

Multiplicative function. A number theoretic function  $f$  is said to be multiplicative if

$$f(mn) = f(m)f(n) \quad \text{whenever } \gcd(m, n) = 1$$

Thm 3 The functions  $\tau$  and  $\sigma$  are both multiplicative functions

Pf Let  $m, n \in \mathbb{N}$  s.t.  $\gcd(m, n) = 1$

Assume  $m > 1, n > 1$  (for  $m=1, n=1$  the result is trivial)

Let  $m$  and  $n$  have prime factorizations:

$$m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$$

$\therefore \gcd(m, n) = 1$  therefore  $p_i \neq q_j$  for any  $i, j$ .

$\therefore$  The prime factorization of the product  $mn$  is given by

$$mn = p_1^{k_1} \dots p_n^{k_n} q_1^{j_1} \dots q_s^{j_s}$$

$$\therefore \tau(mn) = (k_1 + 1) \dots (k_n + 1) (j_1 + 1) \dots (j_s + 1)$$

$$= \tau(m)\tau(n)$$

$$\text{and } \sigma(mn) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \dots \frac{p_n^{k_n+1} - 1}{p_n - 1} \cdot \frac{q_1^{j_1+1} - 1}{q_1 - 1} \dots \frac{q_s^{j_s+1} - 1}{q_s - 1}$$

$$= \sigma(m)\sigma(n)$$

Lemma 4 If  $\gcd(m, n) = 1$  then the set of positive divisors of  $mn$  consists of all products  $d_1 d_2$  where  $d_1 | m$ , and  $d_2 | n$  and  $\gcd(d_1, d_2) = 1$ . Furthermore these products are all distinct.

Pf Assume  $m > 1$  and  $n > 1$  and

$$\text{let } m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$$

$\therefore \gcd(m, n)$  therefore the prime factorizations of  $m$  and

$n$  will not contain any common term i.e.  $p_i \neq q_j, \forall i, j$

Hence the prime factorization of  $mn$  is

$$mn = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}$$

$\therefore$  Any positive divisor of  $mn$  can be uniquely written as

$$d = p_1^{a_1} \dots p_n^{a_n} q_1^{b_1} \dots q_s^{b_s} \quad 0 \leq a_i \leq k_i, \quad 0 \leq b_j \leq j_j$$

Taking  $d_1 = p_1^{a_1} \dots p_x^{a_x}$  and  $d_2 = q_1^{b_1} \dots q_s^{b_s}$  gives us  
 $d = d_1 d_2$  and clearly  $d_1 | m$  and  $d_2 | m$

$$\therefore p_i \neq q_j \quad \forall i, j$$

$$\therefore \gcd(d_1, d_2) = 1$$

Thm 4 If  $f$  is a multiplicative function and  $F$  is defined by

$$F(m) = \sum_{d|m} f(d)$$

then  $F$  is also multiplicative.

Pf Let  $m, n \in \mathbb{Z}$  s.t.  $\gcd(m, n) = 1$

$$\text{Then } F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \quad [\gcd(d_1, d_2) = 1]$$

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

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

$$= F(m) F(n)$$

Example  $m=8$   $n=3$   $m=2^3$   $n=3$

$$F(8 \cdot 3) = \sum_{d|24} f(d)$$

$$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$$

$$= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(2 \cdot 3) + f(8 \cdot 1) \\ + f(4 \cdot 3) + f(8 \cdot 3)$$

$$= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) \\ + f(8)f(1) + f(4)f(3) + f(8)f(3)$$

$$= [f(1) + f(2) + f(4) + f(8)] [f(1) + f(3)]$$

② The Möbius inversion formula

For  $m \in \mathbb{N}$  define  $\mu$

$$\mu(m) = \begin{cases} 1 & \text{if } m=1 \\ 0 & \text{if } p^2 | m \text{ for some prime } p \text{ (i.e. } m \text{ is not square free)} \\ (-1)^r & \text{if } m = p_1 p_2 \dots p_r \text{ where } p_i \text{ are distinct primes} \end{cases}$$

