# §1.2 数论函数和Mobius变换

## 一、数论函数

$\sigma(n)$表示$n$的所有正因子的和，记作$\sigma(n)=\sum\limits_{d|n} d$.

$\tau(n)$表示$n$的正因子的个数，记作$\tau(n)=\sum\limits_{d|n} 1$.

$\varphi(n)$表示$1,2,\cdots,n$中与$n$互素的数的个数，$\varphi(n)$叫做Euler函数.

def 2.1 数论函数$f:\mathbb{P}\to\mathbb{C}$叫做积性函数，是指对任意两个互素的正整数$n$和$m$，均有$f(mn)=f(m)f(n)$

Lemma 2.2 1）数论函数$\tau$和$\sigma$都是积性函数

2）设$n\geq 2$，$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$是$n$的标准分解式，则

$$\tau(n)=(e_1+1)(e_2+1)\cdots(e_s+1)=\prod_{i=1}^{s}(e_i+1)$$

$$\sigma(n)=\frac{p_1^{e_1+1}-1}{p_1-1}\cdot\frac{p_2^{e_2+1}-1}{p_2-1}\cdots\cdots\frac{p_s^{e_s+1}-1}{p_s-1}=\prod_{i=1}^{s}\frac{p_i^{e_i+1}-1}{p_i-1}$$

证：1）设$m,n$是互素的正整数，则$mn$的每个正因子都能唯一地写成$d=d_1d_2$，其中$d_1$和$d_2$分别是$n$和$m$的正因子

因而当$d_1$和$d_2$分别独立地跑过$n$和$m$的正因子时，$d_1d_2$恰好（不重复）给出$nm$的全部正因子.

$$\therefore\ \sigma(nm)=\sum_{d_1|n}\sum_{d_2|m}d_1d_2=\Big(\sum_{d_1|n}d_1\Big)\Big(\sum_{d_2|m}d_2\Big)=\sigma(n)\sigma(m)$$

$$\tau(nm)=\sum_{d_1|n}\sum_{d_2|m}1=\Big(\sum_{d_1|n}1\Big)\Big(\sum_{d_2|m}1\Big)=\tau(n)\tau(m)$$

即$\sigma(n)$与$\tau(n)$都是积性函数.

2）对于素数幂$p^a$（$p$是素数，$a\geq 1$）

由于$p^a$的正因子为$1,p,p^2\cdots p^{a-1}$和$p^a$

$\therefore\ \tau(p^a)=a+1$

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

再由$\tau$和$\sigma$的积性，2）即可证得.

def 2.3 设$f,g\in R$，定义$f$和$g$的卷积为数论函数$h$，表示为$f*g$，它在$n\in R$处的值为：

$$(f*g)(n)=h(n)=\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)$$

由于$d$遍历$n$的所有正因子时，$d'=\frac{n}{d}$也恰好遍历$n$的所有正因子，因而$(f*g)(n)=\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)=\sum_{d'\mid n} f\left(\frac{n}{d'}\right)g(d')=(g*f)(n)$

即卷积满足交换律.

Lemma 2.4 设$f$和$g$是积性数论函数，则$fg$，$\frac{f}{g}$，$f*g$也是积性函数.

证：设$(m,n)=1$，令$h=fg$，由$f$和$g$的积性可知

$$h(mn)=f(mn)g(mn)=f(m)f(n)g(m)g(n)$$
$$=((fg)(m))((fg)(n))=h(m)h(n)$$

$\therefore h=fg$是积性函数；

类似可证：当$g(n)\neq 0$ ($\forall n\in P$)时，$\frac{f}{g}$也是积性的；

令$h=f*g$，则

$$h(mn)=\sum_{d\mid mn} f(d)g\left(\frac{mn}{d}\right)=\sum_{d_1\mid n}\sum_{d_2\mid m} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)$$
$$=\sum_{d_1\mid n}\sum_{d_2\mid m} f(d_1)f(d_2)g\left(\frac{m}{d_2}\right)g\left(\frac{n}{d_1}\right)$$
$$=\left(\sum_{d_1\mid n} f(d_1)g\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2\mid m} f(d_2)g\left(\frac{m}{d_2}\right)\right)$$
$$=((f*g)(n))((f*g)(m))=h(n)h(m)$$

故$f*g$是积性函数.

