3.5. Phi function.

Definition. The function ϕ, called *Euler's phi function* (Euler's *totient function*), 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 $n = 8, 20$.

The positive integers less than 8 and prime to 6 are $1, 3, 5, 7$. Therefore $\phi(8) = 4$.

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

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

Note. The function ϕ is a number-theoretic function.

Theorem 3.5.1. The function ϕ is a multiplicative function. That is, if m and n be relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.

First we prove the following lemmas.

Lemma 1. 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 $d|mn$.

Therefore $gcd(a, mn) \geq d$, but $gcd(a, mn) = 1$ by assumption.

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

We have $anuq + mnvq = nq = 1 - ap$

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

Since $nuq + p$ and vq are integers, it follows that 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.

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 $\{c, c + a, c + 2a, \ldots, c + (n-1)a\}$ that are prime to n is $\phi(n)$.

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

$$c + sa \equiv c + ta \pmod{n} \qquad 0 \leq s < t \leq n - 1$$
$$\Rightarrow s \equiv t \pmod{n}, \text{ a contradiction.}$$

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 the theorem.

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

$$\begin{array}{cccccc}
1 & 2 & \cdots & r & \cdots & m \\
m+1 & m+2 & \cdots & m+r & \cdots & 2m \\
2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\
\cdots & \cdots & & \cdots & & \\
(n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm.
\end{array}$$

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 $r(1 \leq r \leq m)$ is prime to m if r is prime to m. So there are $\phi(m)$ columns of integers prime to m.

Again by lemma 3, each column in the arrangement contains $\phi(n)$ integers prime to n.

Therefore the number of integers those are prime to m as well as n is $\phi(m).\phi(n)$.

This completes the proof.

Note. $\phi(m_1 m_2 \ldots m_r) = \phi(m_1)\phi(m_2)\ldots\phi(m_r)$, where $m_1, m_2, \ldots, m_r$ are pairwise prime.

Theorem 3.5.2. If p be a prime and k be a positive integer,

$$\phi(p^k) = p^k(1 - \tfrac{1}{p}).$$

Proof. The positive integers $\leq p^k$ which are not prime to p^k are $p, 2p, 3p, \ldots, (p^{k-1})p$. Therefore the number of positive integers less than p^k and prime to p^k is $p^k - p^{k-1}$.

Hence $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.

Theorem 3.5.3. If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are prime to one another, $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_r})$.

Proof. $\phi(p_1^{a_1}) = p_1^{a_1}(1 - \frac{1}{p_1}), \phi(p_2^{a_2}) = p_2^{a_2}(1 - \frac{1}{p_2}), \ldots$

Since $p_1^{a_1}$ and $p_2^{a_2}$ are prime to each other,

$\phi(p_1^{a_1} p_2^{a_2}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) = p_1^{a_1} p_2^{a_2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$.

Since $p_3^{a_3}$ is prime to $p_1^{a_1} p_2^{a_2}$, $\phi(p_3^{a_3} p_1^{a_1} p_2^{a_2}) = \phi(p_3^{a_3}).\phi(p_1^{a_1} p_2^{a_2})$

$= p_3^{a_3}(1 - \frac{1}{p_3}).p_1^{a_1} p_2^{a_2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$

$= p_1^{a_1} p_2^{a_2} p_3^{a_3}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3})$.

Proceeding with similar arguments we have

$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_r})$.

To illustrate the theorem, let $n = 12$. The integers less than 12 and prime to 12 are $1, 5, 7, 11$. Here $\phi(12) = \phi(2^2.3) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$.

Some properties of phi function.

1. If $n > 1$, the sum of all positive integers less than n and prime to n is $\frac{1}{2}n.\phi(n)$.

Proof. Let a be a positive integer less than n and prime to n. Then $au + nv = 1$ for some integers u and v.

Therefore $n(v+u)+(n-a)(-u) = 1$. Since $u+v$ and $-u$ are integers, it follows that $n - a$ is also a positive integer less than n and prime to n. Therefore $\phi(n)$ positive integers less than n and prime to n can be expressed as $a_1, a_2, a_3, \ldots, (n - a_3), (n - a_2), (n - a_1)$.

Let $S = a_1 + a_2 + a_3 + \cdots + (n - a_3) + (n - a_2) + (n - a_1)$.

Then $S = (n - a_1) + (n - a_2) + (n - a_3) + \cdots + a_3 + a_2 + a_1$. (sum in the reverse order)

Adding, we have $2S = \phi(n).n$, or, $S = \frac{1}{2}n.\phi(n)$.

2. For any positive integer n, $n = \sum\limits_{d|n} \phi(d)$, where the summation extends over all positive divisors d of n.

