Chapter 1

Number-Theoretic Function

1.1 The function \( \tau \) and \( \sigma \)

Definition 1.1.1. Given a positive integer \( n \), let \( \tau(n) \) denote the number of positive divisor of \( n \) and \( \sigma(n) \) denote the sum of these divisor.

Definition 1.1.2. Any function whose domain of definition is the set of positive integers is called number theoretic function.

Note 1.1.1. \( \sigma(n) \), \( \tau(n) \) are non theoretic function.

Theorem 1.1.1. If \( n = \prod_{i=1}^{r} p_i^{k_i} = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \) is the prime factorization of \( n > 1 \), then

\[
\begin{align*}
a) \quad \tau(n) &= (k_1 + 1)(k_2 + 1) \cdots (k_r + 1). \\
b) \quad \sigma(n) &= (\left(1 + \frac{p_1^{\alpha_1}}{p_1-1}\right)(\frac{p_2^{\alpha_2+1}-1}{p_2-1})\cdots (\frac{p_r^{\alpha_r+1}-1}{p_r-1})).
\end{align*}
\]

Proof. Any divisor \( d \) of \( n \) is of the form \( d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \) where \( 0 \leq \alpha_i \leq k_i \), there are \( k_1 + 1 \) choices for the exponent \( \alpha_1 \), \( k_2 + 1 \) choices for the exponent \( \alpha_2 \),..., \( k_r + 1 \) choices for the exponent \( \alpha_r \), hence there are \( (k_1+1)(k_2+1)\cdots(k_r+1) \) possible divisor of \( n \).

\[
\Rightarrow \tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1) = \prod_{i=1}^{r}(k_i + 1).
\]

To evaluate \( \sigma(n) \) consider the product

\[
(1 + p_1 + p_1^2 + \ldots + p_1^{k_1})(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \ldots + p_r^{k_r})\ldots(1)
\]

each positive divisor of \( n \) is one of the terms in the expansion of this product (1), so that
\[
\sigma(n) = \left(\frac{p_1^{k_1+1}}{p_1-1}\right)\left(\frac{p_2^{k_2+1}}{p_2-1}\right) \cdots \left(\frac{p_r^{k_r+1}}{p_r-1}\right)
\]
\[= \prod_{i=1}^{r}\left(\frac{p_i^{k_i+1}}{p_i-1}\right).\]

Example 1.1.1.  
\[n = 2^3 \cdot 47 = 376\]
\[\tau(n) = (3 + 1)(1 + 1) = 8.\]
\[\sigma(n) = \left(\frac{2^{3-1}}{2-1}\right)\left(\frac{47^{1-1}}{47-1}\right) = 15 \cdot 48 = 720.\]

Definition 1.1.3. A number theoretic functions \(f\) is called multiplicative number theoretic functions if \(f(mn) = f(m) \cdot f(n)\), where \(gcd(m, n) = 1\).

Theorem 1.1.2. The functions \(\tau\) and \(\sigma\) are both multiplicative functions.

Proof. If \(gcd(m, n) = 1\), then the result true if \(m = n = 1\).

Assume \(m > 1, n > 1\), if \(m = p_1^{k_1} \cdots p_r^{k_r}, n = q_1^{j_1} \cdots q_s^{j_s}, p_i \neq q_j\) for \(1 \leq i \leq r, 1 \leq j \leq s\), then
\[mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}\]
\[\tau(mn) = \left(k_1 + 1\right)\left(k_2 + 1\right) \cdots \left(k_r + 1\right)\left(j_1 + 1\right)\left(j_2 + 1\right) \cdots \left(j_s + 1\right)\]
\[= \tau(m) \cdot \tau(n).\]

also
\[\sigma(mn) = \prod_{i=1}^{r}\left(\frac{p_i^{k_i+1}}{p_i-1}\right) \cdot \prod_{j=1}^{s}\left(\frac{p_j^{j+1}}{p_j-1}\right)\]
\[= \sigma(m) \cdot \sigma(n).\]

Definition 1.1.4. \(\sum_{d|n} f(d)\) means the value \(f(d)\) runs over all the positive divisors of the positive integer \(n\).

Example 1.1.2. \(\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)\).

special cases:
\[\tau(n) = \sum_{d|n} 1 = 1 + 1 + 1 + \ldots + 1 \rightarrow number\ of\ divisor.\]
\[\sigma(n) = \sum_{d|n} d \rightarrow sum\ of\ divisor.\]

Example 1.1.3. \(\tau(10) = \sum_{d|10} 1 = 1 + 1 + 1 + 1 = 4\)
\[\sigma(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18\]
Lemma 1.1.1. If \( \gcd(m, n) = 1 \), then the set of positive divisors of \( mn \) consists of all products \( d_1d_2 \), where \( d_1|n, d_2|n \) and \( \gcd(d_1, d_2) = 1 \), further more, these products are all distinct.

