# 基礎數論

李華介

國立台灣師範大學數學系

# 前言

本講義主要目的是針對大一學生介紹有關整數論一些基本的代數和算數上的性質, 以作為將來學習抽象代數之準備. 基於這樣的理由, 在此我們將不介紹有關於整數論之歷史和典故以及其應用. 對整數論之應用 (尤其在資訊方面的應用) 有興趣的讀者, 我們推薦 Silverman 的「A Friendly Introduction to Number Theory」(Prentice Hall, Third Edition 2006). 相信若對本講義內容有相當認識之後應可輕鬆閱讀這本書.

*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 $\mu$-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 $\mu$ 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 1.5.1) 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 $\mu$ 是一個 multiplicative arithmetic function.

要注意 $\mu$ 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 $\mu(ab)\neq\mu(a)\mu(b)$. 要知道你要證一個 arithmetic function $f$ 是 multiplicative 時, 你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. 但當你要說 $f$ 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.** 因 $f$ 是 multiplicative 且 $\gcd(1,1)=1$, 故知 $f(1)=f(1)f(1)$ 得知 $f(1)=1$ 或 $f(1)=0$. 若 $f(1)=0$, 則對任意 $n\in\mathbb{N}$, 由於 $\gcd(n,1)=1$, 可得 $f(n)=f(n)f(1)=0$. 也就是說 $f$ 是 0 函數, 此和 $f$ 是非 0 含數之假設矛盾, 故知 $f(1)=1$.

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, 那麼若能掌握所有質數 $p$ 以及 $t\in\mathbb{N}$ 中 $f(p^t)$ 之值那麼就可以完全了解 $f$ 這一個函數. 不過前題是要確認 $f$ 是否為 multiplicative. 底下我們會給一個常用來確認是 multiplicative 的方法. 這個方法不只可以拿來確認 multiplicative arithmetic function 而且可以幫助我們創造許多 multiplicative arithmetic function. 不過首先我們需要一個補助定理.

**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.

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 1.1.8), 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 $d=6$ 的情形, 我們可以取 $d_1=6,d_2=1$ 和 $d_1'=3,d_2'=2$ 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知 $d_1$ 是唯一的而得證唯一性. 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 $d_1e_1,\dots,d_ie_j,\dots,d_re_s$ 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 $\mu$ 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 $\mu$ 是 möbius $\mu$-function. 因為 $\mu$ 是 multiplicative, 由 Theorem 2.1.5 知 $\delta$ 是 multiplicative. 故要決定 $\delta$ 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

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

## 2.2. 正因數個數及正因數和

我們可以用 multiplicative arithmetic function 的概念很快的求出一正整數其正因數之個數及正因數和.

給定一正整數 $n$, 令 $v(n)$ 表示 $n$ 的正因數個數. 既然對任意 $n\in\mathbb{N}$, $v(n)$ 都有取值, 所以我們可以將其看成是一個函數 $v:\mathbb{N}\to\mathbb{N}$. 從函數的角度來看, $v$ 就是一個 arithmetic function. 給定 $n\in\mathbb{N}$ 如何求 $v(n)$ 值呢? 直接的作法就是將 $n$ 的正因數一一列出然後數有多少個. 例如 6 的正因數有 $1,2,3,6$, 所以 $v(6)=4$. 這樣的求法如何用式子表示呢? 我們可以善用 summation $\sum$ 的符號, 將 $v(n)$ 寫成

$$v(n)=\sum_{d|n,d>0}1.$$

上式的意思就是每次你看到 $d$ 滿足 $d|n$ 且 $d>0$ 就加一次, 所以很自然得到 $n$ 的正因數個數.

**Proposition 2.2.1.** 對任意 $n\in\mathbb{N}$, 令 $v(n)$ 表示 $n$ 的正因數個數. 則 $v:\mathbb{N}\to\mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 $p_i$ 為相異質數, 則 $v(n)=(n_1+1)\cdots(n_r+1)$.

**Proof.** 若令 $\mathbf{l}:\mathbb{N}\to\mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n\in\mathbb{N}$, $\mathbf{l}(n)=1$, 則 $v(n)$ 可表為

$$v(n)=\sum_{d|n,d>0}\mathbf{l}(d).$$

由於對任意 $a,b\in\mathbb{N}$, $\mathbf{l}(ab)=\mathbf{l}(a)\mathbf{l}(b)=1$, 我們知 $\mathbf{l}$ 為 (completely) multiplicative. 因此由 Theorem 2.1.5 知 $v$ 為 multiplicative.

