数论函数

Nicolas Keng

2023/12/24

我们先回顾所谓数论函数 (number theoretic function), 即定义在 $\mathbb{N}_+$ 上的复值函数, 其中的两类函数尤其重要:

定义 1.1 若数论函数 f 和 $\gcd(m,n)=1$ 满足

1. $f(mn)=f(m)+f(n)$, 则称它是加性 (additive) 的, 这时 $f(1)=0$;
2. $f(mn)=f(m)f(n)$, 则称它是乘性 (multiplicative) 的, 这时 $f(1)=1$.

若上述等式对不互素的正整数 m,n 也成立, 则称 f 完全加性或完全乘性.

例 1.1 n 的素因子个数: 计重数 Ω, 不计重数 ω,

$$\Omega(n)=\sum_{p^v\|n} v,\quad \omega(n)=\sum_{p^v\|n}1=\sum_{p|n}1.$$

$\Omega(n)$ 完全加性, $\omega(n)$ 加性.

例 1.2 n 的因子个数和因子 λ 次幂和:

$$\sigma_\lambda(n)=\sum_{d|n} d^\lambda,\ (\lambda\in\mathbb{C}),\quad \tau(n)=\sigma_0(n)=\sum_{d|n}1,\quad \sigma(n)=\sigma_1(n)=\sum_{d|n} d.$$

$\sigma_\lambda(n)$ 表 $x_1x_2\cdots x_\lambda=n$ 自然数解的组数, $\tau(n)$ 表 n 正因子个数; $\tau(n)$ 乘性, 且 $\tau(n)=\prod\limits_{p^v\|q}(v+1)$.

例 1.3 Euler 示性函数 ($\mathbb{Z}/n\mathbb{Z}$ 的单位群之阶 $|\mathbb{F}_n^\times|$):

$$\varphi(n)=\sum_{\substack{1\le d\le n,\\ \gcd(d,n)=1}} 1.$$

$\varphi(n)$ 表不大于 n 且与 n 互素的自然数的个数.

命题 1.1 Euler 函数 $\varphi(n)$ 具有如下性质:

1. $\varphi(n)$ 乘性且 $\varphi(n)=n\prod\limits_{p|n}\left(1-\dfrac{1}{p}\right)$, 但对 $\gcd(m,n)=d$, $\varphi(mn)=\varphi(m)\varphi(n)\left(\dfrac{d}{\varphi(d)}\right)$;
2. $n=\sum\limits_{d|n}\varphi(d)$, $m|n\Rightarrow\varphi(m)|\varphi(n)$.

证明概要 乘性: 将求和指标 $1 \le d \le n, \gcd(d,n) = 1$ 和 $1 \le d \le m, \gcd(d,m) = 1$ 拼成 $1 \le d \le mn, \gcd(d,mn) = 1$ 即可 (验证拼指标是双射).

不完全乘性: 取 n 的单位分解 $n = \prod_{k=1}^{l} p_k^{r_k}$, 注意到 $\varphi(p^m) = p^m - p^{m-1}$, 迭代:

$$\varphi(n) = \prod_{k=1}^{l} p_k^{r_k-1}(p_k - 1) = n \prod_{k=1}^{l} \left(1 - \frac{1}{p_k}\right).$$

求和: 验证 $f(n) = \sum_{d|n} \varphi(d)$ 乘性, 迭代有 $f(p^m) = p^m$; 也可以直接考虑自然数按照某 $d = \gcd(n,k)$ 分类, 满足 $\gcd\left(x, \frac{k}{d}\right)$ 的 k 个数为 $\varphi(k) = \varphi\left(\frac{n}{d}\right)$ 然后求和. □

Möbius 反演变换

例 1.4 Möbius 函数:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & n = p^2 m \\ (-1)^k & n = p_1 p_2 \cdots p_k \end{cases}$$

$\mu(n)$ 乘性, 但不完全乘性 (讨论是否有平方因子即可). 熟知我们应该有

命题 1.2

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1. \end{cases}$$

这里 $I(n)$ 是单位示性函数, 实际上是所有数论函数的环 $\mathbb{A}$ 上的幺元.

证明概要 直接取 n 的标准分解后验证. □

我们直接引入如下的 Möbius 变换公式, 这里的基础是对任意数论函数 f, 指标求和具有对偶性:

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

定理 1.1 $\mathbb{N}$-Möbius 变换: 对数论函数 f 和 g, 则以下两命题等价:

1. $g(n) = \sum_{d|n} f(d)$, $(n \in \mathbb{N}_+)$;
2. $f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$, $(n \in \mathbb{N}_+)$.

