



# Chapter 7

## Multiplicative Functions

---

邱錫彥 老師



# Contents

---

7.1 The Euler Phi-function.....	3
7.2 The sum and number of divisors.....	20
7.3 Perfect numbers and Mersenne primes.....	25



## 7.1 The Euler Phi-function

- Def : An *arithmetic function* is a function that is defined for all **positive integers**.
- Def : An arithmetic function is called *multiplicative* if  $f(mn)=f(m)f(n), \forall (m, n) = 1$ .  
It is called **completely multiplicative** if  $f(mn)=f(m)f(n), \forall m, n \in \mathbb{Z}^+$



- 
- Ex:  $f(n)=1$  is completely multiplicative and hence also multiplicative.

$$\because \forall m, n \in \mathbb{Z}^+, f(m \times n) = 1, f(m) = 1, f(n) = 1 \\ \Rightarrow f(m \times n) = f(m) \times f(n).$$

$g(n)=n$  is completely multiplicative,

$$\because g(m \times n) = m \times n = g(m) \times g(n), \forall m, n \in \mathbb{Z}^+$$



- Thm : If  $n = P_1^{a_1} P_2^{a_2} \dots P_s^{a_s}$ , where  $P_i$  is prime,  
 $\forall 1 \leq i \leq s$ , and if  $f$  is a multiplicative function,  
then  $f(n) = f(P_1^{a_1}) f(P_2^{a_2}) \dots f(P_s^{a_s})$

- Proof :

1. If  $s=1$ , i.e.,  $n = P_1^{a_1}$ , then  $f(n) = f(P_1^{a_1})$ .

2. Suppose that the theorem is true for  $s=k$ .

Let  $n = P_1^{a_1} \dots P_k^{a_k} P_{k+1}^{a_{k+1}}$ ,  $\therefore (P_1^{a_1} \dots P_k^{a_k}, P_{k+1}^{a_{k+1}}) = 1$ ,

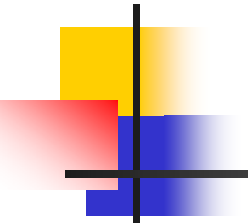
$f(n) = f(P_1^{a_1} \dots P_k^{a_k} P_{k+1}^{a_{k+1}}) f(P_{k+1}^{a_{k+1}}) = f(P_1^{a_1}) \dots f(P_k^{a_k}) f(P_{k+1}^{a_{k+1}})$

the theorem is also true for  $s=k+1$



- Thm : If  $p$  is prime, then  $\phi(p)=p-1$ . Conversely, if  $p \in \mathbb{Z}^+$  and  $\phi(p)=p-1$ , then  $p$  is prime.
- Proof: (1) If  $p$  is prime, then  $1, 2, \dots, p-1$  are relatively prime to  $p$  and less than  $p$ , thus  $\phi(p)=p-1$ .  
(2) Suppose  $p$  is composite, then  $\exists d, 1 < d < p$ , such that  $d \mid p$ , i.e.,  $(d, p) \neq 1$ .  
 $\Rightarrow \phi(p) \leq p-2$ .  
 $\therefore$  if  $\phi(p)=p-1$ , then  $p$  must be prime.

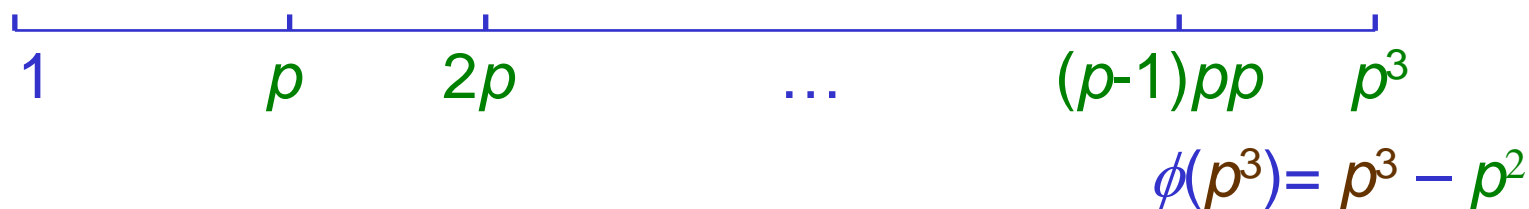
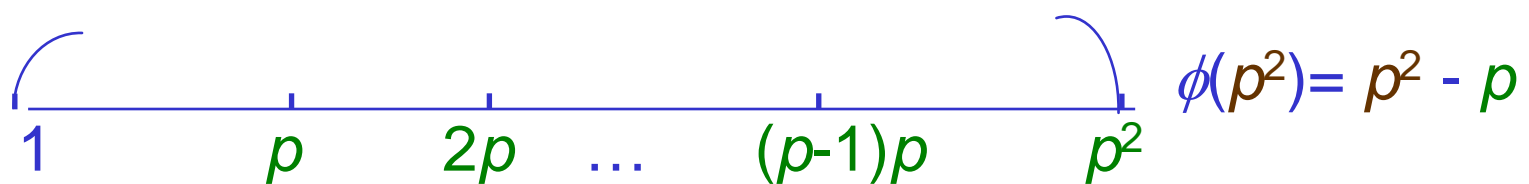


