Dirichlet卷积

Lemma (Dirichlet卷积满足对加法的分配律) 对$\forall$算术函数 f, g, h，有:

① $f*(g+h) = f*g + f*h$

② $(f+g)*h = f*h + g*h$

Proof: ①: $\because$ g和h是 $\mathbb{Z}_{\geq 1} \to \mathbb{C}$ 的映射

$\therefore$ $g+h: \mathbb{Z}_{\geq 1} \longrightarrow \mathbb{C}$ 也是 $\mathbb{Z}_{\geq 1} \to \mathbb{C}$ 的映射

$$x \longmapsto (g+h)(x) = g(x) \underset{\substack{\downarrow \\ \mathbb{C}\text{中的加法}}}{+} h(x)$$

$\therefore$ $f*(g+h)$ 是算术函数.

$\because$ $f*g$ 和 $f*h$ 都是算术函数 $\therefore$ $f*g+f*h$ 也是算术函数.

对$\forall n \in \mathbb{Z}_{\geq 1}$，有:

$$\begin{aligned}
\big(f*(g+h)\big)(n) &= \sum_{\substack{d \mid n \\ d \in \mathbb{Z}_{\geq 1}}} f(d)\,(g+h)\left(\frac{n}{d}\right) \\
&= \sum_{\substack{d \mid n \\ d \in \mathbb{Z}_{\geq 1}}} f(d) \underset{\substack{\downarrow \\ \mathbb{C}\text{中的乘法}}}{\left(\vphantom{\frac{n}{d}}\right.} g\left(\frac{n}{d}\right) \underset{\substack{\downarrow \\ \mathbb{C}\text{中的加法}}}{+} h\left(\frac{n}{d}\right)\left.\vphantom{\frac{n}{d}}\right) \\
&= \sum_{\substack{d \mid n \\ d \in \mathbb{Z}_{\geq 1}}} \left(f(d)\,g\left(\frac{n}{d}\right) + f(d)\,h\left(\frac{n}{d}\right)\right) \\
&= \sum_{\substack{d \mid n \\ d \in \mathbb{Z}_{\geq 1}}} f(d)\,g\left(\frac{n}{d}\right) + \sum_{\substack{d \mid n \\ d \in \mathbb{Z}_{\geq 1}}} f(d)\,h\left(\frac{n}{d}\right) \\
&= (f*g)(n) + (f*h)(n) = (f*g+f*h)(n)
\end{aligned}$$

$\therefore\ f*(g+h) = f*g + f*h$

② $(f+g)*h = h*(f+g) = h*f + h*g = f*h + g*h$ $\square$

定义（Dirichlet卷积的单位元）定义 $\varepsilon: \mathbb{Z}_{\geq 1} \longrightarrow \mathbb{C}$ 为：

$$\begin{aligned} \varepsilon: \mathbb{Z}_{\geq 1} &\longrightarrow \mathbb{C} \\ 1 &\longmapsto 1 \\ \underset{(n\geq 2)}{n} &\longmapsto 0 \end{aligned}$$

Lemma：对$\forall$算术函数 f，有：$\varepsilon * f = f = f * \varepsilon$

Proof：$\because$ ε是算术函数 $\therefore$ $\varepsilon * f$ 和 $f*\varepsilon$ 都是算术函数.

对$\forall\, n \in \mathbb{Z}_{\geq 1}$，有：

$$(\varepsilon * f)(n) = \sum_{\substack{d|n \\ d\in\mathbb{Z}_{\geq 1}}} \varepsilon(d) f\left(\frac{n}{d}\right) = \varepsilon(1) f(n) = f(n)$$

$\therefore\ \varepsilon * f = f$

$\therefore\ f*\varepsilon = \varepsilon * f = f$ $\square$

定义（常值函数 1）定义 $1: \mathbb{Z}_{\geq 1} \longrightarrow \mathbb{C}$ 为：

$$\begin{aligned} 1: \mathbb{Z}_{\geq 1} &\longrightarrow \mathbb{C} \\ n &\longmapsto 1 \end{aligned}$$

