Prime Numbers.

Defn: An integer $p > 1$ is called a preime number, if its only positive divisores are 1 and p.

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

eg: 2, 3, 5, 7 are preime numbers.

4, 6, 8, 9, 10 are Composite numbers.

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

Pf: If $p \mid a$, then there is nothing to prove. Let us assume that $p \nmid a$. Since p is a preime number so the only positive devisors of p are 1 and p. So, $\gcd(a, p) = 1$, [$\because \gcd(a, p) \neq p$, as $p \nmid a$].

Thus $p \mid ab$ and $\gcd(a, p) = 1$. Hence by Euclid's lemma $p \mid b$. ##

[**Euclid's lemma:** If $a \mid bc$, with $\gcd(a, b) = 1$ then $a \mid c$].

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

Pf: We will prove the result by induction on n, the number of factors. When $n = 1$, then the stated conclusion obviously holds. When $n = 2$, then $p \mid a_1 a_2$ implies $p \mid a_1$ or $p \mid a_2$ [By the previous theorem]. So the stated result is true for $n = 1$ and 2. Let the stated result be true for $n = t$

i.e. $p \mid a_1 a_2 \cdots a_t$ implies $p \mid a_k$ for some k, where $1 \le k \le t$.

Now, if

$p \mid (a_1 a_2 \cdots a_t) a_{t+1}$

$\Rightarrow p \mid a_1 a_2 \cdots a_t$ or $p \mid a_{t+1}$

$\Rightarrow p \mid a_k$, $1 \le k \le t$ or $p \mid a_{t+1}$

$\Rightarrow p \mid a_k$, $1 \le k \le t+1$.

Thus the stated result is true for $n = t+1$.

Hence by induction the stated result is true for all n.

i.e. if $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_k$ for some k, $1 \le k \le n$.

∎

Corollary 1. 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, where $1 \leq k \leq n$.

Pf. Let $p \mid q_1 q_2 \ldots q_n$

Then $p \mid q_k$ for some k; where $1 \leq k \leq n$.

Since q_k is a prime so only positive divisors of q_k are 1 and q_k. As p is a divisor of q_k so either $p = 1$ or $p = q_k$. But being a prime p, $p > 1$. Hence $p = q_k$.

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.

Pf :- If n is a prime then there is nothing to prove. Let n be composite. Then $\exists$ an integer d s.t. $d \mid n$ and $1 < d < n$.

Consider the set

$$S = \{ d' : d' \mid n \text{ and } 1 < d' < n \}$$

clearly $S \neq \phi$ as $d \in S$. So by well ordering principle S has a least element say p_1.

$\therefore p_1 \mid n$ and $1 < p_1 < n$.

We claim p_1 is prime.

If p_1 is not a prime number, then $\exists$ a divisor q of p_1 with $1 < q < p_1$. $\Rightarrow q \in S$,
But $q \mid p_1, p_1 \mid n \Rightarrow q \mid n$, which is a contradiction as p_1 is the least positive divisor of n. Hence p_1 is prime.
Thus, $p_1 \mid n \Rightarrow n = p_1 n_1$, $1 < n_1 < n$.
If n_1 is prime we have our desired result as $n = p_1 n_1$, product of primes.
If n_1 is not a prime then we repeat the same argument to produce a second prime p_2 s.t. $n_1 = p_2 n_2$, $1 < n_2 < n_1$.
If n_2 is prime then we get our desired result as $n = p_1 p_2 n_2$, $1 < n_2 < n$.
If n_2 is not a prime then we proceed as above to get another prime p_3 s.t.

$$n_2 = p_3 n_3, \quad 1 < n_3 < n_2.$$

$$\therefore n = p_1 p_2 p_3 n_3, \quad 1 < n_3 < n_2$$

The decreasing sequence

$$n > n_1 > n_2 > n_3 > \cdots > 1$$

cannot continue indefinitely, so after a finite number of steps n_{k-1} is a prime, call it p_k.

$\therefore n = p_1 p_2 \cdots p_k$.

Uniqueness: Let

$n = p_1 p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_s$, $r \le s$.

where p_i and q_j are all primes; written in increasing magnitude so that

$p_1 \le p_2 \le \cdots \le p_r$; $q_1 \le q_2 \le \cdots \le q_s$.

Since $p_1 \mid n \Rightarrow p_1 \mid q_1 \cdot q_2 \cdots q_s$

$\Rightarrow p_1 = q_k$ for some k, $1 \le k \le s$.

$\therefore p_1 \ge q_1$.

Similarly, $q_1 \ge p_1$. Hence $p_1 = q_1$.

$\therefore p_1 p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$

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

Now repeating the process to get $p_2 = q_2$ we get

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

$\Rightarrow p_3 p_4 \cdots p_r = q_3 \cdot q_4 \cdots q_s$.

If $r < s$ then continuing the above process we get

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

which is absurd as $q_{r+1}, \ldots, q_s$ all primes and product of primes cannot be equal to 1. Hence $r = s$

Thus $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_r = q_r$.