Quadrant II- Transcript and Related Materials

Programme: Bachelor of Science (Third Year)

Subject: Mathematics

Paper Code: MTE103

Paper Title: Number Theory

Unit: I - Divisibility Theory in Integers

Module Name: The Fundamental Theorem of Arithmetic

Name of the Presenter: Minoshka D'Souza

Definition 14.1. An integer $p > 1$ is called a **prime number**, if the only positive divisors of p are p and 1. An integer greater than 1 that is not prime is termed as **composite**.

Example 14.2. Among the first 10 positive integers, $2, 3, 5, 7$ are primes and $4, 6, 8, 9, 10$ are composite numbers. Note that the integer 2 is the only even prime, and according to our definition the integer 1 plays a special role, being neither prime nor composite.

Theorem 14.3. *If p is a prime and $p|ab$ then $p|a$ or $p|b$*

Proof. If $p \mid a$, there is nothing to prove.

Suppose $p \nmid a$. Since p is a prime the only divisors of p are p and 1 and therefore we have,

$$\gcd(p, a) = 1$$

Hence, by Euclid's Lemma we see that $p \mid b$. □

Corollary 14.4. *If p is a prime and $p|a_1a_2 \cdots a_n$, then there exist k, $1 \leqslant k \leqslant n$ such that $p|a_k$.*

Corollary 14.5. *If $p, q_1, q_2, \cdots, q_n$ are all primes and $p|q_1q_2 \cdots q_n$ then there exist k, $1 \leqslant k \leqslant n$ such that $p = q_k$.*

Theorem 14.6 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ is either*

a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof. **Existence**

Using strong induction we shall prove that every positive integer $n > 1$ is either a prime or a product of primes.

Since 2 is a prime the statement is true for $n = 2$.

Let $n \geqslant 2$ and assume that the statement holds for all positive integers k, $2 \leqslant k \leqslant n$.

We shall prove that the statement is true for $n + 1$.

Now, $n + 1$ is either prime or composite.

If $n + 1$ is prime, there is nothing to prove.

If $n + 1$ is composite, there exists positive integers a, b such that $2 \leqslant a, b \leqslant n$ and $n + 1 = ab$.

Since $2 \leqslant a \leqslant n$, by the induction hypothesis we see that a is either a prime or a product of primes. Similarly, b is either a prime or a product of primes.

Since $n + 1 = ab$, it follows that $n + 1$ is a product of primes and hence the statement holds for $n + 1$.

It follows that every positive integer $n > 1$ is either a prime or a product of primes.

Uniqueness

Suppose the integer n can be represented as a product of primes in two different ways,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where $r \leqslant s$, $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ and $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$

Since $p_1 \mid q_1 q_2 \cdots q_s$ and $q_1, q_2, \cdots, q_s$ are all primes, $p_1 = q_k$ for some k and hence $p_1 \geqslant q_1$. Similarly we see that $q_1 \leqslant p_1$ and hence, $p_1 = q_1$. It follows that,

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Repeating this process we get $p_2 = q_2$ which implies that,

$$p_3 \cdots p_r = q_3 \cdots q_s$$

We proceed in this manner. If $r < s$, we would eventually arrive at

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

which is a contradiction as each $q_j > 1$. Hence, $r = s$ and $p_i = q_i$, $1 \leqslant i \leqslant r$. □

Corollary 14.7. *Any positive integer $n > 1$ can be written uniquely in a canonical form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, ..., r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.