- 
- Thm : Let  $p$  be a prime and  $a \in \mathbb{Z}^+$  ,  
then  $\phi(p^a) = p^a - p^{a-1}$

- Proof: Since  $p$  is prime,  
we know positive integers  $int$  less than  $p^a$   
and  $(int, p^a) \neq 1$  are the integers  $int = kp$ ,  
where  $1 \leq k \leq p^{a-1}$ .  
 $\therefore \phi(p^a) = p^a - p^{a-1}$ .



- There are  $p$  integers that are less than or equal to  $p^2$  and not relatively prime to  $p^2$



- Ex :  $\phi(5^3) = 5^3 - 5^2 = 100$ .





Ex : Find  $\phi(36)$ .

<sol>:  $\because 36 = 4 \times 9$  and  $(4, 9) = 1$

	column									
row	1	2	3	4	5	6	7	8	9	
1	1	5	9	13	17	21	25	29	33	→ relatively prime to 4
2	2	6	10	14	18	22	26	30	34	
3	3	7	11	15	19	23	27	31	35	→ relatively prime to 4
4	4	8	12	16	20	24	28	32	36	

$\therefore$  there are  $\phi(4)$  rows relatively prime to 4

$1=19 \pmod{9}$ ,  $13=31 \pmod{9}$ ,  $25=7 \pmod{9}$

$5=23 \pmod{9}$ ,  $17=35 \pmod{9}$ ,  $29=11 \pmod{9}$

there are  $\phi(9)$  columns relatively prime to 9.

$$\therefore \phi(36) = \phi(4)\phi(9) = 2 \times 6 = 12$$



- Thm : Let  $m, n \in \mathbb{Z}^+$  and  $(m, n) = 1$ . Then

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

- Fact 1. Let  $(m, n) = 1$ .

Then  $(a, mn) = 1$  iff  $(a, m) = 1$  and  $(a, n) = 1$ .

2. If  $(r, m) = 1$ , then  $(im + r, m) = 1$ .

3. Thm 3.6: If  $\{r_1, r_2, \dots, r_m\}$  is a complete system of residue modulo  $m$  and  $(a, m) = 1$ , then

$\{ar_1 + b, ar_2 + b, \dots, ar_m + b\}$  is also

a complete system of residue modulo  $m$ ,  $\forall b \in \mathbb{Z}$ .



- Proof: The positive integers not exceeding  $mn$  are listed as follows.

	1	$m+1$	...	$(n-1)m+1$
	2	$m+2$	...	$(n-1)m+2$
	⋮	⋮	...	⋮
$m$ rows	$r$	$m+r$	...	$(n-1)m+r$
	⋮	⋮	...	⋮
	$m$	$2m$	...	$mn$
	$n$ columns			

A decorative graphic on the left side of the slide consists of overlapping yellow, red, and blue squares with a black crosshair.

---

- Proof: (Cont.)

By fact 2, we have  $\phi(m)$  rows that are relatively prime to  $m$ .

By fact 3, we have  $\phi(n)$  columns that are relatively prime to  $n$  in each row of  $\phi(m)$  rows.

By fact 1, we have  $\phi(m)\phi(n)$  integers that are relatively prime to  $mn$ .

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



- Thm: Let  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ , where  $p_i$  is prime and  $a_i \in \mathbb{Z}^+, \forall 1 \leq i \leq k$ , then
$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

- Proof:  $\because \phi(n)$  is multiplicative,
$$\begin{aligned} \therefore \phi(n) &= \phi(p_1^{a_1}) \phi(p_2^{a_2}) \dots \phi(p_k^{a_k}) \\ &= (p_1^{a_1} - p_1^{a_1-1}) (p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) \\ &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

A decorative graphic in the top left corner features a vertical black line intersecting a horizontal black line. To the left of the vertical line are three overlapping squares: a yellow one at the top, a red one in the middle, and a blue one at the bottom. The squares have a gradient effect, fading towards the right.