Lemma（Möbius 函数求和公式）对 $\forall n\in\mathbb{Z}_{\geq 1}$，有：

$$\sum_{\substack{d\mid n\\ d\in\mathbb{Z}_{\geq 1}}}\mu(d)=\begin{cases}1 & \text{当}n=1\text{时}\\ 0 & \text{当}n\geq 2\text{时}\end{cases}$$

Proof：当 $n=1$ 时，$d\mid n$ 且 $d\in\mathbb{Z}_{\geq 1}\iff d=1$

$$\therefore \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_{\geq 1}}}\mu(d)=\mu(1)=1$$

对 $\forall n\in\mathbb{Z}_{\geq 2}$，有：$n$ 有素因子分解：$n=p_1^{a_1}\cdots p_r^{a_r}$，其中 $r\in\mathbb{Z}_{\geq 1}$，$p_1,\cdots,p_r$ 是相异素数，$a_1,\cdots,a_r\in\mathbb{Z}_{\geq 1}$

又对 $\forall d\in\mathbb{Z}_{\geq 1}$，有：$d\mid n\iff d=p_1^{e_1}\cdots p_r^{e_r}$，其中 $e_1,\cdots,e_r\in\mathbb{Z}_{\geq 0}$，$e_1\leq a_1,\cdots,e_r\leq a_r$

$\therefore \mu(d)=0\iff \exists e_i\geq 2\ (i\in\{1,\cdots,r\})$

$\mu(d)\neq 0\iff$ 对 $\forall i=1,\cdots,r$，$e_i=0$ 或 1

$$\therefore \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_{\geq 1}}}\mu(d)=\cancel{\binom{n}{0}\mu(1)+}\ \mu(1)+\sum_{i=1}^{r}\mu(p_i)+\sum_{\substack{i<j\\ i,j\in\{1,\cdots,r\}}}\mu(p_ip_j)$$

$$+\sum_{\substack{i<j<k\\ i,j,k\in\{1,\cdots,r\}}}\mu(p_ip_jp_k)+\cdots+\mu(p_1\cdots p_r)$$

$$=1+\binom{r}{1}(-1)^1+\binom{r}{2}(-1)^2+\binom{r}{3}(-1)^3+\cdots+\binom{r}{r}(-1)^r$$

$$=(1+(-1))^r=0^r=0\qquad\square$$

Lemma: $1 * \mu = \varepsilon = \mu * 1$

proof: ∵ 常值函数 1 和 Möbius 函数 μ 都是算术函数 ∴ $1*\mu$ 是算术函数.

对 $\forall n \in \mathbb{Z}_{\geq 1}$, 有:

$$\cancel{(1*\mu)(n) = \sum_{\substack{d|n \\ d\in\mathbb{Z}}} 1(d)\mu\left(\frac{n}{d}\right)}$$

$$(\mu*1)(n) = \sum_{\substack{d|n \\ d\in\mathbb{Z}_{\geq 1}}} \mu(d)\,1\left(\frac{n}{d}\right) = \sum_{\substack{d|n \\ d\in\mathbb{Z}_{\geq 1}}} \mu(d) = \begin{cases} 1 & \text{当 } n=1 \text{ 时} \\ 0 & \text{当 } n\geq 2 \text{ 时} \end{cases} = \varepsilon(n)$$

∴ $\mu * 1 = \varepsilon$

∴ $1*\mu = \mu * 1 = \varepsilon$ □

定理 (Möbius 反演公式) 对 $\forall$ 算术函数 f, g, 有:

$$g = f*1 \iff f = g*\mu$$

Proof: ($\Rightarrow$): ∵ $g = f*1$

∴ $g*\mu = (f*1)*\mu = f*(1*\mu) = f*\varepsilon = f$

∴ $f = g*\mu$

($\Leftarrow$): ∵ $f = g*\mu$

∴ $f*1 = (g*\mu)*1 = g*(\mu*1) = g*\varepsilon = g$

∴ $g = f*1$ □