Euler's Totient Function

Recall that $\phi(n)$ counts all the positive integers less than n, and relatively prime to n.

Lemma : (9.2)

For p prime, and all positive integers n,

$$\phi(p^n) = p^{n-1}(p-1)$$

Proof. The positive integers less than or equal to p^n that are not relatively prime to p^n are exactly the multiples of p.

$$1 \cdot p, \quad 2 \cdot p, \quad \ldots, \quad p^{n-1} \cdot p$$

Since there are p^n positive integers less than or equal to p^n, we have:

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

□

Lemma : (9.3)

If $(a, m) = 1$ and $a \equiv b \mod m$, then $(b, m) = 1$.

Proof. By the definition of congruence, we have that

$$a = b + km, \qquad k \in \mathbb{Z}$$

Suppose that $(b, m) = d > 1$, then $d \mid b$ and $d \mid km$, so $d \mid a$. However, this means that $(a, m) > 1$, which contradicts $(a, m) = 1$. □

Corollary : (9.1)

If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then $r_1, r_2, \ldots r_m$ contains exactly $\phi(m)$ elements relatively prime to m.

Proof. The proof of this follows from Lemma 9.3. □

Theorem : (9.2)

The function ϕ is multiplicative.

Proof. Suppose that $(m, n) = 1$ and write the numbers from 1 to mn as

$$\begin{array}{ccccc} 1, & m+1, & 2m+1, & \ldots, & (n-1)m+1 \\ 2, & m+2, & 2m+2, & \ldots, & (n-1)m+2 \\ & & \vdots & & \\ m, & 2m, & 3m, & \ldots, & mn \end{array}$$

If $(m, r) = d > 1$, then no element in in the rth row of the array is relatively prime to mn

$$r, \quad m+r, \quad 2m+r, \quad \ldots, \quad (n-1)m+r$$

This is because if $d \mid m$ and $d \mid r$, then $d \mid (km + r)$ for any k. If $(m, r) = 1$, we claim that there are exactly $\phi(n)$ elements in the rth row of the array that are relatively prime to mn

$$r, \quad m + r, \quad 2m + r, \quad \ldots, \quad (n-1)m + r$$

If this is true, then since there are $\phi(m)$ rows, it will follow that $\phi(nm) = \phi(n)\phi(m)$ Suppose that for $0 \leq k, j < n$ that,

$$km + r \equiv jm + r \mod n$$

Then, since $(m, n) = 1$, we have that

$$\begin{aligned} km &\equiv jm \mod n \\ k &\equiv j \mod n \\ k &= j \end{aligned}$$

If $(m, r) = 1$, then Corollary 9.1 gives that there are exactly $\phi(n)$ elements in the rth row of the array that are relatively prime to n.

$$r, \quad m + r, \quad 2m + r, \quad \ldots, \quad (n-1)m + r$$

From Lemma 9.3, we have that every element in the rth row of the array is relatively prime to m. It follows that the rth row of the array contains exactly $\phi(n)$ elements relatively prime to mn. Since there are $\phi(m)$ such rows, it will follow that

$$\phi(nm) = \phi(n)\phi(m)$$

□

Theorem : (9.3)

If n has a prime power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. then

$$\phi(n) = p_1^{e_1 - 1}(p_1 - 1)\, p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

Proof. Since ϕ is multiplicative by Theorem 9.2, Theorem 7.5 gives us that

$$\phi(n) = \phi(p_1^{e_1})\, \phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$$

Applying Lemma 9.2, gives us the desired result

$$\phi(n) = p_1^{e_1 - 1}(p_1 - 1)\, p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

□

Example

Calculate $\phi(2700)$.

First, $2700 = 2^2 3^3 5^2$, so

$$\begin{aligned} \phi(2700) &= \phi\left(2^2\right) \phi\left(3^3\right) \phi\left(5^2\right) \\ &= 2^1(2-1) \cdot 3^2(3-1) \cdot 5^1(5-1) \\ &= 720 \end{aligned}$$

Corollary : (9.2)

If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Example

Calculate $\phi(2700)$ using the result of Corollary 9.2.

We have that $2700 = 2^2 3^3 5^2$, so

$$\begin{aligned}
\phi(2700) &= 2700\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\
&= 2700\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\
&= \frac{21600}{30} \\
&= 720
\end{aligned}$$