既然 $v$ 是 multiplicative, 我們可以利用 Proposition 2.1.3 求對任意 $n\in\mathbb{N}$, $v(n)$ 之值. 也就是說我們要先探討對任意質數 $p$ 以及正整數 $t$, $v(p^t)$ 之值. 由於 $p^t$ 的正因數就是 $p^i$, 其中

$i \in \{0,1,\ldots,t\}$, 我們得到 $v(p^t) = t+1$. 因此對任意 $n \in \mathbb{N}$, 若 $n = 1$, 我們知 $v(n) = v(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 $p_i$ 為相異質數, 則由 $v$ 是 multiplicative 知

$$v(n) = v(p_1^{n_1}) \cdots v(p_r^{n_r}) = (n_1+1) \cdots (n_r+1).$$

□

舉例來說, 我們要求 360 的正因數個數, 由於 $360 = 2^3 \cdot 3^2 \cdot 5$, 利用 Proposition 2.2.1, 我們很快就可得 $v(360) = (3+1)(2+1)(1+1) = 24$. 從這裡大家應更能體會 multiplicative arithmetic function 的好處. 或許求 $v(n)$ 的公式大家在高中時學排列組合時就用乘法原理得到過. 可以用乘法原理的原因其實就和 $v$ 是 multiplicative 息息相關.

接下來我們探討正因數和. 給定一正整數 $n$, 令 $\sigma(n)$ 表示 $n$ 的所有正因數之和. 既然對任意 $n \in \mathbb{N}$, $\sigma(n)$ 都有取值, 所以我們可以將其看成是一個函數 $\sigma : \mathbb{N} \to \mathbb{N}$. 從函數的角度來看, $\sigma$ 就是一個 arithmetic function. 給定 $n \in \mathbb{N}$ 如何求 $\sigma(n)$ 值呢? 直接的作法就是將 $n$ 的正因數一一列出然後全部加起來. 例如 6 的正因數有 $1,2,3,6$, 所以 $\sigma(6) = 1+2+3+6 = 12$. 這樣的求法如何用式子表示呢? 我們再一次善用 summation $\sum$ 的符號, 將 $\sigma(n)$ 寫成

$$\sigma(n) = \sum_{d|n, d>0} d.$$

上式的意思就是每次你看到 $d$ 滿足 $d|n$ 且 $d > 0$ 就加 $d$, 所以很自然得到 $n$ 的正因數和.

**Proposition 2.2.2.** 對任意 $n \in \mathbb{N}$, 令 $\sigma(n)$ 表示 $n$ 的正因數個數. 則 $\sigma : \mathbb{N} \to \mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 $p_i$ 為相異質數, 則

$$\sigma(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_r^{n_r+1}-1}{p_r-1}.$$

**Proof.** 若令 $\mathscr{I} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$, $\mathscr{I}(n) = n$, 則 $\sigma(n)$ 可表為

$$\sigma(n) = \sum_{d|n, d>0} \mathscr{I}(d).$$

由於對任意 $a,b \in \mathbb{N}$, $\mathscr{I}(ab) = ab = \mathscr{I}(a)\mathscr{I}(b)$, 我們知 $\mathscr{I}$ 為 (completely) multiplicative. 因此由 Theorem 2.1.5 知 $\sigma$ 為 multiplicative.

既然 $\sigma$ 是 multiplicative, 我們可以利用 Proposition 2.1.3 求對任意 $n \in \mathbb{N}$, $\sigma(n)$ 之值. 也就是說我們要先探討對任意質數 $p$ 以及正整數 $t$, $\sigma(p^t)$ 之值. 由於 $p^t$ 的正因數就是 $p^i$, 其中 $i \in \{0,1,\ldots,t\}$, 我們得到 $\sigma(p^t) = 1 + p + \cdots + p^t$. 由於 $1, p, \ldots, p^t$ 是一個公比為 $p$ 的等比數列, 我們得

$$\sigma(p^t) = \frac{p^{t+1}-1}{p-1}.$$

因此對任意 $n \in \mathbb{N}$, 若 $n = 1$, 我們知 $\sigma(n) = \sigma(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 $p_i$ 為相異質數, 則由 $\sigma$ 是 multiplicative 知

$$\sigma(n) = \sigma(p_1^{n_1}) \cdots \sigma(p_r^{n_r}) = \frac{p_1^{n_1+1}-1}{p_1-1} \cdots \frac{p_r^{n_r+1}-1}{p_r-1}.$$

□

舉例來說, 我們要求 360 的正因數和, 由於 $360 = 2^3 \cdot 3^2 \cdot 5$, 利用 Proposition 2.2.2, 我們很快就可得

$$\sigma(360) = \frac{2^4-1}{2-1}\frac{3^3-1}{3-1}\frac{5^2-1}{5-1} = 15 \cdot 13 \cdot 6 = 1170.$$

## 2.3. The Euler $\phi$-function

我們要探討比 $n$ 小且與 $n$ 互質的正整數個數.

**Definition 2.3.1.** 給定 $n \in \mathbb{N}$, $\phi(n)$ 表示比 $n$ 小且與 $n$ 互質的正整數個數. 這樣定出的函數 $\phi : \mathbb{N} \to \mathbb{N}$, 稱之為 Euler $\phi$-function.

