

(7.2) Euler's Phi-function

Defⁿ (7.1) For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n .

(eg) $\phi(30) = 8$

(1, 7, 11, 13, 17, 23, 29)

$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2$

Remark $\phi(n) = n-1 \iff n$ is prime.

Theorem (7.1) If p is prime and $k > 0$

then $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$

(pf) Since $\gcd(n, p^k) = 1 \iff p \nmid n$

(take $n \geq 1$)

take $n = 3$

$5^2 = p^2$

$\gcd(3, 5^2) = 1$

$\iff 5 \nmid 3$

$1 \& 5^2$

$\{5, 2 \times 5, 3 \times 5, 4 \times 5, \dots, 5 \times 5\}$

$\therefore$ there are p^{k-1} integers between $1 \& p^k$ divisible by p
i.e. $p, 2p, 3p, \dots, (p^{k-1})p$

thus, the set $\{1, 2, \dots, p^k\}$ contains exactly $p^k - p^{k-1}$ integers that are relatively prime to p^k

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

(eg) $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$

$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$

Similarly, $\gcd(a, c) = 1$

Conversely, Assume that $\gcd(a, b) = 1$ & $\gcd(a, c) = 1$

Suppose that $\gcd(a, bc) = d_1 > 1$

Since $d_1 > 1$

$\therefore d_1$ must have prime divisor p .

Since $d_1 | bc$

$$\Rightarrow p | d_1 \text{ \& } d_1 | bc$$

$$\Rightarrow p | bc$$

$$\Rightarrow p | b \text{ or } p | c$$

$\therefore p | b$ & $p | a$

$$\Rightarrow \gcd(a, b) \geq p \text{ (prime)}$$

which is a contradiction since $\gcd(a, b) = 1$

$$\therefore \gcd(a, bc) = 1$$

Theorem (7.2) The function ϕ is multiplicative function
(statement only)

Theorem (7.3) If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) (p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1})$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

(pf) we will use induction on r
i.e. number of distinct prime factor n .

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

$$\text{For } r=1, \quad n = p_1^{k_1}$$

by thm (7.1) (pf) (here)

$$\text{we get } \phi(n) = \phi(p_1^{k_1}) = p_1^{k_1} \left(1 - \frac{1}{p_1}\right)$$

Suppose that it holds for $r=i$

$$\text{Since } \gcd(p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$$

(2)

$$\phi(p_1^{k_1} p_2^{k_2} \dots p_i^{k_i} \dots p_{i+1}^{k_{i+1}})$$

$$= \phi(p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}) \phi(p_{i+1}^{k_{i+1}}) \quad (\because \phi \text{ is multiplicative})$$

$$= \phi(p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}) (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}) \quad (\text{by thm 7.1})$$

Since result is true for $s=i$

$$= (p_1^{k_1} - p_1^{k_1-1}) (p_2^{k_2} - p_2^{k_2-1}) \dots (p_i^{k_i} - p_i^{k_i-1}) (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

$\therefore$ Result is true for $s=i+1$

$$\therefore \phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

(ex) $\phi(360)$

the prime factor decomposition of 360

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$\phi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$$

$$= 96$$

Theorem (7.4) For $n > 2$, $\phi(n)$ is an even integer

(pf) let Assume that $n = 2^k$ where $k \geq 2$

(By thm 7.3)

$$\phi(n) = \phi(2^k)$$

$$= 2^k - 2^{k-1}$$

$$= 2^{k-1} (2-1)$$

$$= 2^{k-1}$$

Since $k \geq 2$ then 2^{k-1} is always even

$$\Rightarrow \phi(2^k) = 2^{k-1} \text{ is even}$$

(or) (ii) If $n \neq 2^k$ and $n > 2$

then n is divisible by some odd prime

let $n = p^k \cdot m$ where p is odd prime

$$\& \text{gcd}(p^k, m) = 1$$

$$= \phi(p^k) \phi(m) \quad \text{when } \gcd(p^k, m) = 1$$

$$= \phi(p^k) \phi(m)$$

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

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

Since p is odd & $p-1$ is even number (multiply by even number)
 $\Rightarrow p^{k-1} (p-1) \phi(m)$ is an even number (as $p-1$ is even) (so, even number)

