就是因為質數這麼不容易出現, 再加上很難判別一個很大的數是否為質數, 所以質數常被應用在密碼學中. 底下我們介紹一種最簡單判斷質數的方法.

Proposition 1.5.8. 假設 $n>1$ 是一整數. 則 n 不是質數若且唯若存在質數 p 小於等於 $\sqrt{n}$ 且整除 n.

Proof. 首先若存在 $p\le\sqrt{n}$ 且 $p\mid n$. 因 $1<p<n$, 得 n 除了 1 和 n 以外還有其他的正因數, 故知 n 不是 prime. 另一方面, 假設 n 不是質數, 依定義知存在 $a,b\in\mathbb{Z}$ 滿足 $1<a\le b<n$ 且 $n=ab$. 由此我們可以確定 $a\le\sqrt{n}$, 否則若 $a>\sqrt{n}$ 會造成 $ab>(\sqrt{n})^2=n$ 而與 $n=ab$ 不合. 而由 Lemma 1.5.4 知存在質數 p 使得 $p\mid a$. 既然 $p\mid a$ 我們得 $p\le a\le\sqrt{n}$ 且 $p\mid n$. □

Proposition 1.5.8 告訴我們的是一個判別 composite number 的等價關係, 所以它也就告訴了我們判別 prime 的方法. 也就是說 n 是質數若且唯若所有小於等於 $\sqrt{n}$ 的質數都不能整除 n. 這種判別質數方法稱為篩法 (sieve method). 它可以幫助我們篩得哪些數是質數. 例如若要找出所有小於 100 的質數. 我們只要將小於 $\sqrt{100}=10$ 的質數 (即 2,3,5,7) 找出, 留下 2,3,5,7 然後將其餘 2,3,5,7 的倍數刪除, 經過這樣篩選後留下來小於 100 的數就都是小於 100 的質數. 這是因為若 $n<100$ 且不是質數, 則由 Proposition 1.5.8 知 n 必有一質因數小於等於 $\sqrt{n}<\sqrt{100}=10$. 因此被我們所刪除 2,3,5,7 的倍數就是所有小於 100 的合成數, 自然剩下的便都是質數了.

Question 1.8. 大於 100 的合成數中, 第一個不能用刪除 2,3,5,7 的倍數篩選出來的是哪一個整數?

1.6. 算術基本定理

算術基本定理 (The fundamental theorem of arithmetic) 即唯一分解定理, 告訴我們每一個大於 1 的整數若不是質數都可以寫成有限多個質因數的乘積且經過適當排序其寫法唯一. 此定理看似自然且明顯, 但仍需一個正式的證明.

這裡我們又碰到一個典型的有關存在性與唯一性的問題. 這裡的存在性指的就是對一大於 1 的整數可以找到有限多個質數使其可以寫成這些質數的乘積, 而唯一性就是指的就是寫法唯一. 由於正整數和負整數的分解只差一個負號, 我們只需考慮正整數的情況.

Theorem 1.6.1 (The Fundamental Theorem of Arithmetic)**.** 假設 $a\in\mathbb{N}$ 且 $a>1$, 則存在 $p_1,\dots,p_r$, 其中 p_i 是相異的質數, 滿足

$$a=p_1^{n_1}\cdots p_r^{n_r},\quad n_i\in\mathbb{N},\forall i\in\{1,\dots,r\}.$$

如果 a 可以分解成另外的形式 $a=q_1^{m_1}\cdots q_s^{m_s}$, 其中 q_i 是相異的質數, 則 $r=s$ 且經過變換順序可得 $p_i=q_i$, $n_i=m_i$, $\forall i\in\{1,\dots,r\}$.

Proof. 我們分開來證存在性與唯一性.