此时, $g(n)$ 称作 $f(n)$ 的 Möbius 变换, 一般记作 $f \overset{\mu}{\rightharpoonup} g$; $f(n)$ 称作 $g(n)$ 的 Möbius 逆变换.

证明概要 $\Rightarrow$: 依定义展开,

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

期望逆转 μ 和 g 的求和顺序. 形式地, 我们探讨逆转后 $\sum f(m)\sum \mu(d)$ 的指标范围. 依次考虑约束条件, 应该有:

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

其展示了整除的对偶性. 然后注意到 $\sum_{d|\frac{n}{m}}\mu(d)=I\left(\frac{n}{m}\right)$, 代入计算即可. 反向类似:

$$\sum_{d|n}f(d)=\sum_{d|n}\sum_{m|d}\mu(m)g\left(\frac{d}{m}\right)=\sum_{m|n}\mu(m)\sum_{r|\frac{n}{m}}g(r)=\sum_{r|n}g(r)\sum_{m|\frac{n}{r}}\mu(m)=\sum_{r|n}g(r)I\left(\frac{n}{r}\right)=g(n).$$

□

定理 1.2 $\mathbb{R}$-Möbius 变换: 设 F 和 G 是在 $[1,+\infty)$ 上定义的函数, 则以下两命题等价:

1. $F(x)=\sum_{n\leq x}G\left(\frac{x}{n}\right),\ (x\geq 1);$
2. $G(x)=\sum_{n\leq x}\mu(n)F\left(\frac{x}{n}\right),\ (x\geq 1).$

此时令 $G(x)\equiv 1$, 即 $\sum_{n\leq x}\mu(n)\lfloor\frac{x}{n}\rfloor=1$, 进而 $\lim_{x\to+\infty}\sum_{n\leq x}\frac{\mu(n)}{n}=0$. 这个结论与素数定理等价.

Möbius 变换是数论中很重要的一个技术手段.

例 1.5 Von mangoldt 函数:

$$\Lambda(n)=\begin{cases}\log p & n=p^v\\ 0 & n\neq p^v\end{cases}$$

命题 1.3 我们有 $-\mu(n)\log n\xrightarrow{\mu}\Lambda(n)\xrightarrow{\mu}\log n.$

证明概要 后者: 设 n 的标准分解式为 $p_1^{l_1}\cdots p_r^{l_r}$, 则有

$$\begin{aligned}\sum_{d|n}\Lambda(d)&=\sum_{k_1=0}^{l_1}\cdots\sum_{k_r=0}^{l_r}\Lambda\left(p_1^{k_1}\cdots p_r^{k_r}\right)\\&=\sum_{k_1=0}^{l_1}\Lambda\left(p_1^{k_1}\right)+\cdots+\sum_{k_r=0}^{l_r}\Lambda\left(p_r^{k_r}\right)\\&=\sum_{k_1=0}^{l_1}\log p_1+\cdots+\sum_{k_r=0}^{l_r}\log p_r\\&=l_1\log p_1+\cdots+l_r\log p_r=\log n,\end{aligned}$$

前者: 代入 Möbius 逆变换, 我们有:

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d}=\log n\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\log d=-\sum_{d|n}\mu(d)\log d.$$

□

推论 $\forall\gcd(m,n)=1,\Lambda(mn)=I(n)\Lambda(m)+I(m)\Lambda(n).$

Dirichlet 卷积

定义 1.2 对于数论函数 f, g, 称

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

为 f 与 g 的 Dirichlet 卷积 (convolution), 记为 $h = f * g$.

定理 1.3 Dirichlet 卷积满足交换律和结合律.

证明概要 交换律: 注意到 $(f*g)(n) = \sum\limits_{ab=n} f(a)g(b)$, 对称, $f*g = g*f$.

结合律: 代入上式,

$$(f*g*h)(n) = \sum_{ab=n} f(a)(g*h)(b) = \sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d),$$

对称, $(f*g)*h = f*(g*h)$. □

显然 $f*I = I*f = f$, 且已证过 $\mu*1 = I$, 这里 $1(n) \equiv 1$. 于是我们可以简化 $\mathbb{N}$-Möbius 变换 (定理 1.1) 的证明:

定理 1.4 $\mathbb{N}$-Möbius 变换: 对数论函数 f 和 g, $g = f*1 \iff f = g*\mu$.