Theorem 1.1.3. If \( f \) is a multiplicative function and \( F \) is defined by \( F(n) = \sum_{d|n} f(d) \); then \( F \) is also multiplicative.

Proof. Let \( g.c.d(m, n) = 1 \), then \( F(mn) = \sum_{d|n} f(d) = \sum_{d_1|n, d_2|n} f(d_1d_2) \).

Since every divisor of \( mn \) can be uniquely written as a product of a divisor \( d_1 \) of \( m \) and a divisor \( d_2 \) of \( n \), where \( g.c.d(d_1, d_2) = 1 \).

By the definition of a multiplicative functions we get

\[
f(d_1d_2) = f(d_1)f(d_2)
\]

\[
F(mn) = \sum_{d_1|n, d_2|n} f(d_1)f(d_2)
\]

\[
= \sum_{d_1|n} f(d_1) \sum_{d_2|n} f(d_2)
\]

\[
= F(m) \cdot F(n) \quad \Box
\]

Example 1.1.4. Let \( m = 8, n = 3 \)

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

\[
= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)
\]

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

\[
= f(1) \cdot f(1) + f(2) \cdot f(1) + f(1) \cdot f(3) + f(4) \cdot f(1) + f(2) \cdot f(3) +
\]

\[
= f(8) \cdot f(1) + f(4) \cdot f(3) + f(8) \cdot f(3)
\]

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

\[
= \sum_{d|8} f(d) \cdot \sum_{d|3} f(d)
\]

\[
= F(8) \cdot F(3).
\]
Definition 1.1.5. We say that \( n \) is not a square free if \( p^2 | n \), \( p \) is prime. And \( n \) is a square free if \( n = p_1 p_2 \cdots p_r \)

### 1.2 The Möbius inversion formula

**Definition 1.2.1.** For a positive integer \( n \), define \( \mu \) by the rules

\[
\mu = \begin{cases} 
1, & \text{if } n = 1 \\
0, & \text{if } p^2 | n \text{ for some } p \\
(-1)^r, & \text{if } n = p_1 p_2 \cdots p_r, \text{where the } p_i \text{ are distinct primes}
\end{cases}
\]

**Example 1.2.1.**
\( \mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1 \), \( \mu(1) = 1 \), \( \mu(2) = -1 \), \( \mu(4) = 0 \), \( \mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1 \).

**Note 1.2.1.** If \( p \) is a prime number, it is clear that \( \mu(p) = -1 \); also, \( \mu(p^k) = 0 \) for \( k \geq 2 \).

**Theorem 1.2.1.** The function \( \mu \) is a multiplicative function.

Proof. We want to show that \( \mu(mn) = \mu(m) \cdot \mu(n) \), where \( \gcd(m, n) = 1 \).
If either \( p^2 | m \) or \( p \) a prime, then \( p^2 | mn \). Hence, \( \mu(mn) = \mu(m) \cdot \mu(n) \), and the formula holds.
Let \( m = p_1 p_2 \cdots p_r \), \( n = q_1 q_2 \cdots q_s \), where \( p_i \neq q_j \) for \( 1 \leq i \leq r \), \( 1 \leq j \leq s \), then
\[
\mu(mn) = \mu(p_1 p_2 \cdots p_r) \cdot \mu(q_1 q_2 \cdots q_s) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m) \cdot \mu(n).
\]

**Note 1.2.2.** If \( n = 1 \), then \( \mu(d) = 1 \), \( \Rightarrow \sum_{d|n} \mu(d) = 1 \)
suppose \( n > 1 \) and put \( F(n) = \sum_{d|n} \mu(d) \)
let \( n = p^k \), the positive divisor of \( p^k \) are \( k + 1 \) integers \((1, p, p^2, ..., p^k)\), so that
\[
F(n) = F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = \mu(1) + \mu(p) = 1 + (-1) = 0
\]
If \( n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \)
if \( p_i \neq p_j \) for \( 1 \leq i \leq r \), \( 1 \leq j \leq r \), \( \gcd(p_i, p_j) = 1 \).
\( \Rightarrow F(n) = \sum_{d|n} \mu(d) \) is multiplicative (since \( \mu(d) \) is multiplicative)
\( \Rightarrow F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0 \)

**Theorem 1.2.2.** For each positive integer \( n \geq 1 \)
\[
\sum_{d|n} \mu(d) = \begin{cases} 
1, & \text{if } n = 1 \\
0, & \text{if } n > 1
\end{cases}
\]
where \( d \) runs through the positive divisors of \( n \).
Example 1.2.2. \( n = 10 \), The divisor of \( n \) are \( 1, 2, 5, 10 \)
\[
\sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) \\
= \mu(1) + \mu(2) + \mu(5) + \mu(10) \\
= 1 + (-1) + (-1) + 1 = 0
\]

Theorem 1.2.3. (Möbius inversion formula)

let \( F \) and \( f \) be tow number-theoretic functions related by the formula

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

then
\[
f(n) = \sum_{d|n} \mu(d)F(d|n) = \sum_{d|n} \mu(n|d)F(d)
\]

Proof. let \( d^\prime = \frac{n}{d} \), as \( d \) ranges over all positive divisors of \( n \), so dose \( d^\prime \).