$$\Rightarrow \phi(n) = p^{k-1} (p-1) \phi(m) \text{ is even number.}$$

Example (7.2) $Q-1, 2, 4, 6, 8, 13, 14, 16$

(Q-1) Calculate $\phi(1001)$, $\phi(5040)$ & $\phi(3600)$

sol) $\phi(1001) = 1001 \times 13 \times 7$

$$= 1001 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{17}\right)$$

$$= 720$$

$$5040 = 2^4 \times 3^2 \times 5 \times 7$$

$$\phi(5040) = 5040 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right)$$

$$= 1152$$

$$3600 = 2^5 \times 3^2 \times 5^2$$

$$\phi(3600) = 3600 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= 9600$$

(Q-2) Verify the equality $\phi(n) = \phi(n+1) = \phi(n+2)$ holds when $n = 5186$

sol) $5186 = 2 \times 2593$

$$\phi(5186) = \phi(2) \phi(2593)$$

$$= 1 \times 2592$$

$$= 2592$$

$$\phi(5188) = \phi(2^2 \times 1297)$$

$$= \phi(2^2) \phi(1297)$$

$$= 2 \times 1296 = 2592$$

$$5187 = 5186 + 1$$

$$\phi(5187) = \phi(3 \times 7 \times 13 \times 19)$$

$$= \phi(3) \phi(7) \phi(13) \phi(19)$$

$$= 2 \times 6 \times 12 \times 18$$

$$= 2592$$

(7.3) Euler's theorem

(lemma) let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \dots, a_{\phi(n)}$ are positive integers less than n & relatively prime to n , then

$aa_1, aa_2, \dots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \dots, a_{\phi(n)}$ in some order.

(pt) let, if possible suppose $aa_i \equiv aa_j \pmod{n}$; $1 \leq i < j \leq \phi(n)$
 $\Rightarrow a_i \equiv a_j \pmod{n}$ (by cancellation law)
 which is contradicted as $1 \leq i < j \leq \phi(n)$

we get No two of the integers $aa_1, aa_2, \dots, aa_{\phi(n)}$ are congruent modulo n .

Since $\gcd(a, n) = 1$ & $\gcd(a_i, n) = 1$ (given)

$\Rightarrow \gcd(aa_i, n) = 1$ (by lemma in 7.2)

fixing on a particular aa_i (say b)

i.e. $\exists$ a unique integer b

where $0 \leq b < n$

for which $aa_i \equiv b \pmod{n}$

$\Rightarrow \gcd(b, n) = \gcd(aa_i, n) = 1$

$\therefore b$ must be one of integers $a_1, a_2, \dots, a_{\phi(n)}$

$\therefore aa_1, aa_2, \dots, aa_{\phi(n)}$

& $a_1, a_2, \dots, a_{\phi(n)}$

are identical (modulo n) in certain order.

$\gcd(a, b) = 1$

$\Rightarrow \gcd(a, b) = 1$

& $\gcd(a, n) = 1$

using (lemma)

$a = b \pmod{n}$

$\Rightarrow \gcd(a, b) = \gcd(b, n)$

(as $\gcd(a, n) = 1 = \gcd(aa_i, n) = \gcd(b, n)$)

only possible

(7.9) Some properties of PHI-Function

theorem (A.6) (Gauss)

For each positive integer $n \geq 1$

$$n = \sum_{d|n} \phi(d)$$

the sum being extended over all positive divisors of n .

(pf) (Two proof are given)
(Here, first proof)

If $n=1$

$$\text{then } \sum_{d|n} \phi(d) = \phi(1) = 1 = n$$

Assuming that $n > 1$

let us consider the number-theoretic function

$$F(n) = \sum_{d|n} \phi(d)$$

we know that ϕ is multiplicative

then by theorem 6.4, we get F is also multiplicative.