CamScanner

## 二. Möbius函数

def 2.5 数论函数 $\mu=\{\mu(n)\}$ 定义为:

$$\mu(n)=\begin{cases}1 & 若 n=1\\ (-1)^r & 若n是r个不同素数的积\\ 0 & 否则 (即 \exists 素数p, 使 p^2|n)\end{cases}$$

—— Möbius函数

对每个数论函数 $f=\{f(n)\}$, 称数论函数 $F=f*\mu$ 为 $f$ 的 Möbius 变换, 即:

$$F(n)=\sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)=\sum_{d|n} f\left(\frac{n}{d}\right)\mu(d) \quad (n\geq 1)$$

Lemma 2.6 关于 $\mu$ 的性质

1) $\mu$ 是积性函数

2) $\sum_{d|n}\mu(d)=\begin{cases}1, & 若 n=1\\ 0, & 若 n\geq 2\end{cases}$

证: 1) 设 $(n,m)=1$

若存在素数 $p$, 使得 $p^2|n$ 或 $p^2|m$,

则 $\mu(n)=0$ 或 $\mu(m)=0$

此时 $p^2|mn$, 于是 $\mu(mn)=0$

从而 $\mu(mn)=\mu(m)\mu(n)$

若 $n$ 和 $m$ 均无平方因子, 则 $n=p_1p_2\cdots p_r$, $m=q_1q_2\cdots q_s$, 其中 $p_1\cdots p_r, q_1\cdots q_s$ 是互不相同的素数.

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

综上, $\mu$ 是积性函数.

2) 方法一：直接证明

令 $f(n)=\sum_{d|n}\mu(d)$ 则 $f(1)=\sum_{d|1}\mu(d)=\mu(1)=1$

对 $n\geq 2$，设 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 是标准分解式 $(r\geq 1)$

$\because d|n$ 故若 $d$ 有平方因子 $l^2$ $(l\geq 2)$ 时，$\mu(d)=0$

$\therefore$ 求 $f(n)$ 时只要考虑 $d$ 是 $p_1,p_2,\cdots,p_r$ 中一部分素数相乘的情况

因而若 $d$ 是 $p_1,p_2,\cdots,p_r$ 中 $i$ 个素数的乘积，

则 $\mu(d)=(-1)^i$

而 $p_1,p_2,\cdots,p_r$ 中取 $i$ 个的方法数为：

$$\binom{r}{i}=\frac{r!}{i!(r-i)!}=\frac{r\cdot(r-1)\cdots(r-i+1)}{i!}\ (=C_r^i)$$

$\therefore$ 当 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\geq 2$ 时，

$$f(n)=\sum_{i=1}^{r}\binom{r}{i}(-1)^i=\sum_{i=0}^{r}C_r^i(-1)^i\cdot 1^{r-i}$$

$$=[1+(-1)]^r=0$$

综上，2) 获证。

方法二：同一法（利用函数的积性）

记 $f(n)=\sum\limits_{d|n}\mu(d)$，则 $f=\mu*\{1\}$

其中 $\{1\}$ 为恒取值为1的数论函数

由1)知，$\mu$ 是积性的，易知 $\{1\}$ 也是积性的.

$\therefore f$ 是积性的

定义数论函数 $E_n=\begin{cases}1, & 若 n=1\\ 0, & 若 n\geq 2\end{cases}$

易证：E是积性的

则要证 $f=E$，只需证：

$f$ 和 $E$ 在每个素数幂 $p^e$ 处取值相等即可.

$f(p^e)=\sum\limits_{d|p^e}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^e)\quad(e\geq 1)$

$=\mu(1)+\mu(p)=1+(-1)^1=0$

$E(p^e)=0$

$\therefore f=E$ 从而<2>获证

Lemma 2.7 1) Euler函数$\varphi$是积性函数

2) $\varphi(1)=1$

对于$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\geq 2$(标准分解式)

有$\varphi(n)=\prod_{i=1}^{r}(p_i^{e_i}-p_i^{e_i-1})=n\prod_{i=1}^{n}(1-\frac{1}{p_i})=n\prod_{\substack{p\\ p\mid n}}(1-\frac{1}{p})$

证: 1) $\because\varphi(n)$是指$1,2,\cdots,n$中与$n$互素的整数的个数

即$\varphi(n)=\sum_{\substack{i=1\\ (i,n)=1}}^{n}1=\sum_{i=1}^{n}\sum_{\substack{d\\ d\mid(i,n)}}\mu(d)$ (由Lemma 2.6)

即$\varphi(n)$是对"$1\leq i\leq n$ 且 $d\mid(i,n)$"的$\mu(d)$求和.

先对$d$求和, $d\mid n$, 然后对每个固定的$d$,

再对$i$求和, 此时要满足$d\mid i$且$1\leq i\leq n$,

从而

$$\varphi(n)=\sum_{\substack{d\\ d\mid n}}\sum_{\substack{i\\ d\mid i}}\mu(d)=\sum_{\substack{d\\ d\mid n}}(\mu(d)\sum_{\substack{i=1\\ d\mid i}}1)$$

$\because d\mid i\quad\therefore i=di'\ (i'\in\mathbb{P})$

又$1\leq i\leq n\quad\therefore 1\leq i'\leq\frac{n}{d}\in\mathbb{P}$

$\therefore\sum_{\substack{i=1\\ d\mid i}}^{n}1=\sum_{i'=1}^{n/d}1=\frac{n}{d}$

$\therefore\varphi(n)=\sum_{\substack{d\\ d\mid n}}\mu(d)\frac{n}{d}=\mu*\{n\}$ ($\{n\}\triangleq f$, 即$f(n)=n$, 易知$f$是积性的)

$\therefore\varphi(n)=\sum_{\substack{d\\ d\mid n}}\mu(d)f(\frac{n}{d})=(\mu*f)(n)$

$\because\mu, f$是积性的 $\therefore\mu*f$是积性的

即Euler函数$\varphi$是积性的

2) ∵ $\varphi$ 是积性的，故只要求出 $\varphi(p^e)$ 的值 $p$ 为素数 $e\geq 1$

在 $1,2,3,\cdots,p^e$ 这 $p^e$ 个数中，与 $p$ 互素的共有 $p^{e-1}$ 个.