(1) \[
\sum_{d|n} \mu(d)F(d|n) = \sum_{d|n} (\sum_{c|(\frac{n}{d})} f(c)) = \sum_{d|n} (\sum_{c|d^\prime} \mu(d)f(c))
\]

claim:
\( d|n \) and \( c|d^\prime = \frac{n}{d} \) iff \( c|n \) and \( d|\frac{n}{c} \).
\( d|n \) \( \Rightarrow \) \( \exists k \in \mathbb{Z} : n = d \cdot k, k = \frac{n}{d} \)
\( \Rightarrow \) \( n = d \cdot \frac{n}{d} \)
If \( c|\frac{n}{d} \) \( \Rightarrow \) \( c|n \) ( because \( c|\frac{n}{d} \) and \( d|\frac{n}{c} \))
also, \( \exists s^\prime \in \mathbb{Z} : n = \frac{n}{d} = cs^\prime \Rightarrow \frac{n}{d} = ds^\prime \Rightarrow d|\frac{n}{d} \)
Because of this, the last expression in (1) becomes

(2) \[
\sum_{d|n} (\sum_{c|d^\prime} \mu(d)f(c)) = \sum_{c|n} \sum_{d|\left(\frac{n}{c}\right)} \left( f(c)\mu(d) \right) \\
= \sum_{c|n} \left( f(c)\sum_{d\left(\frac{n}{c}\right)} \mu(d) \right).
\]

By theorem 6.6 \( \sum_{d\left(\frac{n}{c}\right)} \mu(d) = 0 \) except when \( \frac{n}{d} = 1 \)
That is when \( n = c \), in this case it is equal to 1.
so the right hand side of equation(2) simplifies to
\[
\sum_{c|n} \left( f(c)\sum_{d\left(\frac{n}{c}\right)} \mu(d) \right) = \sum_{c|n} f(c) \cdot 1 = f(n)
\]
\( \square \)
Example 1.2.3. Let $n = 10$, to illustrate how the double sum in (2) is turned. In this instance we find that
\[
\sum_{d|10} \sum_{c|\frac{n}{d}} (\mu(d)f(c)) = \mu(1)[f(1) + f(2) + f(5) + f(10)] + \mu(2)[f(1) + f(5)] + \\
\mu(5)[f(1) + f(2)] + \mu(10)[f(1)] = f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] + \\
f(2)[\mu(1) + \mu(5)] + f(5)[\mu(1) + \mu(2)] + f(10)[\mu(1)] = \sum_{c|10} \sum_{d|\frac{n}{c}} (f(c)\mu(d))
\]

To see how Möbius inversion works in a particular case, we remind the reader that the functions $\tau$ and $\sigma$ may both be described as sum functions
\[
\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d
\]

By theorem 6.7
\[
1 = \left(\sum_{d|n} \mu\left(\frac{n}{d}\right)\tau(d)\right) \quad \text{and} \quad n = \left(\sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma(d)\right)
\]
valid for all $n \geq 1$.

**Theorem 1.2.4.** If $F$ is a multiplicative function and $F(n) = \sum_{d|n} f(d)$, then $f$ is also multiplicative

**Proof.** Let $m$ and $n$ be relatively prime positive integers. we recalled that any divisor $d$ of $mn$ can be uniquely written as $d = d_1d_2$, where $d_1|m$, $d_2|n$ and $gcd(d_1,d_2) = 1$.

Thus, using the inversion formula,
\[
f(mn) = \sum_{d|m} \mu(d)F\left(\frac{mn}{d}\right) = \sum_{d_1|m,d_2|n} \mu(d_1d_2)F\left(\frac{mn}{d_1d_2}\right)
\]
\[
= \sum_{d_1|m,d_2|n} \mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)
\]
\[
= \sum_{d_1|m} \mu(d_1)F\left(\frac{m}{d_1}\right)\sum_{d_2|n} \mu(d_2)F\left(\frac{n}{d_2}\right)
\]
\[
= f(m)f(n)
\]

\[\square\]