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is prime factorization of n ,

$$\begin{aligned} \text{then } F(n) &= F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) \\ &= F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r}) \end{aligned}$$

For each value of i

$$F(p_i^{k_i}) = \sum_{d|p_i^{k_i}} \phi(d)$$

$$= \phi(1) + \phi(p_i) + \phi(p_i^2) + \phi(p_i^3) + \dots + \phi(p_i^{k_i})$$

$$= 1 + (p_i - 1) + (p_i^2 - p_i) + (p_i^3 - p_i^2) + \dots + (p_i^{k_i} - p_i^{k_i-1})$$

$$= p_i^{k_i}$$

$$\therefore F(n) = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = n$$

$$\Rightarrow n = \sum_{d|n} \phi(d)$$

Another proof of Gauss from Book

Sd (type) (from Book)

Theorem (7.7) For $n > 1$, the sum of positive integers less than n & relatively prime to n is $\frac{1}{2} n \phi(n)$.

(pf) let $a_1, a_2, \dots, a_{\phi(n)}$ be positive integers less than n & relatively prime to n .

Now $\gcd(a_i, n) = 1 \Leftrightarrow \gcd(n - a_i, n) = 1$

we have

$$\begin{aligned} a_1 + a_2 + \dots + a_{\phi(n)} &= (n - a_1) + (n - a_2) + \dots + (n - a_{\phi(n)}) \\ &= n - a_1 + n - a_2 + \dots + n - a_{\phi(n)} \\ &= \underbrace{\phi(n)}_{\text{times}} n - (a_1 + \dots + a_{\phi(n)}) \end{aligned}$$

$$\Rightarrow 2(a_1 + \dots + a_{\phi(n)}) = \phi(n) \cdot n$$

$$\Rightarrow a_1 + \dots + a_{\phi(n)} = \frac{\phi(n) \cdot n}{2}$$

$$= \frac{1}{2} n \cdot \phi(n)$$

$$S = \{a_1, a_2, \dots, a_{\phi(n)}\}$$

$$\text{coprime } \& \< n$$

$$\gcd(a_i, n) = 1 \& a_i \in S$$

$$\gcd(a_{\phi(n)}, n) = 1 \&$$

$$a_{\phi(n)} \in S$$

$$\gcd(a_i, n) = \gcd(n - a_i, n)$$

$$\Rightarrow n - a_i \in S \forall 1 \leq i \leq \phi(n)$$

$$a_1 + a_2 + \dots + a_{\phi(n)} = (n - a_1) + \dots + (n - a_{\phi(n)})$$

$$\text{--- (same as above)}$$

(Ex) (7.4) $n = 30$

$$\phi(30) = \phi(2 \times 3 \times 5)$$

$$= \phi(2) \phi(3) \phi(5)$$

$$= 1 \times 2 \times 4 = 8$$

Integers less than & relatively prime to n ($n = 30$)

$$1, 7, 11, 13, 17, 19, 23, 29$$

So, Sum is $1 + 7 + 11 + 13 + 17 + 19 + 23 + 29$

$$= 120$$

$$\text{check Sum} = \frac{1}{2} n \phi(n) = \frac{1}{2} (30) \times 8 = 120$$

(7.8) For any positive integer n

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

(pf) we know that

$$F(n) = \sum_{d|n} \phi(d)$$

By Gauss theorem (7.8)

$$F(n) = n = \sum_{d|n} \phi(d) \quad - (1)$$

By Mobius Inversion formula

$$F(n) = \sum_{d|n} g(d)$$

then $\left| f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \right|$ formula here $f = \phi$ function

$$\Rightarrow \phi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} \quad (\text{use } (1))$$
$$= n \sum_{d|n} \frac{\mu(d)}{d} \quad (\text{Hence Proved})$$

(ex) $n=10$,

$$10 \sum_{d|10} \frac{\mu(d)}{d} = 10 \left[\mu(1) + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10} \right]$$
$$= 10 \left[(1) + \frac{(-1)}{2} + \frac{(-1)}{5} + \frac{(-1)^2}{10} \right]$$
$$= 10 \left[1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10} \right]$$
$$= 10 \times \frac{2}{5} = 4 = \phi(10)$$