Chapter 2

Arithmetic Function

當我們要探討一數系時, 考慮定義在它上面的函數通常是一個重要的方法. 在數論中我們當然就是要探討定義在正整數上的函數, 我們稱之為 arithmetic function. 這一章中我們將討論幾個常見的 arithmetic function.

2.1. Multiplicative Arithmetic Functions

並不是所有的 arithmetic function 都很有趣, 到底要探討哪些 arithmetic function 呢? 這完全決定於於要探討的是有關哪些整數的特性. 因為在此我們著重於整數的分解性質, 所以我們探討所謂的 multiplicative arithmetic function.

Definition 2.1.1. 我們稱從 $\mathbb{N}$ 到 $\mathbb{C}$ 的函數為 *arithmetic function.* 若 $f:\mathbb{N}\to\mathbb{C}$ 是一個 arithmetic function 滿足對任意 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$ 皆有 $f(ab)=f(a)f(b)$, 則稱 f 是一個 *multiplicative arithmetic function.*

要注意當一個 arithmetic function f 是 multiplicative 時, $f(ab)=f(a)f(b)$ 並不一定成立. 這是要在 $\gcd(a,b)=1$ 時才可以確定是對的. 如果 f 的性質強到對任意 $a,b\in\mathbb{N}$ 皆有 $f(ab)=f(a)f(b)$, 那麼我們稱 f 是 *completely multiplicative.* 由於 completely multiplicative arithmetic function 的條件較強, 且並無太多這類有趣的函數, 所以這裡我們只專注於 multiplicative arithmetic function.

我們先來看一個 multiplicative arithmetic function 的例子.

Example 2.1.2. 我們考慮 Möbius μ-function, 其定義為

$$\mu(n)=\begin{cases}1, & \text{若 } n=1;\\ 0, & \text{若存在質數 } p \text{ 使得 } p^2\mid n;\\ (-1)^r, & \text{若 } n=p_1\cdots p_r, \text{ 其中 } p_1,\ldots,p_r \text{ 為相異質數.}\end{cases}$$

我們來驗證 μ 確為 multiplicative. 考慮 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$. 今若 $a=1$ 則由 $\mu(a)=\mu(1)=1$ 得 $\mu(ab)=\mu(b)=\mu(a)\mu(b)$. 同理若 $b=1$ 也得 $\mu(ab)=\mu(a)\mu(b)$. 所以我們僅要考慮 $a>1$ 且 $b>1$ 的情形. 由算數基本定理 (Theorem 1.6.1) 我們可以將 a,b 分別寫

成 $a=p_1^{n_1}\cdots p_r^{n_r}$ 以及 $b=q_1^{m_1}\cdots q_t^{m_t}$ 的形式其中 n_i,m_j 皆大於 0 且由於 a,b 互質所有的質數 p_i 和 q_j 皆相異. 今若 n_i 或 m_j 中有一個大於 1, 不失一般性就假設 $n_1\geq 2$, 則由 $p_1^2|a$ 且 $p_1^2|ab$, 知 $\mu(a)=0$ 且 $\mu(ab)=0$, 故得 $\mu(ab)=\mu(a)\mu(b)$. 最後我們只剩下 $n_1=\cdots=n_r=1$ 且 $m_1=\cdots=m_t=1$ 的情況. 此時由於 $ab=p_1\cdots p_r\cdot q_1\cdots q_t$ 且 $p_1,\ldots,p_r,q_1,\ldots,q_t$ 為相異質數得 $\mu(ab)=(-1)^{r+t}$. 然而 $\mu(a)=(-1)^r$ 且 $\mu(b)=(-1)^t$, 故得證 $\mu(ab)=\mu(a)\mu(b)$. 也就是說 μ 是一個 multiplicative arithmetic function.