■ Remark: Let  $p$ ,  $q$ ,  $r$  be primes. Then

1.  $\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$

2.  $\phi(pqr) = \phi(p)\phi(q)\phi(r) = (p-1)(q-1)(r-1)$

3.  $\phi(p^2q) = \phi(p^2)\phi(q) = (p^2 - p)(q-1)$   
 $\neq (p^2 - 1)(q-1)$



- Thm: Let  $n$  be a positive integer greater than 2.  
Then  $\phi(n)$  is even.

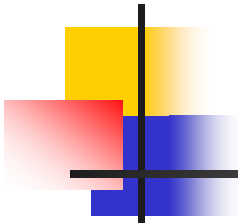
- Proof: If  $n$  is a positive integer greater than 2,  
then the prime-power factorization of  
 $n = p_1^{a_1} \cdots p_s^{a_s}$ ,  $\exists p_j > 2, \ni p_j - 1$  is even.  
 $\therefore \phi(n) = \phi(p_1^{a_1}) \phi(p_2^{a_2}) \cdots \phi(p_s^{a_s})$   
 $= p_1^{a_1-1} (p_1 - 1) \cdots p_s^{a_s-1} (p_s - 1)$  is even.  
 $n = 2^a, a > 1, \phi(n) = 2^a - 2^{a-1}$



- Def : Let  $f$  be an arithmetic function, then  $\sum_{d|n} f(d)$  represents the sum of the value of  $f$  at all the positive divisor of  $n$ .
- Ex :  $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$   
 $\because 1|12, 2|12, 3|12, 4|12, 6|12, 12|12.$
- Property :  $\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right)$





A decorative graphic on the left side of the slide consists of overlapping colored squares (yellow, red, blue) and a black crosshair.

■ Ex :  $\sum_{d|12} d = 1 + 2 + 3 + 4 + 6 + 12 = 28$

$$\sum_{d|12} \frac{12}{d} = 12 + 6 + 4 + 3 + 2 + 1 = 28$$

$$\begin{aligned} \sum_{d|12} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12 \end{aligned}$$



■ Thm : Let  $n \in \mathbb{Z}^+$ , then  $\sum_{d|n} \phi(d) = n$ .

■ Proof : Let  $C_d = \{ m \mid 1 \leq m \leq n \text{ and } (m, n) = d \}$ .

Then  $m \in C_d$  iff  $(m/d, n/d) = 1$

$\therefore |C_d|$  = the number of positive integers not exceeding  $n/d$  that are relatively prime to  $n/d$

$\therefore |C_d| = \phi(n/d)$

$\therefore C_{d_1} \cap C_{d_2} = \emptyset$  if  $d_1 \neq d_2$

$\therefore$  If we divided the integers 1 to  $n$  into  $C_d$ , and  $d \mid n$ , then

$$n = \sum_{d|n} |C_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$



- Ex : Let  $n = 18$ , and classes  $C_d$  contains those integers  $m$  with  $(m, 18) = d$ . Then

$$C_1 = \{1, 5, 7, 11, 13, 17\} \quad |C_1| = \phi(18/1) = \phi(18)$$

$$C_2 = \{2, 4, 8, 10, 14, 16\} \quad |C_2| = \phi(9)$$

$$C_3 = \{3, 15\}, \quad |C_3| = \phi(6)$$

$$C_6 = \{6, 12\} \quad |C_6| = \phi(3)$$

$$C_9 = \{9\} \quad |C_9| = \phi(2)$$

$$C_{18} = \{18\} \quad |C_{18}| = \phi(1)$$



## 7.2 The Sum and Number of Divisors

- Def: The *sum of divisors function*, denoted by  $\sigma$ , is defined by setting  $\sigma(n)$  equal to the **sum** of all the **positive divisors** of  $n$ .

$$\text{i.e. } \sigma(n) = \sum_{d|n} d$$

- Def: The *number of divisor function*, denoted by  $\tau$ , is defined by setting  $\tau(n)$  equal to the **number** of **positive divisor** of  $n$ .

$$\text{i.e. } \tau(n) = \sum_{d|n} 1$$

- Remark: If  $n$  is prime then  $\tau(n) = 2$ ,  $\sigma(n) = n + 1$
- Thm: If  $f$  is multiplicative, then  $F(n) = \sum_{d|n} f(d)$  is also **multiplicative**.



