Euler's Totient function

Euler's Totient function Φ (n) for an input n is the count of numbers in {1, 2, 3, …, n-1} that are relatively prime to n, i.e., the numbers whose GCD (Greatest Common Divisor) with n is 1.

Examples :

Φ(1) = 1

gcd(1, 1) is 1

Φ(2) = 1

gcd(1, 2) is 1, but gcd(2, 2) is 2.

Φ(3) = 2

gcd(1, 3) is 1 and gcd(2, 3) is 1

Φ(4) = 2

gcd(1, 4) is 1 and gcd(3, 4) is 1

Φ(5) = 4

gcd(1, 5) is 1, gcd(2, 5) is 1,

gcd(3, 5) is 1 and gcd(4, 5) is 1

Φ(6) = 2

gcd(1, 6) is 1 and gcd(5, 6) is 1,

The Euler's totient function, or phi (φ) function is a very important number theoretic function having a deep relationship to prime numbers and the so-called order of integers. The totient φ(*n*) of a positive integer *n* greater than 1 is defined to be the number of positive integers less than *n* that are coprime to *n*. φ(*1*) is defined to be 1. The following table shows the function values for the first several natural numbers:

n	$\varphi(n)$	numbers coprime to n
1	1	1
2	1	1
3	2	1, 2
4	2	1,3
5	4	1,2,3,4
6	2	1,5
7	6	1,2,3,4,5,6
8	4	1,3,5,7
9	6	1,2,4,5,7,8
10	4	1,3,7,9
11	10	1,2,3,4,5,6,7,8,9,10
12	4	1,5,7,11
13	12	1,2,3,4,5,6,7,8,9,10,11,12
14	6	1,3,5,9,11,13
15	8	1,2,4,7,8,11,13,14

when *n* is a prime number (e.g. 2, 3, 5, 7, 11, 13), $\varphi(n) = n-1$.

But how about the composite numbers? You may also have noticed that, for example, 15 = 3*5 and $\varphi(15) = \varphi(3)*\varphi(5) = 2*4 = 8$. This is also true for 14,12,10 and 6. However, it does not hold for 4, 8, 9. For example, 9 = 3*3 , but $\varphi(9) = 6 \neq \varphi(3)*\varphi(3) = 2*2 = 4$. In fact, this multiplicative relationship is conditional:

when *m* and *n* are coprime, $\varphi(m*n) = \varphi(m)*\varphi(n)$.

The general formula to compute $\varphi(n)$ is the following:

If the prime factorisation of n is given by $n = p_1^{e_1} * ... * p_n^{e_n}$, then $\varphi(n) = n * (1 - 1/p_1) * ... (1 - 1/p_n)$.

For example:

- $9 = 3^2$, $\varphi(9) = 9 * (1-1/3) = 6$
- $4 = 2^2$, $\varphi(4) = 4 * (1-1/2) = 2$
- $15 = 3*5$, $\varphi(15) = 15 * (1-1/3)*(1-1/5) = 15*(2/3)*(4/5) = 8$

Euler’s theorem generalises Fermat’s theorem to the case where the modulus is not prime. It says that:

if *n* is a positive integer and a, n are coprime, then $a^{\varphi(n)} \equiv 1 \mod n$ where $\varphi(n)$ is the Euler's totient function.

Let's see some examples:

- $165 = 15*11$, $\varphi(165) = \varphi(15)*\varphi(11) = 80$. $8^{80} \equiv 1 \mod 165$
- $1716 = 11*12*13$, $\varphi(1716) = \varphi(11)*\varphi(12)*\varphi(13) = 480$. $7^{480} \equiv 1 \mod 1716$

- $\varphi(13) = 12$, $9^{12} \equiv 1 \bmod 13$

We can see that Fermat's little theorem is a special case of Euler's Theorem: for any prime n, $\varphi(n) = n-1$ and any number a $0 < a < n$ is coprime to n. From Euler's Theorem, we can easily get several useful corollaries. First:

if n is a positive integer and a, n are coprime, then $a^{\varphi(n)+1} \equiv a \bmod n$.

This is because $a^{\varphi(n)+1} = a^{\varphi(n)}*a$, $a^{\varphi(n)} \equiv 1 \bmod n$ and $a \equiv a \bmod n$, so $a^{\varphi(n)+1} \equiv a \bmod n$. From here, we can go even further:

if n is a positive integer and a, n are coprime, $b \equiv 1 \bmod \varphi(n)$, then $a^b \equiv a \bmod n$.

If $b \equiv 1 \bmod \varphi(n)$, then it can be written as $b = k*\varphi(n)+1$ for some k. Then $a^b = a^{k*\varphi(n)+1} = (a^{\varphi(n)})^k*a$. Since $a^{\varphi(n)} \equiv 1 \bmod n$, $(a^{\varphi(n)})^k \equiv 1^k \equiv 1 \bmod n$. Then $(a^{\varphi(n)})^k*a \equiv a \bmod n$. This is why RSA works.