要注意 μ 並非 completely multiplicative. 我們可以從 $a=b=p$, 其中 p 為質數的情形看出. 此時 $\mu(a)=\mu(b)=-1$ 但是 $\mu(ab)=0$, 故知 $\mu(ab)\neq\mu(a)\mu(b)$. 要知道若要證明一個 arithmetic function f 是 multiplicative 時, 必須考慮所有的情況, 即對所有滿足 $\gcd(a,b)=1$ 的正整數 a,b 皆要符合 $f(ab)=f(a)f(b)$, 而不能僅代個例子驗證. 但若要說 f 不是 multiplicative 時, 只要找到一組 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$ 會使得 $f(ab)\neq f(a)f(b)$ 即可.

接下來我們來看 multiplicative arithmetic function 的基本性質.

Proposition 2.1.3. 假設 f 是一個非 0 的 *multiplicative arithmetic function.* 則 $f(1)=1$, 且若對任意的質數 p 以及 $t\in\mathbb{N}$, 都可知 $f(p^t)$ 的值則對任意 $n\in\mathbb{N}$, $f(n)$ 之值就可以確定.

Proof. 對任意 $n\in\mathbb{N}$，因 f 是 multiplicative 且 $\gcd(n,1)=1$, 可得 $f(n)=f(n)f(1)=0$. 現由假設 f 不是 0 函數，知存在 $n\in\mathbb{N}$ 滿足 $f(n)\neq 0$，故由 $f(n)(1-f(1))=0$ 得證 $f(1)=1$.

現對任意 $n\in\mathbb{N}$, 若 $n=1$, 則由前知 $f(n)=f(1)=1$. 若 $n>1$, 則由算數基本定理知 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 p_i 為相異質數且 $n_i\in\mathbb{N}$. 故由 f 是 multiplicative 且 $\gcd(p_1^{n_1},p_2^{n_2}\cdots p_r^{n_r})=1$ 知 $f(n)=f(p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r})=f(p_1^{n_1})f(p_2^{n_2}\cdots p_r^{n_r})$. 繼續下去使用數學歸納法知 $f(n)=f(p_1^{n_1})\cdots f(p_r^{n_r})$. 因此如果已知這些 $f(p_i^{n_i})$ 之值我們便可確定 $f(n)$ 之值. □

依 Proposition 2.1.3 我們知：如果 f 是 multiplicative arithmetic function, 則掌握所有質數 p 以及 $t\in\mathbb{N}$ 中 $f(p^t)$ 之值，就可以完全了解 f 這一個函數。不過前題是要確認 f 是否為 multiplicative。底下我們提供一個在特殊情形可以確保為 multiplicative 的方法. 這個方法乍看之下或許會覺得奇怪，其實它是有關函數所謂 *convolution* 的一個特殊情況。這個方法，不只可以拿來辨識一個 arithmetic function 是否為 multiplicative，更重要的是可以幫助我們創造許多 multiplicative arithmetic function. Convolution 的概念在數學許多領域都有應用，不過在本課程由於介紹其他基礎概念並不需要，就不多談。

要了解這個方法，首先需要一個補助定理.

Lemma 2.1.4. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$. 若 d 是 ab 的正因數, 則存在唯一的 a 的正因數 d_1 以及 b 的正因數 d_2 使得 $d=d_1d_2$.

Proof. 這又是一個存在及唯一的問題. 存在就是要證存在 $d_1|a$ 且 $d_2|b$ 使得 $d=d_1d_2$, 而唯一就是要證滿足這條件的寫法只有一種. 此存在且唯一性可利用算數基本定理 (Theorem 1.6.1) 直接論證；不過因為在實際情形質因數分解是困難的，這裡提供在實際操作時較可行的證明方式。

首先證明存在性. 給定 $d|ab$, 要如何找到 $d_1|a$ 且 $d_2|b$ 使得 $d=d_1d_2$ 呢? 由於要求 $d_1d_2=d$ 以及 $d_1|a$ 所以 d_1 必須是 a 和 d 的公因數. 思考一下, 我們可考慮取 d_1 為 a,d 的最大公因數, 這樣一來 $d_2=d/d_1$ 會比較小比較可能整除 b. 就讓我們取 $d_1=\gcd(a,d)$ 看看是否可行. 此時令 $d_2=d/d_1$, 我們確實有 $d=d_1d_2$ 且 $d_1|a$. 只剩下要驗證是否 $d_2|b$. 然而 $d|ab$ 故知 $(d/d_1)|(a/d_1)b$. 又由 $d_1=\gcd(a,d)$ 知 $\gcd(a/d_1,d/d_1)=1$ (Corollary 1.2.11), 故由 Proposition 1.2.6(1) 知 $(d/d_1)|b$, 也就是說 $d_2|b$.

