メビウス関数 (Möbius function)

目次

1 メビウス関数 (Möbius function)

定義 1 : メビウス関数 (Möbius function) 正の整数 n に対して以下の関数

$$\mu(n) = \begin{cases} 0, & n \text{ が } 1 \text{ 以外の平方因子をもつとき} \\ (-1)^k, & n \text{ が } k \text{ 個の異なる素因数を持つとき} \end{cases}$$

をメイビウス関数とする。また、$\mu(1) = 1$ とする。

定理 1 : 任意の互いに素な正の整数 m, n に対して $\mu(m)\mu(n) = \mu(mn)$ が成立する。

定理 2 : 正の整数 $2 \geq 2$ に対して、

$$\sum_{d|n} \mu(d) = 0$$

となる。

Proof. n の標準素因数分解 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ と書くとする。ここで n のある約数 d に対して $\mu(d) \neq 0$ となる必要十分条件は $d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, $(\delta_i \in \{0, 1\}, 1 \leq i \leq k)$ と書けること

である。したがって

$$\sum_{d|n}\mu(d) = \sum_{\delta_i\in\{0,1\}}\mu(p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}) = \sum_{\delta_i\in\{0,1\}}(-1)^{\delta_1+\delta_2+\cdots+\delta_k} = \sum_{i=0}^{k}(-1)^k\binom{k}{i}$$

となる。二項定理から

$$\sum_{i=0}^{k}(-1)^k\binom{k}{i} = (1-1)^k = 0$$

が示される。 □

2 メビウスの反転公式 (Möbius inversion formula)

<u>定理 **3 :**</u> メビウスの反転公式 (Möbius inversion formula) 正の整数集合を定義域とする関数 $f(n), g(n)$ に対して

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

が成り立つ。この関係式をメビウスの反転公式という。

Proof. まず $f(n) = \sum_{d|n}g(d) \Leftarrow g(n) = \sum_{d|n}\mu(\frac{n}{d})f(d)$ を示す。この左辺の式を代入することで、

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

となる。ここで $m = \frac{n}{d'}, d^* = \frac{d}{d'}$ とおくと、$d^*|m$ を満たす d^* の集合と $d'|d|m$ を満たす d の集合は一体一対応する。さらに、$\frac{n}{d} = \frac{m}{d^*}$ であるため

$$\sum_{d'|n}g(d')\sum_{d'|d|n}\mu\left(\frac{n}{d}\right) = \sum_{d'|n}g(d')\sum_{d^*|m}\mu\left(\frac{m}{d^*}\right)$$

となる。前述の定理から

$$\mu\left(\frac{m}{d^*}\right) = \begin{cases} 0, & m \neq 0 \\ 1, & m = 0 \end{cases}$$

であるため

$$\sum_{d'|n} g(d') \sum_{d^*|m} \mu\left(\frac{m}{d^*}\right) = g(n)$$

となり示された。同様にして $f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$ も示される。 □

3　乗法的関数とディクレ畳み込み

定義 2 : 数論的関数 (arithmetic function) 正の整数の集合を $\mathbb{N}$ とし複素数の集合を $\mathbb{C}$ としたとき

$$f : \mathbb{N} \to \mathbb{C}$$

である写像 f を数論的関数という。

定義 3 : 乗法的関数 (multiplicative function) ある数論的関数 $f : \mathbb{N} \to \mathbb{C}$ が、任意の互いに素な $m, n \in \mathbb{N}$ に対して

$$f(m)f(n) = f(mn)$$

であるとき、f を乗法的関数という。

オイラー関数やメビウス関数、0 以上の約数の個数、約数の個数、値域が 1 の定数関数、恒等関数、1 の指示関数 (1 のときのみ 1 でそれ以外 0 の関数) 等が乗法的関数にあたる。

定義 4 : ディリクレ畳み込み (Dirichlet convolution) 数論的関数 f, g に対して、$f * g$ を

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b)$$

と定義し、これをディリクレ畳み込みという。

定理 4 : ディリクレ畳み込みに対して、一般の畳み込み和等で成立するのと同じように以下が成立する。

i. $f * g = g * f$ (可換性)
ii. $(f + g) * h = f * h + g * h$ (分配律)
iii. $(f * g) * h = f * (h * g)$ (結合律)
iv. $f * \varepsilon$ (単位元)

