# 第2章 数论函数

# 2.1 数论函数的定义

## 2.1 数论函数的定义

数论函数是定义在全体正整数$N$上的函数，它对$\forall n \in N$，指定一个实数或复数$f(n)$。数论函数在数学与计算机科学中有重要应用。

例如，$f(n)=\sqrt{n}\left(n \in N\right)$是数论函数，对自然数$n$指定了一个实数$\sqrt{n}$。

**定义1.1** 设$f(n)$是数论函数，如果对于$\forall m, n \in N$，当$(m,n)=1$时，$f(mn)=f(m)f(n)$，则称$f(n)$是积性的。如果去掉条件$(m,n)=1$，$f(mn)=f(m)f(n)$仍成立，则称$f(n)$是完全积性的。

例如，$f(n)=n^k$（$k$是给定的非负整数）是完全积性的。

**定理1.1** 设 $n=\prod_{i=1}^{s} p_i^{\alpha_i}$ 是$n$ 的标准分解式，$f(n)$ 是非恒0的积性函数的充要条件是 $f(1)=1$ 且

$$f(n)=\prod_{i=1}^{s} f(p_i^{\alpha_i}) \quad (1.1)$$

进一步，$f(n)$ 是完全积性的充要条件是 $f(1)=1$ 且

$$f(n)=\prod_{i=1}^{s} f^{\alpha_i}(p_i) \quad (1.2)$$

**证明** $f(n)$不是恒0的，存在 $n_0 \in N$，使得

$0 \neq f(n_0) = f(n_0 \cdot 1) = f(n_0)f(1)$，所以$f(1)=1$。

**必要性：** 对 $s$用数学归纳法。当 $s=1$时，$n=p_1^{\alpha_1}$，

$f(n)=f(p_1^{\alpha_1})$ 成立。假设式（1.1）对$s$成立，则$s+1$

时，由于$(\prod_{i=1}^{s} p_i^{\alpha_i}, p_{s+1}^{\alpha_{s+1}})=1$，所以

$$f(n)=f(\prod_{i=1}^{s+1}p_i^{\alpha_i})=f\left(\left(\prod_{i=1}^{s}p_i^{\alpha_i}\right)p_{s+1}^{\alpha_{s+1}}\right)$$

$$=f(\prod_{i=1}^{s}p_i^{\alpha_i})f(p_{s+1}^{\alpha_{s+1}})=\left(\prod_{i=1}^{s}f(p_i^{\alpha_i})\right)f(p_{s+1}^{\alpha_{s+1}})=\prod_{i=1}^{s+1}f(p_i^{\alpha_i})$$

如果 $f(n)$ 是完全积性的，则对 $\forall i\in\{1,\cdots,s\}$，

$f(p_i^{\alpha_i})=f^{\alpha_i}(p_i)$ 所以 $f(n)=\prod_{i=1}^{s}f^{\alpha_i}(p_i)$ 。

**充分性：** 若 $m,n$ 中有1个为1，不妨设 $m=1$，由 $f(1)=1$，$f(mn)=f(n)=f(n)f(1)=f(m)f(n)$。当 $m>1,n>1$ 时，设 $m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$n=q_1^{\beta_1}\cdots q_t^{\beta_t}$。如果 $(m,n)=1$，则对 $\forall p_i$，$q_j$ $(1\le i\le s, 1\le j\le t)$，有 $p_i\neq q_j$，$p_1^{\alpha_1},\cdots,p_s^{\alpha_s}$，$q_1^{\beta_1},\cdots,q_t^{\beta_t}$ 两两互素。所以

$$\begin{aligned} f(mn) &= f(p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_t^{\beta_t}) \\ &= f(p_1^{\alpha_1})\cdots f(p_s^{\alpha_s})f(q_1^{\beta_1})\cdots f(q_t^{\beta_t}) = f(m)f(n) \end{aligned}$$

