

Euler's Phi function and Euler's Theorem

Sankita Patel

Sardar Vallabhbhai National Institute of Technology

sjp@coed.svnit.ac.in

February 13, 2024

Euler's Phi-Function

- ▶ Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function plays a very important role in cryptography.
- ▶ The function finds the number of integers that are both smaller than n and relatively prime to n
- ▶ Some rules :
 1. $\phi(1) = 0$
 2. $\phi(p) = p - 1$, if p is prime
 3. $\phi(m \times n) = \phi(m) \times \phi(n)$, if m and n are coprime
 4. $\phi(p^e) = p^e - p^{e-1}$, if p is prime

Euler's Phi-Function...

- ▶ We can combine the previous four rules to find the value of $\phi(n)$.
- ▶ For example, if n can be factored as, $n = p_1^{e_1} \times p_2^{e_2} \times \dots \times p_k^{e_k}$ then we can combine the third and the fourth rule to find,
$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \dots \times (p_k^{e_k} - p_k^{e_k-1})$$

The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n .

Euler's Phi-Function : Examples

- ▶ What is the value of $\phi(13)$?

Solution : Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

- ▶ What is the value of $\phi(10)$?

Solution : We can use the third rule:

$\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

- ▶ What is the value of $\phi(240)$?

Solution : We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

$$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$

- ▶ Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$????

Solution: No. The third rule applies when m and n are relatively prime. Here $49 = 7^2$. We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

- ▶ What is the number of elements in Z_{14}^* ?

Solution : It is $\phi(14) = 6$

Euler's Theorem

- ▶ First Version: If a and n are coprime,

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

- ▶ Second Version: Removes the condition that a and n should be coprime.

$$a^{k\phi(n)+1} \equiv a \pmod{n}$$

The second version of Euler's theorem is used in the RSA cryptosystem

Euler's Theorem: Examples

- Find the result of $6^{24} \bmod 35$

Solution: We have $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$.

- Find the result of $20^{62} \bmod 77$

Solution: If we let $k = 1$ on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)(20^{\phi(77)+1} \bmod 77)$$

$$\bmod 77 = (20)(20) \bmod 77 = 15.$$

References

1. Forouzan, Behrouz A. "Cryptography & Network Security. 2011."

Last updated by S J Patel on February 13, 2024