即被 $p$ 整除的数的个数 $(p,2p,3p,\cdots,p^{e-1}p)$

$\therefore \varphi(p^e)=p^e-p^{e-1}$

$\therefore$ 当 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ 时

$$\varphi(n)=\varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r})=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_r^{e_r}-p_r^{e_r-1})$$

$$=\prod_{i=1}^{r}(p_i^{e_i}-p_i^{e_i-1})$$

Thm 2.8 (Möbius 变换定理)

设 $f,g$ 是两个数论函数，则下面两个命题等价：

A) 对每个 $n\geq 1$，$f(n)=\sum_{d|n} g(d)$

B) 对每个 $n\geq 1$，$g(n)=\sum_{d|n}\mu(\frac{n}{d})f(d)$ $\left(=\sum_{d|n}\mu(d)f(\frac{n}{d})\right)$

证："<A> ⇒ <B>"

$$\sum_{d|n}\mu(\tfrac{n}{d})f(d)=\sum_{d|n}\mu(\tfrac{n}{d})\sum_{e|d}g(e)=\sum_{d|n}\sum_{e|d}\mu(\tfrac{n}{d})g(e)$$

$\because e|d|n$

$$\therefore \sum_{d|n}\sum_{e|d}\mu(\tfrac{n}{d})g(e)=\sum_{e|n}\sum_{e|d|n}\mu(\tfrac{n}{d})g(e)=\sum_{e|n}g(e)\sum_{e|d|n}\mu(\tfrac{n}{d})$$

令 $d'=\frac{d}{e}$ 则 $e|d|n$ 等价于 $d'\in IP$ 且 $d'|\frac{n}{e}$

$$\therefore \sum_{e|d|n}\mu(\tfrac{n}{d})=\sum_{d'|\frac{n}{e}}\mu(\tfrac{n}{e}/d')\triangleq\sum_{d''|\frac{n}{e}}\mu(d'')\quad (d''\triangleq\tfrac{n}{e}/d')$$

$$=\begin{cases}1, & 若\ \frac{n}{e}=1\ (即\ e=n)\\ 0 & 若\ \frac{n}{e}\geq 2\ (即\ e<n)\end{cases}$$

$$\therefore \sum_{e|n}g(e)\sum_{e|d|n}\mu(\tfrac{n}{d})=\sum_{e|n}g(e)\sum_{d''|\frac{n}{e}}\mu(d'')=g(e)=g(n)\quad (n=e 时非0)$$

即 对 $\forall n\geq 1$ $\sum_{d|n}\mu(\frac{n}{d})f(d)=g(n)$

即 <B> 成立.

"$\langle B\rangle \Rightarrow \langle A\rangle$" 类似可证:

$$\sum_{d|n} g(d) = \sum_{d|n}\sum_{e|d} \mu\left(\frac{d}{e}\right) f(e) = \sum_{e|n}\sum_{e|d|n} f(e)\mu\left(\frac{d}{e}\right) \quad (交换和号)$$

$$= \sum_{e|n} f(e) \sum_{e|d|n} \mu\left(\frac{d}{e}\right) = \sum_{e|n} f(e) \sum_{d'|\frac{n}{e}} \mu(d') \quad \left(d' = \frac{d}{e}\right)$$

$$= f(n) \quad \left(\frac{n}{e} > 1 时 \sum_{d'|\frac{n}{e}} \mu(d') = 0\right)$$

即 $\langle A\rangle$ 成立.

Lemma 2.9 对每个正整数 $n$, $\sum_{d|n} \varphi(d) = n$

证: 方法一:

$\{n\}$ 是积性函数 $\sum_{d|n} \varphi(d) = \varphi * \{1\}$ 也是积性函数

因而只需对 $n = p^e$ 验证相等.

$$\sum_{d|p^e} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^e)$$

$$= 1 + (p-1) + (p^2-p) + \cdots + (p^e - p^{e-1}) = p^e = n$$

方法二: 由 Lemma 2.7 证的.

$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$ 即 $\varphi = \mu * \{n\}$

$$\therefore \varphi(n) * \{1\} = (\mu * \{n\}) * \{1\}$$

$$= (\{n\} * \mu) * \{1\}$$

$$= \{n\} * (\mu * \{1\})$$

$$= \{n\} * E = \{n\}$$