- Proof: To show that  $F$  is multiplicative, we need to show that if  $(m, n) = 1$ , then  $F(mn) = F(m)F(n)$ .  
Let  $(m, n) = 1$ , then

$$F(mn) = \sum_{d|mn} f(d) \rightarrow \text{by definition}$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2) \rightarrow \text{if } d | mn, \text{ then } \exists d_1 | m \text{ and}$$

$$d_2 | n, (d_1, d_2) = 1 \ni d_1d_2 = d$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) \rightarrow f \text{ is multiplicative}$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2)$$

$$= F(m)F(n) \quad 7-21$$

A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

■ Corollary: The function of  $\sigma$  and  $\tau$  are multiplicative.

■ Proof: Let  $f(n) = n$  and  $g(n) = 1$ . Both  $f$  and  $g$  are multiplication.

$$\because \sigma(n) = \sum_{d|n} f(d) \text{ and } \tau(n) = \sum_{d|n} g(d) ,$$

$\therefore \sigma$  and  $\tau$  multiplicative.

■ Problem: Given  $n$ , how to find  $\sigma(n)$  and  $\tau(n)$  effectively?



- Lemma: Let  $p$  be prime and  $a \in \mathbb{Z}^+$ . Then

$$\sigma(p^a) = (1 + p + p^2 + \dots + p^n) = \frac{p^{a+1} - 1}{p - 1}$$

$$\text{and } \tau(p^a) = a + 1$$

- Proof: The divisors of  $p^a$  are  $1, p, p^2, \dots, p^{a-1}, p^a$ .

$$\therefore \sigma(p^a) = (1 + p + p^2 + \dots + p^n) = \frac{p^{a+1} - 1}{p - 1}$$

$$\text{and } \tau(p^a) = a + 1$$



- Thm: Let  $n$  have prime factorization  $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ ,

then

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \dots \frac{p_s^{a_s+1} - 1}{p_s - 1} = \prod_{j=1}^s \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

$$\tau(n) = (a_1 + 1)(a_2 + 1) \dots (a_s + 1) = \prod_{j=1}^s (a_j + 1)$$

- Proof:  $\because$   $\sigma$  and  $\tau$  multiplicative. Use above Lemma.





- Ex: Find  $\sigma(720)$  and  $\tau(720)$ .

$$\therefore 720 = 2^4 \cdot 3^2 \cdot 5$$

$$\therefore \sigma(720) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 31 \cdot 13 \cdot 6 = 2418$$

$$\tau(720) = (4 + 1)(2 + 1)(1 + 1) = 30$$



## 7.3 Perfect Numbers and Mersenne Primes

- Def: If  $n$  is a positive integer and  $\sigma(n) = 2n$ , then  $n$  is called a perfect number.

- Recall that  $\sigma(n) = \sum_{d|n} d$ .

- Ex:

$$\sigma(6) = 1 + 2 + 3 + 6 = 12$$

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$$

} Perfect number



## How to find all even perfect numbers?

- Thm:  $n \in \mathbb{Z}^+$  is an even perfect number iff
$$n = 2^{m-1}(2^m-1),$$
where  $m \in \mathbb{Z}^+ \ni m \geq 2$  and  $2^m-1$  is prime.

- Proof:

( $\Rightarrow$ ) Let  $n=2^{m-1}(2^m-1)$  and  $2^m-1$  is prime, then

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1}) \sigma(2^m-1) \\ &= (2^m-1)2^m = 2n\end{aligned}$$

$\therefore n$  is a perfect number.

( $\Leftarrow$ ) Let  $n$  be an even perfect number. Write  $n=2^s t$ , where  $s, t \in \mathbb{Z}^+$  and  $t$  is odd.  $\therefore (2^s, t)=1$

$$\therefore \sigma(n) = \sigma(2^s t) = \sigma(2^s) \sigma(t) = (2^{s+1}-1) \sigma(t) = 2n = 2^{s+1} t$$



- Proof: (Conti.)

$$(\Leftrightarrow) \because (2^{s+1}, 2^{s+1}-1)=1 \Rightarrow 2^{s+1} | \sigma(t)$$

It implies that  $\sigma(t)=2^{s+1}q$

$$\Rightarrow (2^{s+1}-1)2^{s+1}q=2^{s+1}t \Rightarrow (2^{s+1}-1)q=t \Rightarrow q | t$$

and  $q \neq t$

$$\therefore t+q=2^{s+1}q = \sigma(t)$$

If  $q \neq 1$ , then  $\because 1 | t, q | t, t | t, \therefore \sigma(t) \geq t+q+1 > t+q$

$\therefore q=1$  and  $t=2^{s+1}-1$  and  $\sigma(t)=t+1 \Rightarrow t$  is prime.

