Euler ϕ-function

Definition. Let $\phi(n)$ denote the number of integers between 1 and $n-1$ that are relatively prime to n.

Theorem 1 *If* $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ *then*

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

Proof. (k=3) $n = p_1^{n_1} p_2^{n_2} p_3^{n_3}$

#'s $\leq n$

divisible by p_1

divisible by p_2

divisible by p_3

$$\begin{aligned}
\phi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1p_2} + \frac{n}{p_1p_2} + \frac{n}{p_2p_3} - \frac{n}{p_1p_2p_3} \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)
\end{aligned}$$

Euler ϕ-function: Examples

1. Compute $\phi(12)$.

$$\phi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$$

The 4 numbers less than 12 that are relatively prime to 12 are:

$$\boxed{1},\ \cancel{2},\ \cancel{3},\ \cancel{4},\ \boxed{5},\ \cancel{6},\ \boxed{7},\ \cancel{8},\ \cancel{9},\ \cancel{1}0,\ \boxed{11}$$

2. Compute $\phi(p)$, where p is any prime number.

$$\phi(p) = p\left(1-\frac{1}{p}\right) = p-1.$$

3. Compute $\phi(pq)$, where p and q are distinct prime numbers.

$$\phi(pq) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = (p-1)(q-1).$$

The Euler-Fermat Theorem

Theorem 2 *If a and m are relatively prime then*

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

Proof. Let $\{x_1, x_2, \ldots, x_k\}$ be the set of numbers less than m that are relatively prime to m ($k = \phi(m)$). Since a is relatively prime to m, a must have a multiplicative inverse mod m. Therefore,

$$ax \equiv ay \pmod{m} \quad \Leftrightarrow \quad x \equiv y \pmod{m}$$

and thus

$$\{ax_1, ax_2, \ldots, ax_k\} = \{x_1, x_2, \ldots, x_k\}.$$

We conclude that

$$\begin{aligned} a^k x_1 x_2 \cdots x_k &= ax_1 ax_2 \cdots ax_k \\ &\equiv x_1 x_2 \cdots x_k \pmod{m} \end{aligned}$$

But since each of the x_i's is invertible, we have

$$a^k \equiv 1 \pmod{m}$$

as desired.

In other words, the Euler-Fermat Theorem says that

$$\boxed{a^x \equiv a^{x \bmod \phi(m)} \bmod m}$$

Euler-Fermat: Examples

1. Compute 2^{1023} mod 17.

   Since $\phi(17) = 16$, we have

   $$2^{1023} = 2^{64\times 16-1} \equiv 2^{-1} \equiv 9 \mod 17$$

2. Compute 10^{3252} mod 5607

   Given that $5607 = 3^2 \cdot 7 \cdot 89$, we may compute $\phi(5607) = 3168$. Therefore

   $$10^{3252} \equiv 10^{84} \mod 5607$$

   Next write 84 as a sum of powers of 2:

   $$84 = 64 + 16 + 4.$$

   Compute

   $$\begin{aligned} 10^2 &= 100 \\ 10^4 &\equiv 100^2 \equiv 4393 \\ 10^8 &\equiv 4393^2 \equiv 4762 \\ 10^{16} &\equiv 4762^2 \equiv 1936 \\ 10^{32} &\equiv 1936^2 \equiv 2620 \\ 10^{64} &\equiv 2620^2 \equiv 1432 \end{aligned}$$

   Therefore,

   $$10^{84} = 10^{64+16+4} \equiv 1432 \times 1936 \times 4393 \equiv 64$$

Exercises:

1. Compute $\phi(50910363)$ knowing that

$$50910363 = 3^4 \times 7^2 \times 101 \times 127.$$

2. Use your answer from the previous question to compute

$$2^{28576807} \;\; mod \;\; 50910363.$$

3. Compute 3^{999} mod 143.