我們要證明 Euler $\phi$-function 是 multiplicative, 並求其在任意正整數之取值. 由於不容易找到簡單的 multiplicative arithmetic function $f$ 使得 $\phi$ 表示成如 Theorem 2.1.5 的形式, 所以我們要直接證明 $\phi$ 是 multiplicative. 也就是說對任意 $a, b \in \mathbb{N}$ 滿足 $\gcd(a,b) = 1$, 我們要證明 $\phi(ab) = \phi(a)\phi(b)$.

首先我們看一個 $a = 5, b = 4$ 的例子. 我們要說明 $\phi(20) = \phi(5)\phi(4)$. 由於 $\phi(20)$ 表示比 20 小且與 20 互質的正整數個數, 所以我們將小於等於 20 的正整數如下列出:

| | | | |
|---|---|---|---|
| 1 | 6 | 11 | 16 |
| 2 | 7 | 12 | 17 |
| 3 | 8 | 13 | 18 |
| 4 | 9 | 14 | 19 |
| 5 | 10 | 15 | 20 |

很容易看出最後一列 5 10 15 20 中每一個數都是 5 的倍數所以不可能和 20 互質, 因此我們要刪除這一列. 而其餘 4 列每一列中的數除以 5 的餘數都相同且都不等於 0 所以這 4 列的數都和 5 互質. 因此我們只要考慮這 4 列的數哪些和 4 是互質的. 仔細觀察這每一列中的數除以 4 的餘數都相異因此每列中只有餘 1 和餘 3 的兩個數和 4 互質. 總結來說我們發現共有 $\phi(5) = 4$ 列的數和 5 互質, 而這 4 列的數中每列皆有 $\phi(4) = 2$ 個數和 4 互質, 因此 1 到 20 之中共有 $\phi(5)\phi(4) = 8$ 個數和 5 且和 4 互質. 這些數就是 1 到 20 之中和 20 互質的數, 所以知 $\phi(20) = \phi(5)\phi(4)$.

接下來我們就是要用前面的方法證明一般的情形. 要注意前面的方法我們並無真正點出哪些數和 20 互質, 因為我們只想知道個數. 再加上我們的方法幾乎和 $a = 5, b = 4$ 無關所以比實際找出哪些數和 20 互質更能運用在一般的狀況. 首先我們用到和 20 互質的數就是和 5 且和 4 互質的數, 這個性質在一般的情況都對.

**Lemma 2.3.2.** 假設 $a, b, c \in \mathbb{Z}$. 則 $\gcd(ab, c) = 1$ 若且唯若 $\gcd(a,c) = 1$ 且 $\gcd(b,c) = 1$.

**Proof.** 假設 $\gcd(ab,c) = 1$. 若 $d = \gcd(a,c)$, 表示 $d$ 是 $a, c$ 的公因數, 所以 $d$ 也是 $ab$ 和 $c$ 的公因數, 故得 $d = 1$. 同理知 $\gcd(b,c) = 1$.

反之, 假設 $\gcd(a,c) = 1$ 且 $\gcd(b,c) = 1$. 若 $\gcd(ab,c) \neq 1$, 表示存在一質數 $p$ 滿足 $p \mid \gcd(ab,c)$. 也就是說 $p \mid ab$ 且 $p \mid c$. 但 $p$ 是質數, 故由 Lemma 1.4.2 知 $p \mid a$ 或 $p \mid b$. 得知 $p$ 是 $a, c$ 或 $b, c$ 的公因數. 此和 $\gcd(a,c) = 1$ 且 $\gcd(b,c) = 1$ 相矛盾, 故知 $\gcd(ab,c) = 1$. □

在前面求與 20 互質的數中, 另一個重要步驟是任一排中每一個數除以 4 的餘數都相異, 這在一般 $\gcd(a,b)=1$ 的情況都是對的.

**Lemma 2.3.3.** 假設 $a,b,l\in\mathbb{Z}$, $b>1$ 且 $\gcd(a,b)=1$. 則在 $l,l+a,l+2a,\ldots,l+(b-1)a$, 中每一個數除以 $b$ 的餘數皆相異. 而且其中共有 $\phi(b)$ 個元素和 $b$ 互質.

**Proof.** 若 $u,v\in\mathbb{Z}$ 且 $u,v$ 除以 $b$ 的餘數相同, 表示 $b|u-v$. 因此要說 $l,l+a,\ldots,l+(b-1)a$ 中的元素除以 $b$ 的餘數皆相異, 就是說任取 $l+ia,l+ja$, 其中 $0\le i<j\le b-1$, 都無法使得 $b$ 整除 $(l+ja)-(l+ia)$. 今假設 $b|(l+ja)-(l+ia)$, 也就是說 $b|(j-i)a$. 由於 $\gcd(a,b)=1$, Proposition 1.2.6(1) 告訴我們 $b|j-i$. 但此與 $0\le i<j\le b-1$ 相矛盾, 故由反證法知 $b$ 不整除 $(l+ja)-(l+ia)$. 也就是說任取 $l+ia,l+ja$, 其中 $0\le i<j\le b-1$, 則它們除以 $b$ 之餘數皆相異.

