定义 1 (莫比乌斯函数) 将 n 质因数分解为 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \alpha_i \geq 1$, 定义 **莫比乌斯函数** 为:

$$\mu(n) := \begin{cases} 0, & \exists i : \alpha_i \geq 2, \\ (-1)^k, & \forall i : \alpha_i = 1. \end{cases}$$

备注 当 $n = 1$ 时, $k = 0$, 则 α_i 的集合为空集, 由于假命题可以推出任何命题, $(\forall x \in \varnothing : x = 1)$ 是真命题, 从而 $\mu(1) = 1$, 可以不用额外定义.

定义 2 (单位数论函数) 并称 $I(n) = S(n) = \sum_{d|n} \mu(d)$ 为 **单位数论函数**.

备注 定义域为正整数、陪域为复数的函数称为 **数论函数** (**算术函数记**). 单位数论函数命名的缘由可以参考定理 8.

定理 1 单位数论函数可表示为

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

证明 $d \mid n \Leftrightarrow \dfrac{n}{d} \mid n$, 故等式第一行成立, 下证第二行.

1. 当 $n = 1$ 时, $S(1) = \mu(1) = 1$.
2. 当 $n > 1$ 时, $S(n) = \sum_{i=1}^{k} \mathrm{C}_k^i (-1)^i = (1-1)^k = 0$.

推论 $[\gcd(i,j) = 1] = \sum_{d|\gcd(i,j)} \mu(d)$, 这个看似无用的结论将在后文求解欧拉函数时用到.

备注 $\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right)$ 这个显然的事实很有用.

定理 2 (莫比乌斯反演定理)

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

证明

1. 充分性

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{i|\frac{n}{d}} f(i) = \sum_{id|n} \mu(d) f(i) \\ &= \sum_{i|n} f(i) \sum_{d|\frac{n}{i}} \mu(d) = \sum_{i|n} f(i) S\left(\frac{n}{i}\right) = f(n). \end{aligned}$$

2. 必要性

$$
\begin{aligned}
\sum_{d|n} f(d) &= \sum_{d|n}\sum_{i|d} F(i)\mu\left(\frac{d}{i}\right) = \sum_{i|d,d|n} F(i)\mu\left(\frac{d}{i}\right)\\
&= \sum_{i|n}\sum_{i|d,\frac{d}{i}|\frac{n}{i}} F(i)\mu\left(\frac{d}{i}\right) = \sum_{i|n} F(i)S\left(\frac{n}{i}\right) = F(n).
\end{aligned}
$$

备注　上述交换求和的方式称为富比尼原理.

定理 3 (莫比乌斯反演定理的乘积形式)

$$
F(n) = \prod_{d|n} f(d) \quad \Leftrightarrow \quad f(n) = \prod_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)}.
$$

证明

1. 充分性

$$
\begin{aligned}
\prod_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)} &= \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n}\prod_{i|\frac{n}{d}} f(i)^{\mu(d)} = \prod_{id|n} f(i)^{\mu(d)}\\
&= \prod_{i|n}\prod_{d|\frac{n}{i}} f(i)^{\mu(d)} = \prod_{i|n} f(i)^{S\left(\frac{n}{i}\right)} = f(n).
\end{aligned}
$$

2. 必要性

$$
\begin{aligned}
\prod_{d|n} f(d) &= \prod_{d|n}\prod_{i|d} F(i)^{\mu\left(\frac{d}{i}\right)} = \prod_{i|n}\prod_{i|d,\frac{d}{i}|\frac{n}{i}} F(i)^{\mu\left(\frac{d}{i}\right)}\\
&= \prod_{i|n} F(i)^{\sum \mu\left(\frac{d}{i}\right)} = \prod_{i|n} F(i)^{S\left(\frac{n}{i}\right)} = f(n)
\end{aligned}
$$

推论　若 $F(n) = \sum_{n|m} f(m)$, 则 $f(n) = \sum_{n|d} \mu\left(\frac{d}{n}\right) F(d)$.