证明概要 $\Rightarrow$: $g*\mu = f*1*\mu = f*(\mu*1) = f*I = f$;

$\Leftarrow$: $f*1 = g*\mu*1 = g*(\mu*1) = g*I = g$. □

例 1.6 我们用卷积的语言重述若干 Möbius 变换和 Möbius 逆变换的例子:

1. 恒等函数 $\mu(n) \xrightarrow{\mu} I(n) \xrightarrow{\mu} 1$, 即 $I = \mu*1, 1 = I*1$;
2. 因子幂和 $n^\lambda \xrightarrow{\mu} \sigma_\lambda(n)$, 即 $\sum\limits_{d|n} d^\lambda = n^\lambda * 1$;
3. Euler 函数 $\varphi(n) \xrightarrow{\mu} n$, 即 $n = \varphi(n) * 1$;
4. Von mangoldt 函数 $-\mu(n)\log n \xrightarrow{\mu} \Lambda(n) \xrightarrow{\mu} \log n$, 即 $\log = \Lambda * 1, \Lambda = -\mu\log * 1 = \mu * \log$.

我们讨论和卷积有关的指标变换问题. 首先,

定理 1.5 若 f 是一个数论函数且 $f(1) \neq 0$, 则存在唯一的一个数论函数 g 使得

$$f*g = g*f = I,$$

称 g 为 f 的 Dirichlet 逆, 记为 f^{-1}, 并且满足

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

证明概要 我们归纳证明 $\left(f*f^{-1}\right)(n) = I(n)$ 对函数值 $f^{-1}(n)$ 的解唯一. $n=1$ 时显然, 假设 $\forall k < n$, 函数值 $f^{-1}(k)$ 唯一确定, 则展开 $f*f^{-1}$ 为

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = f(1)f^{-1}(n) + \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0,$$

由数学归纳法得证. □

定理 1.6 *若数论函数 f, g 都是乘性的, 则卷积 $f * g$ 也是乘性的.*

证明概要 我们将 d 也写作乘积. 考虑 $h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$, m, n 互素; 令 $a = \gcd(m, d)$, $b = \gcd(n, d)$, 则 $d = ab$. 于是代入计算,

$$\begin{aligned} h(mn) &= \sum_{a|m, b|n} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{a|m, b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) = h(m)h(n). \end{aligned}$$

□

定理 1.7 *若数论函数 f, g 满足 g 和 $h = f * g$ 都乘性, 则 f 也是乘性的.*

证明概要 反证, 假设存在互素的 m, n 使得 $f(mn) \neq f(m)f(n)$, 取最小的 $mn \neq 1$, 则

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m, b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\ &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) - f(m)f(n) + f(mn) \\ &= h(m)h(n) - f(m)f(n) + f(mn), \end{aligned}$$

矛盾! □

于是我们注意到 $g * g^{-1} = I$, 有

推论 *若数论函数 f 乘性, 则 f^{-1} 也乘性.*

形式 Dirichlet 级数

这部分需要适当抽象代数的基础, 若无可以跳过命题 1.4, 定理 1.8 和命题 1.5, 不会影响阅读.

定义 1.3 *设 f 为数论函数, 则称形式级数 (L-函数)*

$$L(f)(S) = D(f, s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

为 f 的形式 Dirichlet 级数. 这只是形式和, 不涉及敛散性. 取 $f(n) \equiv 1$, 即有 ζ 函数

$$D(1, s) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

我们在 $D(f, s)$ 上定义加法和乘法:

$$D(f + g, s) = D(f, s) + D(g, s), \quad D(f * g, s) = D(f, s) \cdot D(g, s),$$

由此我们固定 $s \in \mathbb{C}$, 有双射 $T(f) = D(f, s)$. 容易验证数论函数的全体 $\mathbb{A}$ 在通常的加法与卷积下构成交换环, Dirichlet 级数的全体 $\mathbb{D}$ 也构成一个交换环, 双射 T 诱导环同构. 于是

命题 1.4 $\mathbb{A}$ 的单位群 $\mathbb{A}^\times$ 由满足 $f(1)\neq 0$ 的全体数论函数组成.

证明概要 考虑 $\forall g\in\mathbb{A}$ 与 $f(1)\neq 0$, 利用 $g(1)=\dfrac{1}{f(1)}$ 与所有 $g(d)$, $(d|n)$ 可以计算出所有的 $g(n)$:

$$g(n)=\frac{-1}{f(1)}\sum_{d|n,d\neq n} f\left(\frac{n}{d}\right)g(d).$$

□

推论 乘性函数 f 都可逆, 且 $f(1)=1$.

事实上我们有

定理 1.8 (Cashwell, 1959): 所有数论函数的集合 $\mathbb{A}$ 构成整环; 它事实上是 UFD.

不难验证此时 $T(\mathbb{A})$ 也为整环, 称为 Dirichlet 级数环, 记为 $\mathbb{D}$.