接下來證唯一性. 給定 $d|ab$ 假設存在 $d_1,d_1',d_2,d_2'\in\mathbb{N}$ 分別滿足 $d=d_1d_2$, $d_1|a$ 且 $d_2|b$ 以及 $d=d_1'd_2'$, $d_1'|a$ 且 $d_2'|b$, 我們要證明 $d_1=d_1'$ 且 $d_2=d_2'$. 由於 $d_1d_2=d_1'd_2'$, 我們知 $d_1|d_1'd_2'$. 又由於 $d_1|a$, $d_2'|b$ 以及 $\gcd(a,b)=1$, 我們知 $\gcd(d_1,d_2')=1$. 所以再利用 Proposition 1.2.6(1) 得知 $d_1|d_1'$. 同理可證 $d_1'|d_1$ 再加上 $d_1,d_1'\in\mathbb{N}$ 故知 $d_1=d_1'$, 且得 $d_2=d_2'$. □

在 Lemma 2.1.4 有關於存在性的證明中我們發現並未用到 $\gcd(a,b)=1$ 的假設, 也就是說並不需假設 $\gcd(a,b)=1$, 對任意 ab 的正因數都可以找到 $d_1|a$, $d_2|b$ 使得 $d=d_1d_2$. 不過在證明唯一性時, $\gcd(a,b)=1$ 的假設就需要了. 比方說考慮 $a=6$, $b=4$ 和 $d=12$ 的情形, 我們可以取 $d_1=6,d_2=2$ 和 $d_1'=3,d_2'=4$ 都滿足要求, 所以唯一性在此情況並不成立. 由此我們也再次強調唯一性絕不能用因為 a 和 d 的最大公因數是唯一的而說 d_1 是唯一的. 這是因為無從得知為何 d_1 非得是 a,b 的最大公因數不可. 所以在證明唯一性時, 大家還是要按部就班地先假設有兩種寫法再去說明這兩種寫法是一樣, 這樣的方法來處理比較不會出錯.

事實上 Lemma 2.1.4 告訴我們當 $\gcd(a,b)=1$ 時, 若 $d_1,\dots,d_i,\dots,d_r$ 和 $e_1,\dots,e_j,\dots,e_s$ 分別是 a 和 b 所有的相異正因數, 則 $d_1e_1,\dots,d_ie_j,\dots,d_re_s$ 會是 ab 所有的相異正因數. 這是因為這些 d_ie_j 一定是 ab 的正因數, 再加上 Lemma 2.1.4 告訴我們 ab 的正公因數一定可以寫成 d_ie_j 的形式而且這些 d_ie_j 一定相異. 接下來我們就是要用這性質來利用一個已知的 multiplicative arithmetic function 得到新的 multiplicative arithmetic function.

Theorem 2.1.5. 假設 $f:\mathbb{N}\to\mathbb{C}$ 是一個 *multiplicative arithmetic function.* 考慮函數 $F:\mathbb{N}\to\mathbb{C}$ 其定義為對任意 $n\in\mathbb{N}$,

$$F(n)=\sum_{d|n,d>0}f(d),$$

則 F 是一個 *multiplicative arithmetic function.*

Proof. 首先解釋一下 $F(n)=\sum_{d|n,d>0}f(d)$ 這符號表示如果 $d_1,\dots,d_r$ 是 n 的所有相異正因數那麼 $F(n)=f(d_1)+\cdots+f(d_r)$. 我們要證明 F 是 multiplicative 就是要證明當 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$ 時 $F(ab)=F(a)F(b)$.