即 $f(n)$ 是积性的。

要证 $f(n)$ 是完全积性的，则去掉 $(m,n)=1$ 的条件。此时 $m,n$ 的标准分解式中 $p_i(1\le i\le s)$ 和 $q_j(1\le j\le t)$ 存在相等的元素，将相等的元素合在一起。不妨假定前 $e(e\le s, e\le t)$ 项相等，则 $mn$ 的标准分解式为

$mn=p_1^{\alpha_1+\beta_1}\cdots p_e^{\alpha_e+\beta_e}p_{e+1}^{\alpha_{e+1}}\cdots p_s^{\alpha_s}q_{e+1}^{\beta_{e+1}}\cdots q_t^{\beta_t}$。按照式(1.2)，

$$f(mn)=f^{\alpha_1+\beta_1}(p_1)\cdots f^{\alpha_e+\beta_e}(p_e)f^{\alpha_{e+1}}(p_{e+1})\cdots f^{\alpha_s}(p_s)f^{\beta_{e+1}}(q_{e+1})\cdots f^{\beta_t}(q_t)$$

$$=f^{\alpha_1}(p_1)\cdots f^{\alpha_s}(p_s)f^{\beta_1}(q_1)\cdots f^{\beta_t}(q_t)=f(mn)$$

证毕。

**定理1.2** 设 $f$是不恒为0的积性函数，则 $F(n)=\sum_{d|n} f(d)$ 也是积性函数，其中和号表示对 $n$的所有正因子求和。

**证明** $F(1)=f(1)=1$。当 $n>1$时，设 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，由第1章定理2.14，$p_1^{\beta_1}\cdots p_s^{\beta_s}$ $(0\le\beta_i\le\alpha_i, i=1,\cdots,s)$ 是 $n$的所有因子。$F(n)=\sum_{d|n} f(d)=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_s=0}^{\alpha_s} f(p_1^{\beta_1}\cdots p_s^{\beta_s})$

$$=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_s=0}^{\alpha_s}\left[f(p_1^{\beta_1})\cdots f(p_s^{\beta_s})\right]=\left[\sum_{\beta_1=0}^{\alpha_1} f(p_1^{\beta_1})\right]\cdots\left[\sum_{\beta_s=0}^{\alpha_s} f(p_s^{\beta_s})\right]$$

$$=\left[\sum_{d_1|p_1^{\alpha_1}} f(d_1)\right]\cdots\left[\sum_{d_s|p_s^{\alpha_s}} f(d_s)\right]$$

，所以 $F(n)$ 是积性的。

证毕。

**定理1.3** 设 $f,g$ 是2个积性函数，则 $F(n)=\sum_{d|n} f(d)g(\frac{n}{d})$ 也是积性函数。

**证明** 由 $f(1)=g(1)=1$ 得 $F(1)=1$ 。

当 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ 时，$F(n)=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_s=0}^{\alpha_s} f(p_1^{\beta_1}\cdots p_s^{\beta_s})g(p_1^{\alpha_1-\beta_1}\cdots p_s^{\alpha_s-\beta_s})$

$$=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_s=0}^{\alpha_s}\left[f(p_1^{\beta_1})\cdots f(p_s^{\beta_s})g(p_1^{\alpha_1-\beta_1})\cdots g(p_s^{\alpha_s-\beta_s})\right]$$

$$=\sum_{\beta_1=0}^{\alpha_1}\left[f(p_1^{\beta_1})g(p_1^{\alpha_1-\beta_1})\right]\cdots\left[\sum_{\beta_s=0}^{\alpha_s} f(p_s^{\beta_s})g\left(p_s^{\alpha_s-\beta_s}\right)\right]=F(p_1^{\alpha_1})\cdots F(p_s^{\alpha_s})$$

