(38)

Prime Number: An integer $p > 1$ is called a prime number if its only divisors are 1 and p.

→ An integer greater than 1 that is not a prime is termed Composite.

e.g 2, 3, 5, 7, ... are primes

4, 6, 8, 10, ... are Composites

→ Integer 2 is the only even prime.

→ 1 is neither a prime nor Composite.

39

Theorem: If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$ then the results hold.

Suppose $p \nmid a$.

$\therefore$ the only divisors of p are 1 and p itself.

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

By Euclid's Lemma

$$p \mid b$$

($\gcd(a, p) \neq p$

$\therefore$ if $(a, p) = p$ then $p \mid a$

a contradiction)

(40)

Corollary: If p is a prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_k$ for some k, $1 \le k \le n$.

Proof:

(41)

Corollary: If $p, q_1, q_2, \ldots q_n$ are all primes and $p \mid q_1 q_2 \ldots q_n$ then $p = q_k$ for some k, $1 \le k \le n$.

(42)

Fundamental Theorem of Arithmetic:

Every positive integer $n>1$ can be expressed as a product of primes; this representation is unique apart from the order in which the factors occur.

Proof: Either n is prime or Composite.

If n is prime, there is nothing to prove. Hence the result.

If n is composite, then $\exists\ d \in \mathbb{Z}$ such that $d|n$ and $1<d<n$.

Among all such d, choose p_1 to be the smallest. Then p_1 must be prime number. Otherwise, it too would have a divisor q with

(43)

$1 < q < p_1$ but then $q \mid p_1$

and $p_1 \mid n \Rightarrow q \mid n$ which contradicts the choice of p_1 as the smallest positive divisor of n. $(p_1 \neq 1)$.

$\therefore \quad n = p_1 n_1$

p_1 is a prime and $1 < n_1 < n$.

If n_1 is prime, we are done.

Otherwise, $\exists$ a second prime p_2 s.t

$$n_1 = p_2 n_2 \quad , \quad 1 < n_2 < n_1$$

$$\therefore \quad n = p_1 p_2 n_2 \quad , \quad 1 < n_2 < n$$

If n_2 is a prime, we are done.

otherwise, $n_2 = p_3 n_3$, p_3 is a prime

$$n = p_1 p_2 p_3 n_3 \quad ; \quad 1 < n_3 < n$$

The decreasing sequence

$$n > n_1 > n_2 > \dots > 1$$

(44)

must terminate after a finite number of steps. After finite steps η_{k-1} is a prime call it p_k.

$$\therefore \quad \eta = p_1 p_2 p_3 \cdots p_k$$

Uniqueness:

suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad - \circledast$$

$$r \leq s$$

where p_i and q_j are all primes

and $\quad p_1 \leq p_2 \leq \cdots \leq p_r$

$$q_1 \leq q_2 \leq \cdots \leq q_s$$

$\because \quad p_1 \mid p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

$\Rightarrow \quad p_1 = q_k$ for some k

if $k \neq 1$, then $p_1 > q_1$

Similarly, $q_1 > p_1$

$\Rightarrow \quad p_1 = q_1$

45

Equation ⊛ becomes

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

Repeat this process to get

$$p_2 = q_2$$

$$\Rightarrow \quad p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s$$

$$\vdots$$

$$1 = q_{r+1} q_{r+2} \cdots q_s \quad \text{if } r < s$$

which is absurd $\because q_j > 1$

$$\Rightarrow \quad r = s$$

$$\Rightarrow p_1 = q_1, \; p_2 = q_2, \ldots, p_r = q_r$$

Corollary: Any positive integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $k_i \in \mathbb{Z}^+$, p_i is prime, $\forall i$

$$p_1 < p_2 < p_3 < \cdots < p_r.$$