ここで ε は 1 の指示関数である。

このディリクレ畳み込みは乗法的関数に対する 2 項演算である。例として以下があげられる。

i. $\mu * \mathbf{1} = \varepsilon$
ii. $\varphi * \mathbf{1} = \mathrm{id}$

ここで $\mathbf{1}$ は値域が 1 の定数関数であり、id は恒等関数である。これはメビウス関数のディリクレ畳み込みに対する逆元が $\mathbf{1}$ であるとも言うことができる。よってメビウス反転公式はディリクレ畳み込みによって

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

と書くことができる。ディリクレ畳み込みの性質を用いると簡単に証明することができる。

ディリクレ畳み込みで書かれる

$$\varphi = \mu * \mathrm{id}$$

はよく知られている。この式にディリクレ反転公式を適用すれば

$$\mathrm{id} = \varphi * \mathbf{1}$$

が得られる。これはオイラー関数の性質として知られる式

$$n = \sum_{d|n} \varphi(d)$$

そのものである。

また、ディリクレ畳み込みに対する逆元は以下のディリクレ逆と呼ばれる。

定義 5 : ディリクレ逆 (Dirichlet inverse) ある数論的関数 f に対して $f * g = \varepsilon$ が成立する数論的関数 g をディレイクレ逆という。ディリクレ逆は任意の $f(1) =\neq 0$ を見たす数論的関数に存在する。

4　ディリクレ母関数 (Dirichlet generating function)

定義 6 : ディリクレ級数 (Dirichlet series) 数論的関数 f に対して

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

と書かれる級数をディリクレ級数という。これは数列 $\{f(n)\}_{n\geq 1}$ に付随するディリクレ母関数 (Dirichlet generating function) であるともいう。またディリクレ変換ともいうことができる。

ディリクレ級数とディリクレ畳み込みに対して

$$D(f;s)D(g;s) = D(f*g;s)$$

が成立し、ディリクレ級数を数論的関数におけるフーリエ変換とみることができることがわかる。

リーマンゼータ関数 (Riemann zeta function) は

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = D(\mathbf{id};s)$$

と書けるため

$$D(f;s) = \zeta(s)D(g;s)$$

た成り立つ。

5　反転公式の応用

5.1　周期性をもたない文字列の数

有限集合 Ω をアルファベットとし、Ω^n の元を長さ n の文字列とする。2 つの文字列 $\mathbf{x},\mathbf{y}$ に対して $\mathbf{x}*\mathbf{y}$ を $\mathbf{x}$ と $\mathbf{y}$ を連結 (concatenation) したものとする。次に文字列の周期を定義する。

定義 7： 文字列の周期ある文字列 $\mathbf{x} \in \Omega^n$ に対してある $\mathbf{y} \in \Omega^d$ が存在し

$$\mathbf{x} = \mathbf{y} * \mathbf{y} * \cdots * \mathbf{y}$$

と書けるとき、$\mathbf{x}$ は周期 d を持つという。また $d|n$ であることは自明である。さらに、文字列 $\mathbf{x}$ がもつ周期のうち最小のものが d であるとき、d を $\mathbf{x}$ の最短周期という。

また $\mathcal{F},\mathcal{G}$ をそれぞれ

$$\mathcal{F}(d) = \left\{\mathbf{x} \in \Omega^n \;\middle|\; \mathbf{x}\text{ が周期 }d\text{ をもつ}\right\}$$
$$\mathcal{G}(d) = \left\{\mathbf{x} \in \Omega^n \;\middle|\; \mathbf{x}\text{ の最短周期が }d\text{ である}\right\}$$

とする。$\mathcal{F}(n)$ が長さ n の文字列集合 Ω^n と一致するのは自明であり、また $\mathcal{G}(d)$ $(d|n)$ によって Ω^n が分割される。したがって、数論的関数 f,g をそれぞれ $f(n) = |\mathcal{F}(n)|, g(n) = |\mathcal{G}(n)|$ とすれば

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

が成立する。メビウスの反転公式から

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

が成立し、$f(d) = |\Omega|^d$ であることから

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

とが得られる。そして、$g(n)$ は最短周期が n であるような長さ n の文字列の数であり、すなわち長さ n の周期性を持たない文字列の数である。上式を用いれば長さが n の周期性を持たない文字列の数を比較的用意に得ることができる。