所以 $F(n)$ 是积性的。 证毕。

# 2.2 函数 $\tau(n)$ 和 $\sigma(n)$

## 2.2 函数$\tau(n)$和$\sigma(n)$

**定义2.1** 设 $n \in Z$，定义$\tau(n)=\sum_{d|n} 1$，$\sigma(n)=\sum_{d|n} d$。即$\tau(n)$是$n$的所有正因子的个数，$\sigma(n)$是$n$的所以正因子之和。

**定理2.1** 设 $n \in N$，

（1）$\tau(n)$是积性的。

（2）如果$n$为素数，$\tau(n)=2$。如果$n=p^{\alpha}$（其中$p$为素数），则$\tau(p^{\alpha})=\alpha+1$。

（3）如果$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则$\tau(n)=(\alpha_1+1)\cdots(\alpha_s+1)=\prod_{i=1}^{s}(\alpha_i+1)$

**证明** （1）因为常数函数 $f(n)=1$ 是积性的，$\tau(n)=\sum_{d|n} f(d)$，由定理1.2，$\tau(n)$ 是积性的。

（2）若 $n$ 为素数，则 $n$ 只有2个因子 1，$n$，所以 $\tau(n)=2$。
若 $n=p^{\alpha}$，则 $n$ 的因子为 $n=p^{\beta}\left(0\le\beta\le\alpha\right)$，$\tau(n)=\sum_{\beta=0}^{\alpha}1=(\alpha+1)$

（3）$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ 时，

$$\tau(n)=\tau(p_1^{\alpha_1})\cdots\tau(p_s^{\alpha_s})=(\alpha_1+1)\cdots(\alpha_s+1)。$$

证毕。

**定理2.2** 设 $n \in N$,

（1） $\sigma(n)$是积性的。

（2） 如果 $n$为素数，则$\sigma(n) = n+1$。如果 $n = p^{\alpha}$（ $p$为素数），则 $\sigma(p^{\alpha}) = \dfrac{p^{\alpha+1}-1}{p-1}$

（3） 如果$n = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则$\sigma(n) = \dfrac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\dfrac{p_s^{\alpha_s+1}-1}{p_s-1} = \prod_{i=1}^{s}\dfrac{p_i^{\alpha_{i+1}}-1}{p_i-1}$

**证明** (1)因为恒等函数$f(n)=n$是积性的,$\sigma(n)=\sum_{d|n} d=\sum_{d|n} f(d)$

由定理1.2，$\sigma(n)$是积性的。

（2）如果$n$为素数，$n$只有2个因子1和$n$,$\sigma(n)=\sum_{d|n} d=1+n$

如果$n=p^{\alpha}$，则$\sigma(n)=\sum_{\beta=0}^{\alpha} p^{\beta}=1+p+\cdots+p^{\alpha}=\dfrac{p^{\alpha+1}-1}{p-1}$

（3）如果$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则

$$\sigma(n)=\sigma(p_1^{\alpha_1})\cdots\sigma(p_s^{\alpha_s})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}=\prod_{i=1}^{s}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

证毕。

# 2.3 函数$\mu(n)$及Möbius变换

## 2.3 函数$\mu(n)$及Möbius变换

**定义3.1** 设$n\in N$，$n$的标准分解式为$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，定义函数：

$$\mu(n)=\begin{cases}1, & n=1;\\ 0, & \text{如果存在 } i\in\{1,\cdots,s\}\text{，使得 } \alpha_i\geq 2;\\ (-1)^s, & \text{其他.}\end{cases}$$

称函数$\mu(n)$为Möbius函数。

由定义可见，若$n$含有素数的平方因子，则$\mu(n)=0$。如果$n$是偶数个不同素数的乘积，$\mu(n)=1$；如果是奇数个不同素数的乘积，$\mu(n)=-1$。

下表是一些 $n$ 的 $\mu(n)$ 函数值。

表3.2　一些 $n$ 的 $\mu(n)$ 函数值

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 100 | 101 | 102 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mu(n)$ | 1 | -1 | -1 | 0 | -1 | 1 | -1 | 0 | 0 | 1 | 0 | -1 | -1 |