對於 $i\in\{0,1,\ldots,b-1\}$ 若令 $r_i$ 表示 $l+ia$ 除以 $b$ 的餘數, 由於 $0\le r_i\le b-1$ 且這 $b$ 個 $r_i$ 皆相異, 我們知 $\{r_0,r_1,\ldots,r_{b-1}\}$ 這一個集合和 $\{0,1,\ldots,b-1\}$ 是相同的. 然而 Lemma 1.3.1 告訴我們 $\gcd(l+ia,b)=\gcd(r_i,b)$, 所以 $\{l,l+a,\ldots,l+(b-1)a\}$ 中和 $b$ 互質的數和 $\{0,1,\ldots,b-1\}$ 中和 $b$ 互質的數之個數相同. 依定義知 $\{0,1,\ldots,b-1\}$ 中共有 $\phi(b)$ 個數與 $b$ 互質, 故得證. □

接下來我們證明 $\phi$ 是一個 multiplicative arithmetic function.

**Proposition 2.3.4.** 若 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$, 則 $\phi(ab)=\phi(a)\phi(b)$.

**Proof.** 我們將小於 $ab$ 的正整數依下列方法排成 $b$ 列:

$$\begin{array}{cccc} 1 & 1+a & \cdots & 1+(b-1)a \\ 2 & 2+a & \cdots & 2+(b-1)a \\ \vdots & \vdots & \ddots & \vdots \\ a & 2a & \cdots & ba \end{array}$$

其中第 $l$ 列為 $l,l+a,\ldots,l+(b-1)a$. 由 Lemma 1.3.1 知這裡每一數和 $a$ 的最大公因數皆與 $l$ 和 $a$ 的最大公因數相同. 換言之, 若 $l$ 和 $a$ 互質則第 $l$ 列中每一數皆和 $a$ 互質; 而若 $l$ 和 $a$ 不互質則第 $l$ 列中每一數皆和 $a$ 不互質. 又因為 $1\le l\le a$, 故依定義共有 $\phi(a)$ 個 $l$ 會與 $a$ 互質. 而我們就僅考慮這 $\phi(a)$ 列的數 (其餘的數都和 $a$ 不互質故和 $ab$ 不互質).

這 $\phi(a)$ 列的數雖都和 $a$ 互質但並不都和 $b$ 互質. 然而每一列皆為 $l,l+a,\ldots,l+(b-1)a$ 的形式, 故由 $\gcd(a,b)=1$ 以及 Lemma 2.3.3 知每一列皆有 $\phi(b)$ 個數和 $b$ 互質. 故 1 到 $ab$ 中總共有 $\phi(a)\phi(b)$ 個元素和 $a$ 且和 $b$ 互質. 由 Lemma 2.3.2 這些數就是和 $ab$ 互質的數. 故得證 $\phi(ab)=\phi(a)\phi(b)$. □

既然 $\phi$ 是 multiplicative, 我們就可以利用 Proposition 2.1.3 算出 $\phi$ 之值.

**Proposition 2.3.5.** 若 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中 $p_i$ 為相異質數, 則

$$\phi(n)=(p_1^{n_1}-p_1^{n_1-1})\cdots(p_r^{n_r}-p_r^{n_r-1})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r}).$$

**Proof.** 我們先求對任意質數 $p$ 以及正整數 $t$, $\phi(p^t)$ 之值. 由於 $p$ 是 $p^t$ 唯一的質因數, $u$ 和 $p^t$ 不互質表示 $p$ 必為 $u$ 之因數. 因此要計算小於 $p^t$ 的正整數中有多少與 $p^t$ 互質, 只要算出這些數中有哪些是 $p$ 的倍數再扣掉即可. 然而 1 到 $p^t$ 中共有 $p^t/p$ 個數是 $p$ 的倍數. 故得知 1 到 $p^n$ 中共有 $p^t - p^{t-1}$ 個整數和 $p^t$ 互質.

現考慮任意 $n \in \mathbb{N}$. 若 $n = 1$, 我們知 $\phi(n) = \phi(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 $p_i$ 為相異質數, 則由 $\phi$ 是 multiplicative 知

$$\phi(n) = \phi(p_1^{n_1}) \cdots \phi(p_r^{n_r}) = (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_r^{n_r} - p_r^{n_r-1}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

□

既然 $\phi$ 是 multiplicative, 我們可以利用 Theorem 2.1.5 造出另一個 multiplicative arithmetic function. 考慮 $F : \mathbb{N} \to \mathbb{N}$ 其定義為對任意 $n \in \mathbb{N}$, $F(n) = \sum_{d|n, d>0} \phi(d)$. 由於 $F$ 是 multiplicative, 且對任意質數 $p$ 以及 $t \in \mathbb{N}$, 我們有

$$F(p^t) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^t) = 1 + (p-1) + (p^2 - p) + \cdots + (p^t - p^{t-1}) = p^t.$$

因此我們有以下之結果.

