Euler Totient Function

Shivansh Subramanian

22nd May 2020

1 Introduction

$\phi(x)$ is defined as the number of integers d less than or equal to x such that gcd(d, x) = 1

2 Theorems

2.1

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

2.2

$$\phi(p^k) = p^k - p^{k-1} = p^k \times [1 - \frac{1}{p}]$$

Proof
We know that for gcd(n, p^k) = 1, n must not be divisible by p
$1p, 2p, ...(p^{k-1})p$ are all divisible by p
Therefore, there are p^{k-1} numbers divisible by p, hence

$$\phi(p^k) = p^k - p^{k-1} = p^k \times [1 - \frac{1}{p}]$$

2.3 Multiplicativeness

If gcd(m,n) = 1, then

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

Proof:
All numbers between 1 and mn can be written as

$$\begin{array}{cccccccccc}
1 & 2 & . & . & . & r & . & . & m \\
m+1 & m+2 & . & . & . & m+r & . & . & 2m \\
. & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . \\
(n-1)m+1 & (n-1)m+2 & . & . & . & (n-1)m+r & . & . & nm
\end{array}$$

We know $\phi(mn)$ is equal to number of entries in this array such that the element is relatively prime to mn

$$gcd(km+r,m) = gcd(r,m)$$

This implies that the numbers in a given column are relatively prime to m iff r is relatively prime to m, therefore $\phi(m)$ such numbers exist in each row
Now in such a row where gcd(r,m) = 1, we have n elements

$$r, m+r, 2m+r, ...(n-1)m+r$$

Here, we have to show that there exist no two numbers such that they give the same remainder on being divided by n
Assume

$$km+r \equiv (lm+r)modn$$

$$km \equiv (lm)modn$$

Since m and n are relatively prime

$$k \equiv lmodn$$

Therefore it is not possible for different k and l to give same remainder.
This implies that all the elements in row map to 1 , 2 . . (n-1) as modulo n
Say element s maps to t modulo n

$$s \equiv tmodn$$

We can easily prove that gcd(s, n) = 1 iff gcd(t, n) = 1
Which implies $\phi(n)$ such integers exist in each row
Hence we conclude that

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

2.4

If

$$n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$$

Then

$$\phi(n) = n \prod_{x=1}^{r} [1 - \frac{1}{p_x}]$$

Proof:
Since we know $\phi(n)$ is multiplicative

$$\phi(n) = \prod_{x=1}^{r} \phi(p_x^{k_x})$$

From Theorem 2.2

$$\phi(n) = \prod_{x=1}^{r} p_x^{k_x} \times [1 - \frac{1}{p_x}]$$

$$\phi(n) = n \prod_{x=1}^{r} [1 - \frac{1}{p_x}]$$

2.5

For any positive integer n

$$\sqrt{\frac{n}{2}} \leq \phi(n) \leq n$$

Proof:
The part of proving $\phi(n) \leq n$ is trivial, we look at the other part then
Let

$$n = p_1 p_2 ... p_k q_1^{a_1} q_2^{a_2} .. q_l^{a_l}$$

Let

$$s = p_1 p_2 .. p_k$$

$$t = q_1^{a_1} q_2^{a_2} .. q_l^{a_l}$$

We know

$$\phi(n) = \phi(st) = \phi(s)\phi(t)$$

$$\frac{\phi(n)}{\sqrt{n}} = \frac{\phi(s)}{\sqrt{s}} \frac{\phi(t)}{\sqrt{t}}$$

Then

$$\frac{\phi(s)}{\sqrt{s}} = \prod_{x=1}^{k} \frac{p_x - 1}{\sqrt{p_x}}$$

For all p ≥ 2 , we have $\frac{p-1}{\sqrt{p}} > 1$
Therefore there are two cases, where m contains only 2 and where n contains 2 and some other factors
The former cases is trivial, and since in the latter case the fraction for other factors other than 2 is greater than 1, we can easily prove

$$\frac{\phi(s)}{\sqrt{s}} \geq \frac{1}{\sqrt{2}}$$

$$\frac{\phi(t)}{\sqrt{t}} = \prod_{x=1}^{l} q_x^{a_x - 1}(q_x - 1) \geq 1$$

Therefore we arrive at the conclusion

$$\sqrt{\frac{n}{2}} \leq \phi(n) \leq n$$

2.6

If

$$n = p_1^{a_1} p_2^{a_2} .. p_r^{a_r}$$

Then

$$\phi(n) \geq \frac{n}{2^r}$$

Proof:
Since we know ϕ is multiplicative

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_r^{a_r})$$

Since for any p

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

We know that

$$\frac{1}{2} \geq \frac{1}{p}$$

Therefore

$$\phi(p^a) = p^a[1 - \frac{1}{p}] \geq \frac{p^a}{2}$$

$$\phi(n) \geq \frac{n}{2^r}$$

2.7

If n is a composite number,

$$\phi(n) \leq n - \sqrt{n}$$

Proof:
Let p be the smallest prime divisor of n, then
Let

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

Where p = p_1 Then

$$\phi(n) = n \prod_{k=1}^{r} [1 - \frac{1}{p_k}]$$

Assume such a n' that p $\nmid$ n. Then

$$\phi'(n') = n' \prod_{k=2}^{r} [1 - \frac{1}{p_k}]$$

And

$$\phi'(n') \leq n'$$

$$\phi'(n') \times p^{a_1} \leq n' \times p^{a_1}$$

$$\phi'(n') \times p^{a_1} \leq n$$

$$\phi'(n') \times p^{a_1} \times [1 - \frac{1}{p}] \leq n \times [1 - \frac{1}{p}]$$

$$\phi(n) \leq n \times [1 - \frac{1}{p}]$$

And since

$$p \leq \sqrt{n}$$

$$\phi(n) \leq n \times [1 - \frac{1}{p}] \leq n \times [1 - \frac{1}{\sqrt{n}}]$$

$$\phi(n) \leq n - \sqrt{n}$$