证明

$$
\begin{aligned}
\sum_{n|d} \mu\left(\frac{d}{n}\right) F(d) &= \sum_{n|d} \mu\left(\frac{d}{n}\right) \sum_{d|i} f(i) = \sum_{n|i} f(i) \sum_{d'|\frac{i}{n}} \mu(d')\\
&= \sum_{n|i} f(i) S\left(\frac{i}{n}\right) = f(n)
\end{aligned}
$$

定理 4 (富比尼原理的应用)

$$
\sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor = 1.
$$

证明

$$
\sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor = \sum_{d=1}^{n} \mu(d) \sum_{d|l,l\le n} 1 = \sum_{l=1}^{n}\sum_{d|l} \mu(d) = 1.
$$

定理 5 (欧拉函数的性质)

$$\varphi(n)=n\sum_{d\mid n}\frac{\mu(d)}{d}.$$

证明

$$\begin{aligned}\varphi(n)&=\sum_{m\le n,(m,n)=1}1=\sum_{m=1}^{n}\sum_{d\mid(m,n)}\mu(d)\\&=\sum_{d\mid n}\mu(d)\sum_{d\mid m,m\le n}1=\sum_{d\mid n}\frac{n}{d}\mu(d).\end{aligned}$$

推论 将 n 质因数分解为 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\alpha_i\ge 1$, 则

$$\varphi(n)=n\sum_{d\mid p_1^{\alpha_1}\cdots p_k^{\alpha_k}}\frac{\mu(d)}{d}=n\sum_{d\mid p_1\cdots p_k}\frac{\mu(d)}{d}.$$

定理 6 (欧拉函数的计算) 将 n 质因数分解为 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\alpha_i\ge 1$, 则

$$\varphi(n)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{k}p_i^{\alpha_i-1}\left(p_i-1\right).$$

证明 显然. 但我不知道如何由定理 5 推得.

定义 3 (狄利克雷卷积) $(f*g)(n):=f(n)*g(n):=\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right).$

备注 另一常用形式是 $f(n)*g(n)=\sum_{ab=n}f(a)g(b).$

定理 7 狄利克雷卷积满足 **交换律** 和 **结合律**.

证明 交换律由定理 1 的备注即得, 下证结合律.

$$\begin{aligned}f(n)*[g(n)*h(n)]&=\sum_{ad=n}f(a)\sum_{bc=d}g(b)h(c)=\sum_{abc=n}f(a)g(b)h(c)\\&=\sum_{dc=n}\left(\sum_{ab=d}f(a)g(b)\right)h(c)=[f(n)*g(n)]*h(n).\end{aligned}$$

定理 8 单位数论函数是卷积单位元, 即

$$f(n)*I(n)=I(n)*f(n)=f(n).$$

证明

$$f(n)*I(n)=\sum_{d\mid n}f(d)I\left(\frac{n}{d}\right)=\sum_{d\mid n}f(d)\left\lfloor\frac{d}{n}\right\rfloor=f(n).$$

备注 可利用狄利克雷卷积证明莫比乌斯反演公式.

定义 4 (狄利克雷逆) 若数论函数满足 $f*g=g*f=I$, 则称 f 和 g 互为对方的 **狄利克雷逆**.

备注 后文的 f^{-1} 一律指狄利克雷逆; 在代数中 f^{-1} 一般指逆函数; 在分析中 f^{-1} 一般指倒数.

例子

- $\mu^{-1}(n) = U(n) \equiv 1$.
- $\varphi^{-1}(n) = \sum_{d|n} d\mu(d)$.

定理 9 狄利克雷卷积在 $G = \{f(n) \mid f \text{ 是数论函数, 且 } f(1) \neq 0\}$ 上构成阿贝尔群.

证明 由上可知, 该代数系统是封闭的、结合的、交换的, 且具有幺元, 下证逆元存在.