**Corollary 2.3.6** (Gauss)**.** 若 $n \in \mathbb{N}$ 則

$$\sum_{d|n, d>0} \phi(d) = n.$$

**Proof.** 令 $F(n) = \sum_{d|n,d>0} \phi(d)$, 由前知 $F$ 不是 0 函數故由 $F$ 是 multiplicative, 利用 proposition 2.1.3 知 $F(1) = 1$. 若 $n \in \mathbb{N}$ 且 $n > 1$ 時, 將 $n$ 寫成 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 $p_i$ 為相異質數, 再由上面 $F(p^t) = p^t$ 的結果及 Proposition 2.1.3 知

$$F(n) = F(p_1^{n_1}) \cdots F(p_r^{n_r}) = p_1^{n_1} \cdots p_r^{n_r} = n,$$

得證本定理. □

## 2.4. Convolution

我們可以利用 convolution 定義出新的 multiplicative arithmetic function, 另外 convolution 也提供了一個較簡明的方法來證明下一節要探討的 Möbius inversion formula. 雖然本節及下一節的內容在本講義中以後不會用到, 但希望利用此介紹讓大家知道有時適當定義一些運算對解決問題有很大的幫助.

**Definition 2.4.1.** 給定兩 arithmetic functions $f, g$ 我們記其 *convolution* 為 $f * g$, 其定義為對任意 $n \in \mathbb{N}$,

$$f * g(n) = \sum_{d|n, d>0} f(d)g(n/d).$$

依照 convolution 的定義, 要求 $f * g(n)$ 之值, 首先找出 $n$ 的所有正因數, 然後對於每一個 $n$ 的正因數 $d$, 我們求 $f(d)g(n/d)$ 之值, 再將這些值加起來. 若 $d$ 是 $n$ 的正因數, 令

$e=n/d$, 我們自然有 $de=n$. 反之, 若 $d,e$ 是正整數滿足 $de=n$, 則我們自然有 $d|n$. 因此我們也可以用如下的表示法表示 $f*g$. 即,

$$f*g(n)=\sum_{\substack{de=n\\ d,e\in\mathbb{N}}} f(d)g(e).$$

這樣的表示法雖然看來像兩個變數, 但實質上若給定 $d$, 則 $e$ 自然確定. 我們選用這個表示法是因為底下要推導 convolution 的性質時用這種表法較簡明.

由於 $f$ 和 $g$ 是 arithmetic function, 所以 $f*g$ 在任意正整數皆有取值, 因此 $f*g$ 仍為 arithmetic function. 換言之 convolution 可以看成是一個 arithmetic function 之間的運算 (你可以將它看成是兩個 arithmetic function 之間的乘法). 接下來我們就是要探討這種運算的基本性質.

**Proposition 2.4.2.** 設 $f,g,h$ 皆為 *arithmetic function.* 令 $\delta:\mathbb{N}\to\mathbb{N}$ 定義為

$$\delta(n)=\begin{cases}1, & n=1;\\ 0, & n>1.\end{cases}$$

關於 *convolution* 我們有以下之性質.

(1) $f*\delta=\delta*f=f$.

(2) $f*g=g*f$.

(3) $(f*g)*h=f*(g*h)$.

**Proof.** (1) 依定義對任意 $n\in\mathbb{N}$, $f*\delta(n)=\sum_{d|n,d>0}f(d)\delta(n/d)$. 由於當 $n/d>1$ 時 $\delta(n/d)=0$. 因此在 $\sum$ 內, 只有 $d=n$ 這一項留下, 故得 $f*\delta(n)=f(n)\delta(1)=f(n)$. 換言之, $f$ 和 $f*\delta$ 在任意 $n\in\mathbb{N}$ 的取值皆相同. 故從函數的觀點來看, 它們是相同的函數. 同理可證 $\delta*f=f$.

(2) 由於對任意 $n\in\mathbb{N}$,

$$f*g(n)=\sum_{\substack{de=n\\ d,e\in\mathbb{N}}} f(d)g(e)=\sum_{\substack{de=n\\ d,e\in\mathbb{N}}} g(e)f(d)=\sum_{\substack{de=n\\ d,e\in\mathbb{N}}} g(d)f(e)=g*f(n).$$

我們得證 $f*g=g*f$.