首先來看存在性: 簡單來說存在性就是要證明每一個大於 1 的整數都可以寫成有限多個 (可以相同) 質數的乘積. 我們用數學歸納法來證明. 當 $a=2$ 時由於 2 是質數, 所以在這情

況存在性是對的. 接著假設對所有從 2 到 $a-1$ 的整數存在性是對的. 如果 a 是質數, 那存在性自然成立. 如果 a 不是質數, 則知 $a=a_1\cdot b_1$ 其中 $a_1,b_1\in\mathbb{N}$ 且 $1<a_1<a$ 及 $1<b_1<a$. 故利用歸納假設知 a_1 和 b_1 都可寫成有限多個質數的乘積, 所以得證 $a=a_1\cdot b_1$ 也可以寫成有限多個質數的乘積.

要證明唯一性, 我們假設

$$a=p_1^{n_1}\cdots p_r^{n_r}=q_1^{m_1}\cdots q_s^{m_s},$$

其中 $p_1,\ldots,p_r$ 是兩兩相異的質數, 且 $q_1,\ldots,q_s$ 也是兩兩相異的質數. 首先我們證明 $P=\{p_1,\ldots,p_r\}$ 和 $Q=\{q_1,\ldots,q_s\}$ 這兩個集合是一樣的. 任取 $p_i\in P$, 由於 $p_i\mid a$, 而 $a=q_1^{m_1}\cdots q_s^{m_s}$, 故由 p_i 是質數以及 Corollary 1.5.3 知存在 $q_j\in Q$ 使得 $p_i\mid q_j$. 再由 q_j 亦為質數, 得 $p_i=q_j\in Q$. 我們證明了 $P\subseteq Q$. 同理可證 $Q\subseteq P$. 因此得 $P=Q$, 亦即 $r=s$, 且經由適當排列, 我們有 $p_1=q_1,p_2=q_2,\ldots,p_r=q_r$. 換言之現在我們有

$$a=p_1^{n_1}\cdots p_r^{n_r}=p_1^{m_1}\cdots p_r^{m_r}. \tag{1.1}$$

接下來我們要說明, 對所有 $i\in\{1,\ldots,r\}$ 皆有 $n_i=m_i$, 因而證得唯一性. 我們可以用反證法, 也就是說假設存在 $n_i\neq m_i$, 會造成矛盾. 不失一般性, 我們假設 $n_1\neq m_1$, 我們更進一步假設 $n_1>m_1$. 此時將式子 (1.1) 同除以 $p_1^{m_1}$, 我們得

$$p_1^{n_1-m_1}p_2^{n_2}\cdots p_r^{n_r}=p_2^{m_2}\cdots p_r^{m_r}.$$

由於 p_1 是質數, 且 $n_1-m_1>0$, 故由 $p_1\mid p_2^{m_2}\cdots p_r^{m_r}$ 以及 Corollary 1.5.3 知 $p_2,\ldots,p_r$ 中必存在某個 p_j 滿足 $p_1\mid p_j$, 此和當初假設 $p_1,p_2,\ldots,p_r$ 為相異質數相矛盾. 故得證唯一性. □

一般來說我們將一正整數 a 寫成質數之乘積 $a=p_1^{n_1}\cdots p_r^{n_r}$ 時, 為了唯一性我們要求每個質數 p_i 的次方 n_i 都是正的, 也就是說我們只挑出 a 的質因數 $p_1,\ldots,p_r$. 不過當要討論兩正數 a,b 時為了方便比較, 我們通常會挑出 a 和 b 所有的質因數再將 a,b 寫成這些質數之乘積的樣子. 也就是說可寫成 $a=p_1^{n_1}\cdots p_r^{n_r}$ 以及 $b=p_1^{m_1}\cdots p_r^{m_r}$ 其中對於 $i\in\{1,\ldots,r\}$, $n_i\geq 0$ 且 $m_i\geq 0$. 注意這裡由於 a 的質因數未必就是 b 的質因數, 反之亦然, 所以 n_i,m_i 有可能為 0. 這樣寫法的方便性就是我們不必區分哪些 p_i 是 a 的質因數, 哪些是 b 的質因數. 利用這樣的寫法我們很容易將 a,b 的最大公因數表示出來.

