Euler's phi (or totient) function

- **Euler's phi (or totient) function** of a positive integer n is the number of integers in $\{1,2,3,...,n\}$ which are relatively prime to n.
- This is usually denoted $\varphi(n)$.

integer n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

The Euler Phi Function

Theorem: Formula for Φ(n)

Let p be prime, e, m, n be positive integers

1) $\Phi(p) = p-1$

2) $\Phi(p^e) = p^e - p^{e-1}$

3) If $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$,then

$$\Phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$$

Proof for (2):
There are total p^e numbers, subtract the numbers p, 2p, 3p .....(p^(e)-1)*p numbers from the p^e.

Proof of phi(pq)=(p-1) * (q-1):
There are total pq numbers, subtract p,2p,3p.....q*p (total q numbers) and also q,2q,3q.....p*q (total p numbers), but in this we have subtracted pq two times so add it.
pq-p-q+1=(p-1) * (q-1).
Hence proved.

phi(pq)=phi(p)*phi(q); only for p and q are co-prime.

If both are individual prime, then:
phi(p)*phi(q)=(p-1)*(q-1).

Theorem: If **p** is a prime and **a** is a positive integer, then:

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

Proof. We want to calculate the number of non-negative integers less than $n = p^a$ that are relatively prime to n. As in many cases, it turns out to be easier to calculate the number that are *not* relatively prime to n, and subtract from the total. List the non-negative integers less than p^a: 0, 1, 2, …, $p^a - 1$; there are p^a of them. The numbers that have a common factor with p^a (namely, the ones that are not relatively prime to n) are the multiples of p: 0, p, $2p$, …, that is, every pth number. There are thus $p^a/p = p^{a-1}$ numbers in this list, so $\phi(p^a) = p^a - p^{a-1}$.∎

The key principle behind the fermat principle is that, if we multiply an integer (say a) co prime with p, where p is prime, to the Zp, then the set will not change. One to one mapping will exist.

Fermat's Little Theorem

If **a** is an integer , **p** is a prime number and **a** is not divisible by **p**, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof:

Let $S = \{1, 2, 3, \cdots, p-1\}$. Then, we claim that the set $a \cdot S$, consisting of the product of the elements of S with a, taken modulo p, is simply a permutation of S. In other words,

$$S \equiv \{1a, 2a, \cdots, (p-1)a\} \pmod{p}.$$

Clearly none of the ia for $1 \leq i \leq p-1$ are divisible by p, so it suffices to show that all of the elements in $a \cdot S$ are distinct. Suppose that $ai \equiv aj \pmod{p}$. Since $\gcd(a, p) = 1$, by the cancellation rule, that reduces to $i \equiv j \pmod{p}$, which means $i = j$ as $1 \leq i, j \leq p-1$.

Thus, $\mod p$, we have that the product of the elements of S is

$$1a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Cancelling the factors $1, 2, 3, \ldots, p-1$ from both sides, we are left with the statement $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem

Let Φ(n) be Euler's totient function. If n is a positive integer, Φ(n) is the number of integers in the range {1, 2, 3…,n} which are relatively prime to n. If a is an integer and m is a positive integer relatively prime to a, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof:

Consider the set of numbers $A = \{n_1, n_2, ...n_{\phi(m)}\} \pmod{m}$ such that the elements of the set are the numbers relatively prime to m. It will now be proved that this set is the same as the set $B = \{an_1, an_2, ...an_{\phi(m)}\} \pmod{m}$ where $\gcd(a, m) = 1$. All elements of B are relatively prime to m so if all elements of B are distinct, then B has the same elements as A. In other words, each element of B is congruent to one of A. This means that $n_1n_2...n_{\phi(m)} \equiv an_1 \cdot an_2...an_{\phi(m)} \pmod{m} \implies a^{\phi(m)} \cdot (n_1n_2...n_{\phi(m)}) \equiv n_1n_2...n_{\phi(m)} \pmod{m} \implies a^{\phi(m)} \equiv 1 \pmod{m}$ as desired. Note that dividing by $n_1n_2...n_{\phi(m)}$ is allowed since it is relatively prime to m. □