(3) 依定義, 對任意 $n\in\mathbb{N}$,

$$\begin{aligned}(f*g)*h(n) &= \sum_{\substack{de=n\\ d,e\in\mathbb{N}}}(f*g)(d)h(e)\\ &= \sum_{\substack{de=n\\ d,e\in\mathbb{N}}}\Big(\sum_{\substack{rs=d\\ r,s\in\mathbb{N}}} f(r)g(s)\Big)h(e)\\ &= \sum_{\substack{rse=n\\ r,s,e\in\mathbb{N}}} f(r)g(s)h(e).\end{aligned}$$

同理我們有

$$f*(g*h)(n)=\sum_{\substack{duv=n\\ d,u,v\in\mathbb{N}}} f(d)g(u)h(v).$$

因此得證 $(f*g)*h=f*(g*h)$. □

Proposition 2.4.2 告訴我們, 若將 $*$ 看成是 arithmetic function 之間的運算, 則 $\delta$ 這一個 arithmetic function 就如同乘法運算的 1 (這樣的元素, 我們稱之為 identity). 而且 $*$ 這個運算滿足交換率以及結合率. $*$ 這個運算其實對於 multiplicative arithmetic function 也具有封閉性. 也就是說我們有以下之性質.

**Theorem 2.4.3.** 假設 $f,g$ 皆為 *multiplicative arithmetic function,* 則 $f*g$ 也是 *multiplicative arithmetic function.*

**Proof.** 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$, 我們要證明 $f*g(ab)=(f*g(a))(f*g(b))$. 對任意 $d,e\in\mathbb{N}$ 滿足 $de=ab$, 我們皆有 $d|ab$ 且 $e|ab$. 依 Lemma 2.1.4 知分別存在唯一的一組 $d_1,d_2$ 以及 $e_1,e_2$ 滿足 $d=d_1d_2$ 及 $e=e_1e_2$ 其中 $d_1,e_1$ 為 $a$ 的正因數且 $d_2,e_2$ 為 $b$ 的正因數. 又因 $\gcd(a,b)=1$, 故 $\gcd(d_1,d_2)=1$ 且 $\gcd(e_1,e_2)=1$. 所以由 $f,g$ 是 multiplicative 以及定義知

$$f*g(ab)=\sum_{\substack{de=ab\\ d,e\in\mathbb{N}}}f(d)g(e)=\sum_{\substack{d_1d_2e_1e_2=ab\\ d_1|a,d_2|b,e_1|a,e_2|b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}}f(d_1)f(d_2)g(e_1)g(e_2).$$

現對任意 $d_1,d_2,e_1,e_2\in\mathbb{N}$ 滿足 $d_1d_2e_1e_2=ab$ 且 $d_1,e_1$ 和 $d_2,e_2$ 分別是 $a$ 和 $b$ 的因數. 因為 $d_1e_1|ab$, 又因 $\gcd(a,b)=1$ 且 $d_1,e_1$ 是 $a$ 的因數, 知 $\gcd(d_1e_1,b)=1$. 因此由 Proposition 1.2.6(1) 知 $d_1e_1|a$. 另一方面 $a|d_1e_1d_2e_2$, 再由 $\gcd(a,b)=1$ 以及 $d_2,e_2$ 為 $b$ 之因數, 得 $\gcd(a,d_2e_2)=1$. 因此知 $a|d_1e_1$. 所以得證 $a=d_1e_1$, 同理得證 $b=d_2e_2$. 反之, 若 $d_1,d_2,e_1,e_2\in\mathbb{N}$ 滿足 $a=d_1e_1$ 且 $b=d_2e_2$, 則我們有 $d_1d_2e_1e_2=ab$ 且 $d_1,e_1$ 和 $d_2,e_2$ 分別是 $a$ 和 $b$ 的因數. 因此我們有

$$\sum_{\substack{d_1d_2e_1e_2=ab\\ d_1|a,d_2|b,e_1|a,e_2|b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}}f(d_1)f(d_2)g(e_1)g(e_2)=\sum_{\substack{d_1e_1=a,d_2e_2=b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}}f(d_1)f(d_2)g(e_1)g(e_2).$$

另一方面

$$(f*g(a))(f*g(b))=\sum_{\substack{d_1e_1=a\\ d_1,e_1\in\mathbb{N}}}f(d_1)g(e_1)\sum_{\substack{d_2e_2=b\\ d_2,e_2\in\mathbb{N}}}f(d_2)g(e_2).$$

利用分配率知

$$\sum_{\substack{d_1e_1=a\\ d_1,e_1\in\mathbb{N}}}f(d_1)g(e_1)\sum_{\substack{d_2e_2=b\\ d_2,e_2\in\mathbb{N}}}f(d_2)g(e_2)=\sum_{\substack{d_1e_1=a,d_2e_2=b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}}f(d_1)f(d_2)g(e_1)g(e_2).$$

因此得證本定理. □

若令 $\mathbf{1}:\mathbb{N}\to\mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n\in\mathbb{N}$, $\mathbf{1}(n)=1$, 則對任意的 arithmetic function $f$, 皆有當 $n\in\mathbb{N}$ 時,

$$f*\mathbf{1}(n)=\sum_{\substack{de=n\\ d,e\in\mathbb{N}}}f(d)\mathbf{1}(e)=\sum_{d|n,d>0}f(d).$$

因為 $\mathbf{1}$ 是一個 multiplicative arithmetic function, 從這個角度看 Theorem 2.1.5 只是 Theorem 2.4.3 的一個特殊情況.

