If $k < m$, then after k steps the left hand side reduces to 1 and the right hand side becomes the product of $m-k$ q's, each of which is a prime.

This can not happen. Therefore $k \geq m$.

If $k > m$, then after m steps the right hand side reduces to 1 and the left hand side becomes the product of $k-m$ p's, each of which is a prime.

This can not happen.

So, $k = m$ and the products $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_m$ give the same representation except for the order of the factors.

Thus $n (>1)$ is expressed as the product of a number of primes, the representation being unique except for the order of the factors.

For example, $3150 = 2.3.3.5.5.7 = 2.3^2.5^2.7$

$210 = 2.3.5.7$

Note 1. By ~~Fundamental~~ Fundamental theorem of Arithmetic any integer $n(>1)$ can be written as $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where the primes $p_i, i=1,2,\ldots,r$ are distinct with $p_1 < p_2 < \cdots < p_r$ and the exponents α_i, $i=1,2,\ldots,r$ are positive integer. This form is called the canonical form.

2. An integer is said to be square-free if no α_i in the canonical form of n is greater than 1.

Example: $210 = 2.3.5.7$. So, 210 is a square free integer.

<u>Arithmetic function</u> : A real or complex valued function whose domain is the set of all positive integers is called an Arithmetic function.

4.6 Some Arithmetic functions

4.6.1 <u>Phi function</u> : The function ϕ, called Euler's phi function is an arithmetic function and is defined for all positive integers by, $\phi(1) = 1$ and for $n > 1$

$\phi(n)$ = the number of positive integers less than n and prime to n.

For example, let $n = 8$

The positive integers less than 8 and prime to 8 are $1, 3, 5, 7$. So, $\phi(8) = 4$

Let $n = 20$

The positive integers less than 20 and prime to 20 are $1, 3, 7, 9, 11, 13, 17, 19$. So, $\phi(20) = 8$

If p is a prime then every positive integer less than p is prime to p. So, $\phi(p) = p - 1$

<u>Theorem 4.6.2</u> The function ϕ has the property that

$\phi(mn) = \phi(m) \cdot \phi(n)$ where m and n relatively prime integers.

First we prove the following lemmas:

<u>Lemma 1.</u> a is prime to mn if and only if a is prime to m and

a is prime to n.

Proof: Let a be prime to mn and $d = \gcd(a, m)$. Then $d|a$ and $d|m$ and this implies $d|mn$.

So, ~~gcd(a, m) ≥ d~~ $\gcd(a, mn) \geq d$, but ~~gcd(a, mn)~~ $\gcd(a, mn) = 1$ by assumption. Hence $d = 1$, proving that a is prime to m. By ~~simil~~ similar arguments, a is prime to n.

Conversely, let a be prime to m and a be prime to n

Since a is prime to m, there exists integers u and v such that $au + mv = 1$. Since a is prime to n, there exists integers p and q such that $ap + nq = 1$

We have $aunq + mvnq = nq = 1 - ap$

or, $a(unq + p) + mn(vq) = 1$

Since $unq + p$ and vq are integers, so, a is prime to mn

Lemma 2 If r be the residue of a modulo n and r is prime to n then a is prime to n.

Proof: Since $\gcd(qn + r, n) = \gcd(r, n)$, the lemma follows.

Lemma 3 If c be an integer and a is prime to n then the number of integers in the set $\{c, c+a, c+2a, \dots, c+(n-1)a\}$ that are prime to n is $\phi(n)$

Proof: No two integers of the set are congruent modulo n, because

$$c + sa \equiv (c + ta) \pmod{n} \quad 0 \le s < t \le n-1$$

$$\Rightarrow s \equiv t \pmod{n}, \text{ a contradiction.}$$

Therefore the set of integers is congruent modulo n to $0, 1, 2, \ldots, (n-1)$ in some order. Since the number of integers among $0, 1, 2, \ldots, n-1$ that are prime to n is $\phi(n)$, the lemma follows.

Proof of Theorem 4.6.2. Since $\phi(1) = 1$, the theorem is trivially true when m or n equals 1. Let us assume that $m > 1$ and $n > 1$. We arrange mn integers in n rows and m columns as follows:

$$\begin{array}{cccccccc}
1 & 2 & \ldots & r & \ldots & m \\
m+1 & m+2 & \ldots & m+r & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+r & \ldots & 3m \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+r & \ldots & nm
\end{array}$$

The number of integers among these, that are prime to mn is $\phi(mn)$. By lemma 1, these integers are both prime to m and n.

The number of integers in the first row that are prime to m is $\phi(m)$. By lemma 2, each integer in the column of r $(1 \le r \le m)$ is prime to m if r is prime to m