**定理3.1** 设 $n \in N$，

（1）$\mu(n)$ 是积性的；

（2）设 $\nu(n) = \sum\limits_{d|n} \mu(d)$，则 $\nu(n) = \begin{cases} 1, & \text{如果} n=1; \\ 0, & \text{如果} n>1。\end{cases}$

**证明** （1）由定义，$\mu(1)=1$。设 $m, n \in N$, $(m,n)=1$，如果 $m$ 或 $n$ 有素数平方因子，即 $\mu(m)=0$ 或 $\mu(n)=0$，则 $mn$ 也有素数平方因子，因此 $\mu(mn)=0$，所以 $\mu(mn)=\mu(m)\mu(n)$

否则，设 $m = p_1 \cdots p_s$，$n = q_1 \cdots q_t$。由 $(m,n)=1$，有

$p_i \neq q_j \ (i=1,\dots,s; j=1,\dots,t)$，

$\mu(mn) = \mu(p_1 \cdots p_s q_1 \cdots q_t) = (-1)^{s+t} = (-1)^s(-1)^t = \mu(m)\mu(n)$。

（2） $n=1$时，$\nu(1)=\sum_{d|n}\mu(d)=1$。$n>1$时，由 $\mu(n)$是积性的及定理1.2，知$\nu(n)$是积性的。因此求$\nu(n)$只需对$n$的标准分解式中的每一项素数幂进行。

$$\nu(p^\alpha)=\sum_{d|p^\alpha}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^\alpha)$$

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

所以 $\nu(n)=0$ 。 证毕。

在函数 $\tau(n)=\sum_{d|n}1$中取 $f(n)=1$，$\sigma(n)=\sum_{d|n}d$ 中取 $f(d)=d$ ，$\nu(n)=\sum_{d|n}\mu(d)$中取 $f(d)=\mu(d)$ ，都是形如

$$F(n)=\sum_{d|n}f(d)\quad (n\in N)\text{（3.1）}$$

的函数。特别地，当$f(n)$是积性函数时，$F(n)$是容易计算的。称(3.1)式是函数$f(n)$的Möbius变换，而由$F(n)$求$f(n)$称为函数$F(n)$的Möbius反变换。

**定理3.2** 设$f(n), F(n)\ (n\in N)$是数论函数，则(3.1)式成立的充要条件是：

$$f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(\frac{n}{d})F(d) \quad (3.2)$$

**证明 必要性：** 假设(3.1)式成立，则

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

由定理3.1的(2)，当$\frac{n}{m}=1$时，$\sum_{d|\frac{n}{m}}\mu(d)=1$；否则$\sum_{d|\frac{n}{m}}\mu(d)=0$。

所以上式等于$f(n)$。

**充分性：** 设(3.2)式成立，则

$$\sum_{d|n} f(d)=\sum_{d|n}\sum_{m|d}\mu(m)F(\frac{d}{m})=\sum_{m|n}\mu(m)\sum_{m|d,\ d|n}F(\frac{d}{m})$$ 。令 $d=mk$，

则 $\sum_{d|n} f(d)=\sum_{m|n}\mu(m)\sum_{k|\frac{n}{m}}F(k)=\sum_{k|n}F(k)\sum_{m|\frac{n}{k}}\mu(m)$ 。

由定理3.1的(2)，当 $\frac{n}{k}=1$ 时，$\sum_{m|\frac{n}{k}}\mu(m)=1$；否则 $\sum_{m|\frac{n}{k}}\mu(m)=0$ 。