Möbius  $\mu$ -function

Example  $\mu(1) = 1, \mu(2) = (-1)^1 = -1$

$\mu(3) = (-1)^1 = -1$

$\mu(4) = 0 \quad \because 2^2 | 4$

$\mu(5) = -1$

$\mu(6) = (-1)^2 = 1$

Thm 5  $\mu$  is a multiplicative function

Pf Let  $m, n \in \mathbb{Z}$  s.t.  $\gcd(m, n) = 1$

Suppose either of  $m$  and  $n$  are divisible by  $p^2$  i.e.

either  $p^2 | m$  or  $p^2 | n$ . ~~Anyway~~ Either way  $p^2 | mn$

$\therefore \mu(mn) = 0 = \mu(m)\mu(n)$  [Either  $\mu(m) = 0$  or  $\mu(n) = 0$ ]

Suppose both  $m$  and  $n$  are square free. Suppose

$m = p_1 p_2 \dots p_r$  and  $n = q_1 q_2 \dots q_s$

Note that all the primes  $p_i$ 's and  $q_j$ 's are distinct. Then

$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$

Thm 6 For each +ve integer  $n \geq 1$

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$$

Pf  $n=1 \quad \sum_{d|1} \mu(d) = \mu(1) = 1$

$n>1$  Firstly, calculate  $\sum_{d|n} \mu(d)$  for powers of a prime say for  $n = p^k$

$$F(m) = F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \dots + \mu(p^k)$$

$$= \mu(1) + \mu(p) + 0 + 0 + \dots + 0$$

$$= 1 + (-1) = 0$$

Now let us suppose ~~prop~~  $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

Then  $F(m) = \sum_{d|m} \mu(d)$  is a multiplicative f<sup>n</sup> By Thm 4.6  
∴  $\mu$  is multiplicative

$$\therefore F(m) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r}) = 0 \cdot 0 \dots 0 = 0$$

Thm 7 (Möbius inversion formula) Let  $F$  and  $f$  be two number-theoretic f<sup>n</sup> related by the formula

$$F(m) = \sum_{d|m} f(d)$$

Then  $f(m) = \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d|m} \mu\left(\frac{m}{d}\right) F(d)$

Q7 We have  $\sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d|m} \left( \mu(d) \sum_{c|m/d} f(c) \right)$

$$= \sum_{d|m} \sum_{c|m/d} \mu(d) f(c)$$

Now  $d|m$  and  $c|m/d \Rightarrow d \cdot c = m$  and  $\frac{m}{d} = c$   
 $\Leftrightarrow m = d \cdot d'$  and  $m = d \cdot c \cdot c' \Leftrightarrow c|m$   
~~predecessor~~  $\updownarrow$   
 $d|m/c$

$$\therefore \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d|m} \sum_{c|m/d} \mu(d) f(c) = \sum_{c|m} \left( \sum_{d|m/c} f(c) \mu(d) \right)$$

$$= \sum_{c|m} \left( f(c) \sum_{d|m/c} \mu(d) \right)$$

Now we have two cases

Case 1 If  $m/c \neq 1$  then  $\sum_{d|m/c} \mu(d) = 0 \Rightarrow \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = 0$

Case 2 If  $m/c = 1$  then  $\sum_{d|m/c} \mu(d) = 1$

$$\sum_{d|m} \mu(d) = 1$$

$$\sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{\substack{d|m \\ c=m}} f(c) \cdot 1 = f(m)$$

Now let us replace the dummy index  $d$  by  $d' = \frac{m}{d} \Rightarrow m = d'd$   
 $\therefore d'$  is also a positive divisor of  $m$ . and

$$f(m) = \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d'|m} \mu\left(\frac{m}{d'}\right) F(d')$$

Thm 8 If  $F$  is a multiplicative  $f_n$  and

$$F(m) = \sum_{d|m} f(d)$$

then  $f$  is also multiplicative

P/ Let  $m, n \in \mathbb{Z}$  s.t.  $\gcd(m, n) = 1$

~~Let~~ Let  $d$  be a divisor of  $mn$ . Then we can write  $d$  as  $d = d_1 d_2$  where  $d_1 | m$  and  $d_2 | n$  and  $\gcd(d_1, d_2) = 1$

Using the inversion formula:

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1) \mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$\Rightarrow f(mn) = \sum_{d_1|n} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$
$$= f(mn)$$