現假設 $d_1,\dots,d_i,\dots d_r$ 和 $e_1,\dots,e_j,\dots,e_s$ 分別是 a 和 b 所有的正因數. 我們有 $F(a)=f(d_1)+\cdots+f(d_i)+\cdots+f(d_r)$ 以及 $F(b)=f(e_1)+\cdots+f(e_j)+\cdots+f(e_s)$. 因此知 $F(a)F(b)=f(d_1)f(e_1)+\cdots+f(d_i)f(e_j)+\cdots+f(d_r)f(e_s)$. 由於 $\gcd(a,b)=1$ 而 d_i,e_j 分別是 a,b 的因數, 我們知 $\gcd(d_i,e_j)=1$. 再加上 f 是 multiplicative, 故得對所有 d_i,e_j 皆有 $f(d_i)f(e_j)=f(d_ie_j)$. 因此得 $F(a)F(b)=f(d_1e_1)+\cdots+f(d_ie_j)+\cdots+f(d_re_s)$. 然而 Lemma 2.1.4 告訴

我們由於 $\gcd(a,b)=1$, 這些 $d_1e_1,\ldots,d_ie_j,\ldots,d_re_s$ 剛好就是 ab 所有的相異正因數, 故得證 $F(ab)=F(a)F(b)$. □

最後我們來看看 Example 2.1.2 中的 μ 利用 Theorem 2.1.5 所創造出來的 multiplicative arithmetic function 為何.

Example 2.1.6. 令 $\delta:\mathbb{N}\to\mathbb{C}$ 是一個 arithmetic function 其定義為, 對任意 $n\in\mathbb{N}$,

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

其中 μ 是 möbius μ-function. 因為 μ 是 multiplicative, 由 Theorem 2.1.5 知 δ 是 multiplicative. 故要決定 δ 之值由 Proposition 2.1.3 知只要先考慮 $\delta(p^t)$ 之值即可, 其中 p 是質數 $t\in\mathbb{N}$. 然而 p^t 所有的正因數為 $1,p,p^2,\ldots,p^t$, 故由定義知

$$\delta(p^t)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^t)=1-1+0+\cdots+0=0.$$

故若 $n>1$, 則由 $n=p_1^{n_1}\cdots p_r^{n_r}$ 知 $\delta(n)=\delta(p_1^{n_1})\cdots\delta(p_r^{n_r})=0$. 然而由定義 $\delta(1)=\mu(1)=1$, 所以我們可得

$$\delta(n)=\sum_{d|n,d>0}\mu(d)=\begin{cases}1, & \text{當 } n=1;\\ 0, & \text{當 } n>1.\end{cases}$$

Exercise 2.1. 給定整數 a，我們定義一個 arithmetic function ρ 為 $\rho(1)=1$ 且對 $n>1$ 定義 $\rho(n)=a^m$ 其中 m 為 n 的相異質因數個數.

(1) 試證明 ρ 是 multiplicative 且說明 ρ 不是 completely multiplicative 若且唯若 $a\neq 0$ 且 $a\neq 1$.

(2) 令

$$f(n)=\sum_{d|n,d\in\mathbb{N}}\rho(d).$$

若 $n=p_1^{n_1}\cdots p_r^{n_r}$ 為 n 的質因數分解, 試求 $f(n)$.

(3) 若 $a=-1$，試求 $f(270000)$.

Exercise 2.2. 所謂的 Liouville λ-function 是一個 arithmetic function λ 其定義如下: $\lambda(1)=1$ 且對 $n>1$ 若 n 的質因數分解為 $n=p_1^{n_1}\cdots p_r^{n_r}$, 則

$$\lambda(n)=(-1)^{n_1+\cdots+n_r}.$$

(1) 試證明 λ 是 completely multiplicative.

(2) 令

$$F(n)=\sum_{d|n,d\in\mathbb{N}}\lambda(d),$$

試證明如果存在 $a\in\mathbb{N}$ 使得 $n=a^2$, 則 $F(n)=1$; 否則 $F(n)=0$.