所以 $\sum_{d|n} f(d)=F(n)$ 。

证毕。

定理 2.3.2 设 $f(n)$、$F(n)$ $(n\in N)$ 是数论函数，则 $F(n)=\sum_{d|n} f(d)$ 成立的充要条件是

$\boxed{P_{19}}$

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

证明：必要性 $(\Rightarrow)$：$F(n)=\sum_{d|n} f(d) \Rightarrow f(n)=\sum_{d|n}\mu(d)\cdot F\left(\frac{n}{d}\right)$

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

$$\left\{(d,m)\,\middle|\,\left(d|n,\ m\,\middle|\,\frac{n}{d}\right)\right\}$$

$$\Leftrightarrow \left\{(d,m)\,\middle|\,(d|n,\ md|n)\right\}$$

$$\Leftrightarrow \left\{(d,m)\,\middle|\,\left(m|n,\ d\,\middle|\,\frac{n}{m}\right)\right\}$$

$$=\sum_{m|n}\sum_{d|\frac{n}{m}}\mu(d)\cdot f(m)$$

在内循环 $\left[\sum_{d|\frac{n}{m}}\mu(d)\cdot f(m)\right]$ 中 当 $d$ 遍历 $\frac{n}{m}$ 的因子集时 $f(m)$ 是常数，可提出来

$$=\sum_{m|n} f(m)\sum_{d|\frac{n}{m}}\mu(d)$$

$$v(n)=\sum_{d|n}\mu(d)=\left\lfloor\frac{1}{n}\right\rfloor=\begin{cases}1, & n=1\\ 0, & n>1\end{cases}$$

$$=\sum_{m|n} f(m) * \left\lfloor\frac{m}{n}\right\rfloor$$

$$=f(n)$$

充分性（⇐）:

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

$$\sum_{d\mid n} f(d) = \cancel{\sum_{d\mid n} \sum_{m\mid d} \mu(m)\cdot F\left(\frac{d}{m}\right)}$$

$$= \sum_{d\mid n} \sum_{m\mid \frac{n}{d}} \mu(m)\cdot F\left(\frac{n}{md}\right)$$

$$= \sum_{d\mid n} \sum_{m\mid \frac{n}{d}} \mu\left(\frac{n}{md}\right)\cdot F(m)$$

$$= \sum_{m\mid n} \sum_{d\mid \frac{n}{m}} \mu\left(\frac{n}{md}\right)\cdot F(m)$$

$$= \sum_{m\mid n} F(m)\cdot \sum_{d\mid \frac{n}{m}} \mu\left(\frac{n}{md}\right)$$

$$= \sum_{m\mid n} F(m)\cdot \left\lfloor \frac{m}{n} \right\rfloor$$

$$= F(n)$$

证毕。

**推论** $f(n), F(n)$ 如定理3.2所述，则 $f(n)$ 是积性的充要条件是 $F(n)$ 是积性的。

**证明** **必要性：** 即为定理1.2。

**充分性：** 在定理1.3中取 $f(d)=\mu(d), g(\frac{n}{d})=F(\frac{n}{d})$，即得。

证毕。

**Theorem**:

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

if and only if

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

and $f(n)$ is multiplicative if and only if $F(n)$ is multiplicative.

**Example**: From before $n = \sum_{d|n} \phi(n)$. Write $n = p_1^{k_1} \dots p_m^{k_m}$. Then

$$\begin{aligned} \phi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \\ &= n \sum_{d|n} \mu(d) \frac{1}{d} \\ &= n \left(1 - \sum_i \frac{1}{p_i} + \sum_{i \ne j} \frac{1}{p_i p_j} - \dots \right) \\ &= n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right) \end{aligned}$$

which is another way to derive the formula for $\phi$.

Gauss encountered the Möbius function over 30 years before Möbius when he showed that the sum of the generators of $\mathbb{Z}_p^*$ is $\mu(p-1)$. More generally, if $\mathbb{Z}_n^*$ has a generator, then the sum of all the generators of $\mathbb{Z}_n^*$ is $\mu(\phi(n))$. This can be seen by considering the sums of the roots of polynomials of the form $x^d - 1$ where $d|\phi(n)$.