**Example 2.4.4.** 我們可以利用 Theorem 2.4.3 來求對任意 $n \in \mathbb{N}$,

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

之值, 其中 $\mu$ 為 Möbius $\mu$-function (參見 Example 2.1.2).

令 $\mathscr{I} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$, $\mathscr{I}(n) = n$. 考慮 $F : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$,

$$F(n) = \sum_{d|n,d>0} \mu(d)\frac{n}{d} = \sum_{d|n,d>0} \mu(d)\mathscr{I}(\frac{n}{d}).$$

依定義我們知 $F = \mu * \mathscr{I}$. 然而 $\mu$ 和 $\mathscr{I}$ 皆為 multiplicative, 故利用 Theorem 2.4.3 知 $F$ 也是 multiplicative. 因此我們只要檢視對任意質數 $p$ 以及 $t \in \mathbb{N}$, $F(p^t)$ 之值為何. 依定義 $\mu(1) = 1$, $\mu(p) = -1$ 且當 $i > 1$ 時 $\mu(p^i) = 0$, 故得

$$F(p^t) = \mu(1)\mathscr{I}(p^t) + \mu(p)\mathscr{I}(p^{t-1}) = p^t - p^{t-1}.$$

注意此和 $\phi(p^t)$ 的值相同 (參見 Proposition 2.3.5), 故利用 $F$ 和 $\phi$ 皆為 multiplicative 以及 Proposition 2.1.3 知 $F = \phi$. 也就是說對任意 $n \in \mathbb{N}$ 皆有

$$\sum_{d|n,d>0} \mu(d)\frac{n}{d} = \phi(n).$$

## 2.5. The Möbius Inversion Formula

前面在介紹 Euler's $\phi$-function 時, 我們曾提及不容易找到 arithmetic function $f$ 將 $\phi$-function 表成 $\phi(n) = \sum_{d|n,d>0} f(d)$ 這樣的形式. 事實上 Möbius inversion formula 可以幫助我們找到這樣的 $f$.

**Theorem 2.5.1** (Möbius Inversion Formula)**.** 假設 $F, f$ 皆為 *arithmetic function,* $\mu$ 為 *möbius* $\mu$*-function.* 則對任意 $n \in \mathbb{N}$, $F, f$ 滿足

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

若且唯若對任意 $n \in \mathbb{N}$, $F, f$ 滿足

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

**Proof.** 令 $\mathbf{1} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$, $\mathbf{1}(n) = 1$. 依 convolution 的定義我們要證明 $F = f * \mathbf{1}$ 若且唯若 $f = F * \mu$.

若 $F = f * \mathbf{1}$, 則 $F * \mu = (f * \mathbf{1}) * \mu$. 利用 Proposition 2.4.2(3) 知 $F * \mu = f * (\mathbf{1} * \mu)$. 然而對任意 $n \in \mathbb{N}$, $\mathbf{1} * \mu(n) = \mu * \mathbf{1}(n) = \sum_{d|n,d>0} \mu(d)$, 由 Example 2.1.6 知 $\mathbf{1} * \mu = \mu * \mathbf{1} = \delta$, 其中 $\delta : \mathbb{N} \to \mathbb{N}$ 定義為

$$\delta(n) = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$$

換言之, 我們有 $F * \mu = f * (\mathbf{1} * \mu) = f * \delta$. 因而利用 Proposition 2.4.2(1) 得證 $F * \mu = f$.

反之, 若 $f = F*\mu$, 則 $f*\mathbf{1} = (F*\mu)*\mathbf{1} = F*(\mu*\mathbf{1})$. 故再利用 $\mu*\mathbf{1} = \delta$ 得知 $f*\mathbf{1} = F*\delta = F$. □

注意 Möbius inversion formula 需要對任意 $n \in \mathbb{N}$ 對才能使用. 也就是說你不能看到

$$F(6) = f(1)+f(2)+f(3)+f(6)$$

就下結論說

$$f(6) = F(1)\mu(6)+F(2)\mu(3)+F(3)\mu(2)+F(6)\mu(1) = F(1)-F(2)-F(3)+F(6).$$

需要檢驗所有 $n \in \mathbb{N}$ 都對才可下此結論 (至少在此例中還要多檢查 $F(1) = f(1)$ , $F(2) = f(1)+f(2)$ 以及 $F(3) = f(1)+f(3)$).