由定义代入 $n = 1$ 得 $f^{-1}(1) = \dfrac{1}{f(1)}$, 将此式代入定义, 得

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d), \quad (n > 1)$$

因此狄利克雷逆元存在且唯一, 因此 $\langle G, * \rangle$ 是阿贝尔群.

备注 进一步, $\langle G, +, * \rangle$ 还是阿贝尔环.

定理 10 若数论函数 $f(n), g(n)$ 满足 $f(1) \neq 0, g(1) \neq 0$, 则

$$(f * g)^{-1} = f^{-1} * g^{-1}.$$

证明 $f^{-1} * (f * g) = I * g = g$, 这是阿贝尔群的直接推论.

定义 5 (积性函数) 若任意 $\gcd(m, n) = 1$, 有 $f(mn) = f(m)f(n)$, 则数论函数 $f(n)$ 称为 **积性函数**.

定义 6 (完全积性函数) 若 $\forall m, n \in \mathbb{Z}$, 有 $f(mn) = f(m)f(n)$, 则称数论函数 $f(n)$ 为 **完全积性函数**.

例子

- 积性函数: $\mu(n)$, $\varphi(n)$, $\sigma_\lambda(n)$.
- 非积性函数
  - 冯·曼戈尔特函数: 当 n 是质数 p 的整数幂时 $\Lambda(n) = \ln(p)$, 否则 $\Lambda(n) = 0$.
  - 不大于正整数 n 的质数的数量 $\pi(n)$.
  - 整数拆分的数目 $P(n)$.

定理 11 (积性函数的性质)

1. 若积性函数 $f(n)$ 非恒等于 0, 则 $f(1) = 1$.
2. 若 $f(n)$ 和 $g(n)$ 都是积性函数, 则 $f(n) * g(n)$ 也是积性函数.
3. 若 $f(n)$ 是积性函数, 则 $f^{-1}(n)$ 也是积性函数.
4. 若 $f(n) * g(n)$ 和 $g(n)$ 都是积性函数, 则 $f(n)$ 也是积性函数.

证明

1. 记 $f(a) \neq 0$, 则由 $f(1)f(a) = f(a)$ 可推出 $f(1) = 1$.

2.
$$
\begin{aligned}
(f*g)(mn) &= \sum_{d\mid mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{a\mid m, b\mid n} f(ab)g\left(\frac{mn}{ab}\right) \\
&= \left(\sum_{a\mid m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b\mid n} f(b)g\left(\frac{n}{b}\right)\right) \\
&= [(f*g)(m)]\cdot[(f*g)(n)].
\end{aligned}
$$

3. 利用递推表达式, 使用数学归纳法.

   1. 当 $mn=1$ 时, $f^{-1}(1)=\dfrac{1}{f(1)}=1.$

   2. 当 $mn>1$ 时,

$$
\begin{aligned}
f^{-1}(mn) &= \frac{-1}{f(1)} \sum_{d\mid mn, d<mn} f\left(\frac{mn}{d}\right) f^{-1}(d) \\
&= -\sum_{a\mid m, b\mid n, ab<mn} f\left(\frac{m}{a}\right) f^{-1}(a) f\left(\frac{n}{b}\right) f^{-1}(b) \\
&= -\left(\sum_{a\mid m, a<m} \sum_{b\mid n, b<n} + \sum_{a=m, b\mid n, b<n} + \sum_{b=n, a\mid m, a<m}\right) \\
&\qquad f\left(\frac{m}{a}\right) f^{-1}(a) f\left(\frac{n}{b}\right) f^{-1}(b) \\
&= -\left[f^{-1}(m)f^{-1}(n) - f^{-1}(m)f^{-1}(n) - f^{-1}(m)f^{-1}(n)\right] \\
&= f^{-1}(m)f^{-1}(n).
\end{aligned}
$$

4. 由 $f=(f*g)*g^{-1}$ 知其为积性函数.