---

Ben Lynn *blynn@cs.stanford.edu*

**例**3.1 设 $n\in N$，$\boldsymbol{n}$的标准分解式是 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ ， 定义

$$\Omega(n)=\begin{cases}\alpha_1+\cdots+\alpha_s, & n>1;\\ 0, & n=1.\end{cases}$$

及 $\lambda(n)=(-1)^{\Omega(n)}\left(n\geq 1\right)$ 。求 $\lambda(n)$ 的Möbius变换。

**解：** 由 $\Omega(mn)=\Omega(m)+\Omega(n)$可得$\lambda(n)$是完全积性的。由定理1.2知，$\lambda(n)$ 的Möbius函数 $F(n)$ 也是积性的，

$$F(p^{\alpha})=\sum_{d|p^{\alpha}}\lambda(d)=\sum_{d|p^{\alpha}}(-1)^{\Omega(d)}=(-1)^{\Omega(1)}+(-1)^{\Omega(p)}+\cdots+(-1)^{\Omega(p^{\alpha})}$$

$$=(-1)^{0}+(-1)^{1}+(-1)^{2}+\cdots+(-1)^{\alpha}=\begin{cases}1, & 2\,|\,\alpha\ ;\\ 0, & 2\nmid\alpha .\end{cases}$$

所以$F(n)=\prod_{i=1}^{s}F(p_i^{\alpha_i})=\begin{cases}1, & n\text{是完全平方，即}2\,|\,\alpha_1,\cdots,2\,|\,\alpha_s\ ;\\ 0, & \text{其他；}\end{cases}$

**例3.2** 求 $F(n)=n^t$ 的Möbius逆变换。

**解：** 易知 $n^t$ 是积性函数，由（3.2）式得

$$f(p^{\alpha})=\sum_{d\mid p^{\alpha}}\mu(d)F(\frac{p^{\alpha}}{d})=\mu(1)F\left(p^{\alpha}\right)+\mu\left(p\right)F\left(p^{\alpha-1}\right)$$

$$=p^{\alpha t}-p^{(\alpha-1)t}=p^{\alpha t}(1-p^{-t})\text{。}$$

所以 $f(n)=\prod_{p\mid n}f(p^{\alpha})=n^t\prod_{p\mid n}(1-p^{-t})$ 。

# 2.4 函数 $\varphi(n)$

## 2.4 函数 $\varphi(n)$

**定义4.1** 设 $n \in N$, $\varphi(n)$ 定义为不大于 $n$ 且与 $n$ 互素的正整数的个数，即 $\varphi(n) = \sum\limits_{\substack{1 \le k \le n \\ (k,n)=1}} 1$。称 $\varphi(n)$ 为 $n$ 的Euler函数。

下表是一些数的Euler函数值。

表4.1 一些数的Euler函数值

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 100 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 40 |

**定理4.1** 设 $n \in N$，则 $\sum_{d|n}\varphi(d)=n$ 。

**证明** 设 $S_n$ 表示有理数的集合 $S_n=\left\{\frac{1}{n},\frac{2}{n},\cdots,\frac{n}{n}\right\}$，$T_n$ 表示 $S_n$ 中即约分数（即分子与分母互素的分数）的集合。显然 $|S_n|=n$ ，$|T_n|=\varphi(n)$。例如，$S_6=\left\{\frac{1}{6},\frac{2}{6},\frac{3}{6},\frac{4}{6},\frac{5}{6},\frac{6}{6}\right\}$ ，$T_6=\left\{\frac{1}{6},\frac{5}{6}\right\}$ 。

将 $S_n$ 中的数全部化简为即约的，得 $S_n'$，如 $S_6'=\left\{\frac{1}{6},\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{5}{6},\frac{1}{1}\right\}$

