Mathematics, Patna University, Patna

Content-Fundamental Theorem of Arithmetic or Uniqueness theorem

Statement: Every Postive integer n>1 can be expressed as the product of prime factors uniquely.

Proof: Let n>1 be an integer. If n is a prime number, then we have nothing to do to prove the theorem.

If n is a composite number , then there exists a prime p, such that for some integer n, we have ;

$n=p_1 n_1$ .... (i)

If n_1 is a prime number, then n is expressible as the product of prime Factors by equation (i)

But if n_1 is a composite number, then there exists a prime number p_2 such that

$n_1=p_2n_2$, For some integers n_2...(ii)

Therefore from (i)

$n=p_1 n_1$

$n=p_1 p_2 n_2$ .... (using (ii)..........................(iii)

If n_2 is a prime number , then n is expressed by (iii) as the product of prime Factors. But if n_2 is a composite number, then we continue the process .

Since , $n > n_1 > n_2 >$ ....,

the process cannot continue infinitely.

Therefore , after finite number of steps ,we get

$n=p_1 p_2 \ldots\ldots\ldots\ldots\ldots p_k$,

where all p_i's are prime numbers.

Now, suppose if possible n can be represented as a product of primes in two ways as follows,

$n=p_1.p_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots p_r \quad = \quad q_1.q_2 \ldots\ldots\ldots\ldots\ldots q_s$, r<s ....(iv)

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

$p_1 \leq p_2 \leq \ldots\ldots\ldots\ldots\ldots\ldots\leq p_r$

$q_1 \leq q_2 \leq \ldots\ldots\ldots\ldots\ldots\ldots\ldots\leq q_s$

Since ,$p_1 \mid q_1 q_2 \ldots\ldots\ldots\ldots q_s$, there exist some primes q_k such that $p_1 | q_k$.

But p_1 and q_k are both primes

Therefore $p_1= q_k$

We rearrange q_i's such that $p_1=q_1$

Now cancelling p_1 and q_1 in (iv) ,we get

$P_2 \cdot P_3 P_4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots = q_2 q_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots q_s$

We continue this process till all p_i's are exhausted.

Also ,as r<s ,we are therefore left only with

$1=q_{r+1}.q_{r+2}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots q_{r+s}$

But it is not possible as q_i's are primes.

Therefore , r cannot be less than S.

Similarly ,we can show that S cannot be less than r .Hence r=s and ,

$p_i=q_i$,$\forall$ i

This suggests that the representation is unique

If n is not divisible by any prime $\leq \sqrt{n}$, then prove that n is prime

Suppose if possible n is not a prime.

Then, it is a composite number.

Therefore, by Fundamental theorem of arithmetic, n can be written as,

$n=p_1^{q_1}\ldots\ldots\ldots\ldots P_r^{q_r}$,

(where p_i's are primes and q_i's≥ 1 are ntegers)

$n \geq p_1 . p_2$ ....(i)

Since it is given that n isn't divisible by any prime $\leq \sqrt{n}$ i.e , n is divisible by primes $> \sqrt{n}$, therefore we have ;

$P_1 | n$, $P_2 | n = p_1, p_2 > \sqrt{n}$

$= p_1 p_2 > \sqrt{n}\sqrt{n}$ .... (ii)

From (i) and (ii) ,it follows that

$n \geq p_1 p_2 > \sqrt{n}\sqrt{n}$ ....

$= n \geq \sqrt{n}\sqrt{n}$

Which is impossible

Hence , n must be n prime number.

Hence Proved