~~(Ch-6)~~ Number Theoretic functions

(6.1) (Defn)
A function whose domain of definition is the set of positive integers is said to be number theoretic (or arithmetic fun).

(Defn) Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

(e.g) $n = 12$, where positive divisors $1, 2, 3, 4, 6, 12$

$\tau(12) = 6$

$\sigma(12) = 1+2+3+4+6+12 = 28$

$\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$,

$\tau(5) = 2$, $\tau(6) = 4$

$\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$

$\sigma(6) = 12$

Notation

$\tau(n) = \sum_{d|n} 1$ where $\sum_{d|n} 1$ denotes the sum of as many 1's as there are positive divisor of n.

(where d runs over all positive divisors of positive integer n)

$\sigma(n) = \sum_{d|n} d$ where $\sum_{d|n}$ is sum of all positive divisors of n.

(e.g) $\tau(10) = \sum_{d|10} 1 = 1+1+1+1 = 4$

$(1, 2, 5, 10)$

$\sigma(10) = \sum_{d|10} d = 1+2+5+10 = 18$

$\tau(12) = \sum_{d|12} 1 = 1+1+1+1+1+1 = 6$

$(1, 2, 3, 4, 6, 12)$ $\sigma(12) = 1+2+3+4+6+12 = 28$

Remark

① $\tau(n) = 2 \iff n$ is prime number
② $\sigma(n) = n+1 \iff n$ is prime number

Theorem (6.1) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \le a_i \le k_i \ (i = 1, 2, \ldots, r)$

(Pf) let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

and $d \mid n$

to show: $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \ (0 \le a_i \le k_i)$

when $a_1 = a_2 = \cdots = a_r = 0$ then

1 can be written as

$$1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

and n is also divisor of n

$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ (where take $a_1 = k_1, a_2 = k_2, \ldots a_r = k_r$)

suppose $d \mid n$; non-trivially

say $n = d d'$ where $d > 1, d' > 1$

By (Prime factorization thm) (non-trivially means $d \ne 1$ & $d' \ne 1$)

Express d & d' as product of (not necessarily distinct) primes ①

$d = q_1 q_2 \cdots q_s$ & $d' = t_1 t_2 \cdots t_u$

where q_i, t_j primes.

Then, $n = d d'$

i.e. $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 q_2 \cdots q_s t_1 t_2 \cdots t_u$ → ②

are two prime factorization of positive integer n.

By Uniqueness of prime factorization we can form each prime q_j must be one of p_j. d

[Prime factorization thm
every number > 1 is either prime or product of primes]

collecting the equal primes into a single integral power we get (or) from (1) & (2), we get d (as)

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$ (Hence Proved)

where the possibility that $a_i = 0$ is allowed.

Conversely every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \le a_i \le k_i)$

to show: $d \mid n$

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

$$= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r})$$

$$= d\, d'$$

with $d' = p_1^{k_1-a_1} p_2^{k_2-a_2} \cdots p_r^{k_r-a_r}$

and $k_i - a_i \ge 0$ for each i.

then $d' > 0$ & $d \mid n$.

so, $n = d\,d'$, $d' > 0$ & $n > 1$ $\Rightarrow d > 0$ ($\because$ we show positive divisor) $\Rightarrow d \mid n$

Theorem (6.2) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$.

then (a) $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$

(b) $$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

(Pf) (By thm 6.1)

The positive divisors of n, are those integers

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \quad \text{where } 0 \le a_i \le k_i$$

So, there are (k_1+1) (as $0 \le a_i \le k_i$) choices for the exponent a_1 (i.e $p_1^{a_1}$ has exactly (k_1+1) positive divisors)

(k_2+1) choices for a_2 ($p_2^{a_2}$ has exactly (k_2+1) positive divisors)

$\vdots$

(k_r+1) choices for a_r

Hence there are $(k_1+1)(k_2+1)\cdots(k_r+1)$ possible divisors of n.

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

$\tau(n)$ = (numbers of positive divisors) $= (k_1+1)\cdot(k_2+1)\cdots(k_r+1)$ is number

Now $n > 1$

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

positive divisors of $p_1^{k_1}$ are $p_1^0, p_1^1, \ldots p_1^{k_1}$

Sum of positive divisors of $p_1^{k_1} = 1 + p_1 + p_1^2 + \cdots + p_1^{k_1}$

$$= \frac{p_1^{k_1+1} - 1}{p_1 - 1}$$

Sum of " " " $p_2^{k_2} = 1 + p_2 + p_2^2 + \cdots + p_2^{k_2}$

$$= \frac{p_2^{k_2+1} - 1}{p_2 - 1}$$

" " " " $p_r^{k_r}$ are $\dfrac{p_r^{k_r+1} - 1}{p_r - 1}$

$\therefore$ Sum of positive divisors of $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$$= \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right)$$

Notation for product $\prod$

$\prod_{d|n} f(d)$ means product the value $f(d)$ as d runs over all positive divisors of positive integer n.