则 $\frac{e}{d} \in S_n'$ 当且仅当 $d \mid n$，$1 \le e \le d$，且 $(e,d)=1$。即对 $n$ 的固定因子 $d$，$\frac{e}{d}$ 构成集合 $T_d$，所以 $|T_d| = \varphi(d)$。对 $S_n'$ 按照 $d$ 划分，得到不相交的集合 $T_d$。有 $S_n' = \bigcup_{d|n} T_d$，

$n = |S_n'| = \sum_{d|n} T(d) = \sum_{d|n} \varphi(d)$。 证毕。

**定理4.2** 设 $n \in N$，

（1） $\varphi(n)$ 是积性的。

（2） 如果 $n$ 为素数，则 $\varphi(n)=n-1$。如果 $n=p^{\alpha}$（ $p$ 为素数），则 $\varphi(n)=p^{\alpha}-p^{\alpha-1}=p^{\alpha}(1-\frac{1}{p})$ 。

（3） 如果 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ ，$\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$ 。

**证明** （1）在定理4.1中取 $F(n)=n$，由定理3.2，$\varphi(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})$。因$F(n)$是积性的，由定理3.2的推论知$\varphi(n)$是积性的。

（2）如果$n$为素数，则$1,2,\cdots,n-1$ 都与$n$互素，所以$\varphi(n)=n-1$。如果$n=p^{\alpha}$，则在$1,2,\cdots,p^{\alpha}$中与$n$不互素的数一定包含因子$p$，即 $p,2p,3p,\cdots,(p^{\alpha-1})p$ 是与$n$不互素的数，有$p^{\alpha-1}$个。因此与$n$互素的数有
$\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}=p^{\alpha}(1-\frac{1}{p})$ 个。

（3）对 $s$ 用归纳法，当 $s=1$ 时，即为（2）。设 $s-1$ 时成立，则当 $s$ 时，因 $(p_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}}, p_s^{\alpha_s})=1$，由 $\varphi(n)$ 的积性得 $\varphi(n)=\varphi(p_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}})\varphi(p_s^{\alpha_s})$

$$= p_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}}\left[\prod_{i=1}^{s-1}(1-\frac{1}{p_i})\right]p_s^{\alpha_s}(1-\frac{1}{p_s})$$

$$= p_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}}p_s^{\alpha_s}\prod_{i=1}^{s}(1-\frac{1}{p_i})=n\prod_{p|n}(1-\frac{1}{p})$$

证毕。

**例4.1** 求 $F(n)=\varphi(n)$ 的Möbius反变换。

**解** 因 $\varphi(n)$ 是积性的，由定理3.2的推论知它的反变换也是积性的。设 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ ，只需求每一个素因子幂的Möbius反变换。由式（3.2），

$$f(p^\alpha)=\sum_{d\mid p^\alpha}\mu(d)F\left(\frac{p^\alpha}{d}\right)=\mu(1)F(p^\alpha)+\mu(p)F(p^{\alpha-1})$$

$$+\mu(p^2)F(p^{\alpha-2})+\cdots=F(p^\alpha)-F(p^{\alpha-1})$$ 。

当$\alpha=1$时，$F(p^{\alpha})-F(p^{\alpha-1})=p-2=p(1-\frac{2}{p})=p^{\alpha}(1-\frac{2}{p})$ 。

当$\alpha\ge 2$时，$F(p^{\alpha})-F(p^{\alpha-1})=p^{\alpha}-p^{\alpha-1}-(p^{\alpha-1}-p^{\alpha-2})$

$$=p^{\alpha}-2p^{\alpha-1}+p^{\alpha-2}=p^{\alpha}(1-\frac{1}{p})^2$$

所以，由定理1.1得，$f(n)=n\prod_{p\|n}(1-\frac{2}{p})\prod_{p^2|n}(1-\frac{1}{p})^2$ 。

其中$p\|n$表示$p\mid n$但$p^2\nmid n$ 。