我们可以从 Dirichlet 级数角度考虑乘性. 先从一个熟知的乘积开始:

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1},$$

该公式可以由以下更广义的结论推出:

命题 1.5 数论函数 f 是乘性的充要条件是它的形式 Dirichlet 级数可以展开成 Euler 乘积:

$$D(f,s)=\prod_p\left(1+\sum_{v\geq 1}\frac{f\left(p^v\right)}{p^{vs}}\right).$$

我们可以得到 Möbius 变换与 Dirichlet 级数的关系:

$$f\overset{\mu}{\to}g\iff D(g,s)=\zeta(s)D(f,s),$$

由其可以重述例 1.6 中的 Möbius 变换:

例 1.7 我们用 Dirichlet 级数的语言重述若干 Möbius 变换和 Möbius 逆变换的例子:

1. 恒等函数 $\mu(n)\overset{\mu}{\to}I(n)\overset{\mu}{\to}1$, 即 $D(I,s)=1$, $D(\mu,s)=\dfrac{1}{\zeta(s)}$;
2. 因子幂和 $n^\lambda\overset{\mu}{\to}\sigma_\lambda(n)$, 即 $D(\sigma_\lambda,s)=\zeta(s)\zeta(s-\lambda)$;
3. Euler 函数 $\varphi(n)\overset{\mu}{\to}n$, 即 $D(\varphi,s)=\dfrac{\zeta(s-1)}{\zeta(s)}$.

特殊地, 我们利用 Dirichlet 级数重述 Von mangoldt 函数. 定义数论函数 f 的导数为 $f'(n)=f(n)\log(n)$, 从 ζ 函数出发,

$$\zeta'(s)=-\sum_{n=1}^{\infty}\frac{\log n}{n^s}=-D(\log,s),$$

$$\frac{\mathrm{d}^k}{\mathrm{d}s^k}\zeta(s)=(-1)^k\sum_{n=1}^{\infty}\frac{\log^k n}{n^s}=(-1)^kD\left(\log^k,s\right).$$

对 ζ 函数的 Euler 乘积取对数再取导数,

$$\log\zeta(s) = -\sum_p \log\left(1-\frac{1}{p^s}\right) = \sum_p\sum_{n=1}^{\infty}\frac{1}{np^{sn}},$$

$$\frac{\zeta'}{\zeta}(s) = -\sum_p\sum_{n=1}^{\infty}\frac{\log n}{p^{sn}} = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = -D(\Lambda,s).$$

由此及乘积性质可以建立 Von mangoldt 函数与自然对数间的 Möbius 变换关系.

定理 1.9 Selberg 公式:

$$\sum_{n\le x}\Lambda(n)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x),$$

我们考虑其初等形式

$$\Lambda(n)\log n = \sum_{d|n}\mu\left(\frac{n}{d}\right)\log^2 d - \sum_{d|n}\Lambda(d)\Lambda\left(\frac{n}{d}\right).$$

这部分的证明简化自[TravorLZH: Selberg 渐近公式 (https://zhuanlan.zhihu.com/p/360553655)].

证明概要 利用 Dirichlet 级数可以给出一个简洁的证明. 有

$$\frac{\zeta'}{\zeta}(s) = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = -D(\Lambda,s),$$

求导

$$\frac{\mathrm{d}}{\mathrm{d}s}\frac{\zeta'}{\zeta}(s) = \frac{\zeta''}{\zeta}(s) - \left(\frac{\zeta'}{\zeta}(s)\right)^2 = \sum_{n=1}^{\infty}\frac{\Lambda(n)\log n}{n^s} = D(\Lambda\cdot\log,s),$$

于是直接考虑级数分解

$$D(\Lambda\cdot\log,s) = D\left(\log^2,s\right)D(\mu,s) - D^2(\Lambda,s) = D\left(\log^2\circ\mu - \Lambda\circ\Lambda,s\right)$$

即证. □

这实际上已经是偏向解析数论的方法了.

对于进一步学习, 华罗庚: 数论导引和 Apostol: Introduction to Analytic Number Theory 都是很好的解析数论入门选择; 若复分析基础较为薄弱, Stein: Complex Analysis 和 Karatsuba: Basic Analytic Number Theory 也是很好的选择.

代数方向来讲, 冯克勤: 代数数论无疑是入门的最佳教材, 加藤和也: 数论 I 也是软入门的不二之选. 剩下的事情, 就留待大家自己探索了. 前路漫漫, 最后以一句话作为共勉:

Wir müssen wissen. Wir werden wissen.

我们必将知道, 我们终将知道.