$\therefore n=2^s(2^{s+1}-1)$ , where  $2^{s+1}-1$  is prime.

- To find even perfect numbers, we need to find **primes** of the form  $2^m-1$ . How to find primes of the form?



- Thm: If  $m \in \mathbb{Z}^+$  and  $2^m - 1$  is prime, then  $m$  must be prime.
- Proof: Assume that  $m$  is not prime, (i.e.,  $m = ab$ ,  $1 < a < m$  and  $1 < b < m$ ) then
$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$$
Thus,  $2^m - 1$  is composite if  $m$  is not prime. Therefore, if  $2^m - 1$  is prime, then  $m$  must be prime.
- Q: Is it true that if  $m$  is prime then  $2^m - 1$  is prime?  
A: No.



- Def: If  $m \in \mathbb{Z}^+$ , then  $M_m = 2^m - 1$  is called the  $m$ -th Mersenne number.  
If  $p$  is prime and  $M_p = 2^p - 1$  is also prime, then  $M_p$  is called a Mersenne prime.



- Thm: If  $p$  is an odd prime, and if  $g|M_p=2^p-1$ , then  $g$  must be of the form  $2kp+1$ ,  $k \in \mathbb{Z}^+$ .
- Proof: Let  $g$  be prime and  $g|M_p=2^p-1$ 
  - $\because g$  is prime, we have  $g|2^{g-1}-1$
  - $\because g|(2^p-1, 2^{g-1}-1) = 2^{(p,g-1)}-1 > 1$
  - $\therefore (p, g-1) = p \Rightarrow p|g-1, \therefore \exists m \in \mathbb{Z}^+ \ni g-1 = mp$
  - $\because g$  is odd,  $\therefore m$  is even.  $\Rightarrow m = 2k, k \in \mathbb{Z}^+$ .
  - $\therefore g = mp + 1 = 2kp + 1$



- Above Thm can be used to develop an algorithm for deciding whether  $M_m = 2^m - 1$  is a prime or not.

- Algorithm:

Input:  $M_m = 2^m - 1, m$       Output: Yes or No.

1. Find  $\lfloor \sqrt{M_m} \rfloor = n$
2. For  $k=1$  to  $\lfloor \frac{n}{2m} \rfloor$
3. If  $2km+1 \mid M_m$ , then output = No. Go to 6.
4. Next  $k$ .
5. Output = Yes
6. End



A decorative graphic on the left side of the slide, consisting of overlapping yellow, red, and blue squares with a black crosshair.

- Lucas-Lehmer Test  
(Primality test for large Mersenne number)

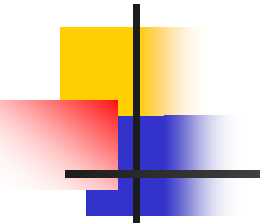
Let  $p$  be a prime and  $M_p = 2^p - 1$

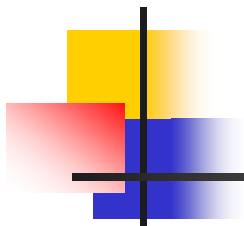
Define  $r_1 = 4$  and for  $k \geq 2$

$$r_k = r_{k-1}^2 - 2 \pmod{M_p}, \quad 0 \leq r_k \leq M_p$$

Then  $M_p$  is prime iff  $r_{p-1} = 0 \pmod{M_p}$



- 
- A decorative graphic on the left side of the slide, featuring overlapping yellow, red, and blue squares with a black crosshair.
- Corollary: Let  $p$  be prime. It is possible to determine whether  $M_p$  is prime by using  $O(p^3)$  bit operations.
  - Proof:  $p-1 \times \underbrace{(\log M_p)^2}_{\text{squaring}} = O(p^3)$  bit operations.



- Conjecture: There are infinitely many Mersenne prime, although, at 1992, a total of 32 Mersenne primes are known. (Has not been proved)