Proof. Let $S = \{1, 2, \ldots, n\}$, $n > 1$. Let $d_1, d_2, \ldots, d_k$ be positive divisors of n. For a divisor d of n, let us define a subset S_d of S by

$$S_d = \{a \in S : gcd(a, n) = d\}.$$

Then each element of S belongs to exactly one of the subsets $S_{d_1}, S_{d_2}, \ldots, S_{d_k}$ and $S = S_{d_1} \cup S_{d_2} \cup \ldots \cup S_{d_k}$.

Let $d < n$. $a \in S_d \Rightarrow gcd(a, n) = d \Rightarrow a = \lambda d$ and $n = d'd$, where λ is less than $d'(= \frac{n}{d})$ and prime to d'.

Thus S_d contains integers of the type λd, where λ is less than d' and prime to d'. Therefore S_d contains $\phi(d')$ elements.

Since the total number of elements in S is n and they are distributed into distinct and disjoint subsets of S, $n = \sum\limits_{d|n} \phi(d')$, where $dd' = n$.

As d runs through all positive divisors of n, d' does so. Therefore $\sum\limits_{d|n} \phi(d') = \sum\limits_{d'|n} \phi(d') = \sum\limits_{d|n} \phi(d)$. If $n = 1$, $\sum\limits_{d|n} \phi(d) = \phi(1) = 1$. This completes the proof.

To elucidate the proof, let us take $n = 15$. The divisors of 15 are 1, 3, 5 and 15.

$S_1 = \{a : gcd(a, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$;
$S_3 = \{a : gcd(a, 15) = 3\} = \{3, 6, 9, 12\}$;
$S_5 = \{a : gcd(a, 15) = 5\} = \{5, 10\}$;
$S_{15} = \{a : gcd(a, 15) = 15\} = \{15\}$.

S_1 contains $\phi(15)$ elements, S_3 contains $\phi(5)$ elements, S_5 contains $\phi(3)$ elements and S_{15} contains $\phi(1)$ elements.

$\phi(1) = 1, \phi(3) = 2, \phi(5) = 4, \phi(15) = 8$.

$\sum\limits_{d|15} \phi(d) = \phi(1) + \phi(3) + \phi(5) + \phi(15) = 1 + 2 + 4 + 8 = 15$.

3. If $n > 2$, then $\phi(n)$ is an even integer.

Proof. **Case 1.** Let n be a power of 2. Let $n = 2^k$, $k > 1$.

Then $\phi(n) = \phi(2^k) = 2^k(1 - \frac{1}{2}) = 2^{k-1}$, an even integer.

Case 2. Let n be not a power of 2. Then n has an odd prime divisor, say, p. Let $n = p^\alpha q$, where $\alpha \geq 1$ and p, q are prime to each other.

$$\begin{aligned} \text{Then } \phi(n) &= \phi(p^\alpha).\phi(q), \text{ since } p^\alpha, q \text{ are prime to each other} \\ &= p^\alpha(1 - \tfrac{1}{p}).\phi(q) = p^{\alpha-1}(p-1).\phi(q). \end{aligned}$$

Since $(p - 1)$ is even, it follows that $\phi(n)$ is even.

This completes the proof.

Another proof of Euclid's theorem on infinitude of primes.

Let the number of primes be finite and $p_1, p_2, \ldots, p_m$ be the enumeration of all primes. Let $p = p_1 p_2 \ldots p_m$.

Let k be an integer satisfying $2 \leq k \leq p$. Then by the fundamental theorem, k is either a prime, i.e., one of $p_1, p_2, \ldots, p_m$, or k has a prime divisor, say q which is one of $p_1, p_2, \ldots, p_m$.

Thus in any case, $gcd(k, p) > 1$. Therefore every integer k satisfying $1 < k \leq p$ is not prime to p and this gives $\phi(p) = 1$.

But p is clearly an integer > 2 and by the property of the phi function, $\phi(n)$ is even for every integer $n > 2$. We arrive at a contradiction.

Therefore the number of primes is infinite and this completes the proof.

Worked Examples.

1. Find the number of integers less than n and prime to n, when $n =$ 324, 900.

$324 = 2^2.3^4$. Therefore $\phi(324) = 324(1 - \frac{1}{2})(1 - \frac{1}{3}) = 108$.

$900 = 2^2.3^2.5^2$. Therefore $\phi(900) = 900(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 240$.

2. If n be an odd positive integer, prove that $\phi(2n) = \phi(n)$.

Since n is odd, $gcd(2, n) = 1$.

Therefore $\phi(2n) = \phi(2)\phi(n) = \phi(n)$, since $\phi(2) = 1$.

3. If n be an even positive integer, prove that $\phi(2n) = 2\phi(n)$.

Let $n = 2^k.p$, where p is an odd positive integer.

Then $\phi(n) = \phi(2^k).\phi(p) = 2^k(1 - \frac{1}{2}).\phi(p) = 2^{k-1}\phi(p)$ and $\phi(2n) = \phi(2^{k+1}p) = \phi(2^{k+1})\phi(p) = 2^k\phi(p)$. Therefore $\phi(2n) = 2\phi(n)$.