**Example 2.5.2.** 現在我們來看看如何利用 Möbius inversion formula, 找到 $f$ 使得 $\phi(n) = \sum_{d|n,d>0} f(d)$. 由 Möbius inversion formula 知此時 $f = \mu*\phi$. 由於 $\mu$ 和 $\phi$ 皆為 multiplicative, 由 Theorem 2.4.3 知 $f$ 亦為 multiplicative. 因此我們先觀察對任意質數 $p$ 以及 $t \in \mathbb{N}$, $f(p^t)$ 之值. 然而

$$f(p^t) = \sum_{d|p^t,d>0} \mu(d)\phi(\frac{p^t}{d}) = \mu(1)\phi(p^t)+\mu(p)\phi(p^{t-1}) = \phi(p^t)-\phi(p^{t-1}).$$

因此知 $f(p) = p-1-1 = p-2$ 且當 $t \geq 2$ 時 $f(p^t) = p^t-p^{t-1}-(p^{t-1}-p^{t-2}) = p^{t-2}(p-1)^2$. 因此若 $n = p_1^{n_1}\cdots p_r^{n_r}$, 其中 $p_i$ 為相異質數, 可以得 $f(n) = f(p_1^{n_1})\cdots f(p_r^{n_r})$. 但是接下來很難將 $f$ 寫成很好的形式 (注意要區分有某個 $n_i = 1$ 的情形). 事實上若沒有 Möbius inversion formula, 我們也很難證出這個 $f$ 確實滿足 $\mu(n) = \sum_{d|n,d>0} f(d)$. 所以當初在證明 $\phi$ 是 multiplicative 時, 我們並沒有利用 Theorem 2.1.5 證得.

事實上利用 Example 2.5.2 的方法我們可以證出任何的 arithmetic function $F$ 皆可找到唯一的 arithmetic function $f$ 使得對任意 $n \in \mathbb{N}$, 皆有 $F(n) = \sum_{d|n,d>0} f(d)$. 當我們找到的 $f$ 是 multiplicative 時, Theorem 2.1.5 告訴我們 $F$ 也是 multiplicative. 反之, 以下 Corollary 告訴我們若已知 $F$ 是 multiplicative, 則找出的 $f$ 一定也是 multiplicative.

**Corollary 2.5.3.** 假設 $F, f$ 皆為 *arithmetic function.* 若對任意 $n \in \mathbb{N}$, 皆有

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

且已知 $F$ 是一個 *multiplicative arithmetic function,* 則 $f$ 亦為一個 *multiplicative arithmetic function.*

**Proof.** 由 Theorem 2.5.1 知 $f = \mu*F$, 故由 $\mu$ 是 multiplicative 以及 $F$ 是 multiplicative 的假設, 利用 Theorem 2.4.3 知 $f = \mu*F$ 亦為 multiplicative. □

**Example 2.5.4.** 前面幾節中我們曾利用 multiplicative arithmetic function 得到一些有趣的等式, 接下來的例子我們將利用 Möbius inversion formula 得到更多等式.

(1) 令 $v(n)$ 表示 $n$ 的正因數個數. 已知對任意 $n \in \mathbb{N}$, 皆有

$$v(n) = \sum_{d|n, d>0} 1 = \sum_{d|n, d>0} \mathbf{I}(d),$$

其中對所有 $n \in \mathbb{N}$, $\mathbf{I}(n) = 1$. 故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$,

$$1 = \mathbf{I}(n) = \sum_{d|n, d>0} \mu(d) v(\frac{n}{d}) = \sum_{d|n, d>0} v(d) \mu(\frac{n}{d}).$$

(2) 令 $\sigma(n)$ 表示 $n$ 的所有正因數之和. 已知對任意 $n \in \mathbb{N}$ 皆有

$$\sigma(n) = \sum_{d|n, d>0} d = \sum_{d|n, d>0} \mathscr{I}(d),$$

其中對所有 $n \in \mathbb{N}$, $\mathscr{I}(n) = n$. 故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$,

$$n = \mathscr{I}(n) = \sum_{d|n, d>0} \mu(d) \sigma(\frac{n}{d}) = \sum_{d|n, d>0} \sigma(d) \mu(\frac{n}{d}).$$

(3) 由 Corollary 2.3.6 知對任意 $n \in \mathbb{N}$ 皆有

$$n = \mathscr{I}(n) = \sum_{d|n, d>0} \phi(d).$$

故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$, 皆有

$$\phi(n) = \sum_{d|n, d>0} \mu(d) \mathscr{I}(\frac{n}{d}) = \sum_{d|n, d>0} \mu(d) \frac{n}{d}.$$

Example 2.5.4(3) 的等式在前一節 Example 2.4.4 中我們曾用 multiplicative 的性質得到. 事實上 Example 2.5.4 中的等式都可以用 multiplicative 的性質得到. 不過要注意的是 Möbius inversion formula 並不侷限於 multiplicative 的情形, 它對一般的 arithmetic function 皆適用.