(eg) $\prod_{1 \le d \le 5} f(d) = f(1) \cdot f(2) \cdot f(3) \, f(4) \cdot f(5)$

$\prod_{d|9} f(d) = f(1) \, f(3) \, f(9)$

$\prod_{\substack{p|30 \\ p \text{ is prime}}} f(p) = f(2) f(3) f(5)$

thm 6.2) can be rewritten as

$$\tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

(e.g) $180 = 2^2 \cdot 3^2 \cdot 5$

has $\tau(180) = (2+1)(2+1)(1+1) = 18$

$$\sigma(180) = \left(\frac{2^3-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$$

$$= 7 \cdot 13 \cdot 6 = 548$$

(Note) product of positive divisors of an integer $n > 1$ is $n^{\tau(n)/2}$

i.e $\prod_{d \mid n} d = n^{\tau(n)/2}$

(eg) $n = 16$, divisor of $n = 1, 2, 4, 8, 16$

$$\prod_{d \mid n} d = n^{\tau(n)/2}$$

$1 \cdot 2 \cdot 4 \cdot 8 \cdot 16 = 1024$

and $16^{\tau(16)/2}$ and $\tau(16) = \tau(2^4)$

$= 4 + 1 = 5$

$\therefore 16^{5/2} = (\sqrt{16})^5$

$= 4^5 = 1024$

(Defn) (6.2) A number-theoretic function f is said to be multiplicative if

$f(mn) = f(m) f(n)$ whenever $\gcd(m,n) = 1$

Theorem (6.3) The functions τ and σ are both multiplicative f. ①

(Pf) (By Def^n) Let $\gcd(m,n)=1$, we are done if either m or n is equal to 1, since

$\sigma(mn) = \sigma(1\cdot n)$ or $\sigma(m\cdot 1)$
$= \sigma(n)$ or $\sigma(m)$
$= \sigma(1)\sigma(n)$ or $\sigma(1)\sigma(m)$ (with i as)

Let $m>1$ & $n>1$
if $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ (By prime factorization thm)
are prime factorization of m & n ~~because gcd(a,b)=1~~
Since $\gcd(m,n)=1$
So, No p_i can occur among the q_j.
It follows that the prime factorization of product mn is given by

$$mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \cdot q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

(Using thm 6.2), we get

$$\tau(mn) = (k_1+1)(k_2+1)\cdots(k_r+1)(j_1+1)\cdots(j_s+1)$$
$$= \tau(m)\,\tau(n)$$

Similarly we get

$$\sigma(mn) = \left[\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)\right]\left[\left(\frac{q_1^{j_1+1}-1}{q_1-1}\right)\cdots\left(\frac{q_s^{j_s+1}-1}{q_s-1}\right)\right]$$
$$= \sigma(m)\,\sigma(n)$$

Thus τ & σ are multiplicative function.

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

(Pf) Let $m>1$ & $n>1$
Let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$
be their respective prime factorization of m & n

primes $p_1, p_2, \ldots, p_r$ & $q_1, \ldots, q_s$ are all distinct
the prime factorization of mn is

$$mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \cdot q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

$\therefore$ Any divisor (positive) d of mn will be uniquely respresentable in the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \quad \begin{pmatrix} 0 \le a_i \le k_i \\ 0 \le b_i \le j_i \end{pmatrix} \text{ (by thm. 6.1)}$$

i.e $d = d_1 d_2$ (prime factorization)

where $d_1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ & $d_1 | m$

$d_2 = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ $\quad d_2 | n$

Since No p_i is equal to any q_j

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

(Theorem 6.4) If f is multiplicative function and F is defined by

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

then F is also multiplicative.

(Pf) let m & n be relatively prime positive integers

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

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

($\because$ every divisior d of mn can be uniquely written as product of divisior d_1 of m & d_2 of n (by lemma above) where gcd $(d_1, d_2) = 1$)

By defn of multiplicative fun

$$f(d_1 d_2) = f(d_1) f(d_2) \text{ (given)}$$

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

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

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