Proposition 1.6.2. 假設 $a,b\in\mathbb{N}$ 且 $a,b>1$. 若 $a=p_1^{n_1}\cdots p_r^{n_r}$ 且 $b=p_1^{m_1}\cdots p_r^{m_r}$, 其中 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i\geq 0$, 則 a,b 的正公因數都可寫成 $p_1^{t_1}\cdots p_r^{t_r}$ 的形式, 其中 $0\leq t_i\leq\min\{n_i,m_i\}$. 特別地, 我們有

$$\gcd(a,b)=p_1^{\min\{n_1,m_1\}}\cdots p_r^{\min\{n_r,m_r\}}.$$

Proof. 首先回顧一下 $\min\{x,y\}$ 表示 x,y 中最小之數. 現假設 d 是 a,b 的正公因數, 則由 $d\mid a$ 我們知若 p 是 d 的質因數, 則由 $p\mid d$ 知 $p\mid a$. 故由 Corollary 1.5.3 知存在 $i\in\{1,\ldots,r\}$ 使得 $p\mid p_i$. 因此由 p,p_i 皆為質數得 $p=p_i$. 也就是說 d 的質因數必在 $\{p_1,\ldots,p_r\}$ 中, 故 d 一定可以寫成 $p_1^{t_1}\cdots p_r^{t_r}$ 的形式, 其中 $t_i\geq 0$. 又由於對任意 $i\in\{1,\ldots,r\}$ 皆有 $p_i^{t_i}\mid d$ 故 $p_i^{t_i}\mid a$, 亦即 $p_i^{t_i}\mid p_1^{n_1}\cdots p_r^{n_r}$. 由於當 $i\neq j$ 時 $p_i\neq p_j$, 因此 $\gcd(p_i^{t_i},p_j^{n_j})=1$, 故由 Proposition 1.2.6(1)

得 $p_i^{t_i} \mid p_i^{n_i}$. 此時若 $t_i > n_i$, 會造成 $p^{t_i-n_i} \mid 1$ 之矛盾, 因此知 $t_i \le n_i$. 同理由 $d \mid b$ 可得 $t_i \le m_i$, 故得證 $0 \le t_i \le \min\{n_i, m_i\}$.

接著我們探討 $\gcd(a,b)$. 為了方便起見, 對於所有 $i \in \{1,\dots,r\}$, 我們令 $d_i = \min\{n_i, m_i\}$. 首先說明 $p_1^{d_1} \cdots p_r^{d_r}$ 為 a,b 的公因數. 對於 $i \in \{1,\dots,r\}$, 由於 $d_i \le n_i$, 故知 $p_i^{d_1} \mid p_i^{n_i}$. 因此得 $p_i^{d_i} \mid a$. 由於這是對所有 $i = 1,\dots,r$ 皆成立又因為 $p_1^{d_1},\dots,p_r^{d_r}$ 兩兩互質故由 Question 1.8 (2) 知 $p_1^{d_1} \cdots p_r^{d_r} \mid a$. 同理可得 $p_1^{d_1} \cdots p_r^{d_r} \mid b$. 最後對於任意 a,b 之公因數 d. 由上知 $d = p_1^{t_1} \cdots p_r^{t_r}$ 且 $0 \le t_i \le d_i$, 故由前面的討論知 $d \mid p_1^{d_1} \cdots p_r^{d_r}$. 得證 $\gcd(a,b) = p_1^{d_1} \cdots p_r^{d_r}$. □

雖然 Proposition 1.6.2 也是一個求得兩個數之最大公因數之方法, 不過在實際情況 (尤其是處理很大的數時) 由於分解質因數是很困難的事情, 所以仍是以輾轉相除法得最大公因數較管用. Proposition 1.6.2 重要之處是它很明確的告訴我們最大公因數長什麼樣子, 這在一些抽象理論的推導是有用的.

接下來我們可以利用 Proposition 1.4.2 將最小公倍數寫下.

Corollary 1.6.3. 假設 $a,b \in \mathbb{N}$ 且 $a,b > 1$. 若 $a = p_1^{n_1} \cdots p_r^{n_r}$ 且 $b = p_1^{m_1} \cdots p_r^{m_r}$, 其中 $p_1,\dots,p_r$ 為相異質數且 $n_i, m_i \ge 0$, 則

$$\operatorname{lcm}(a,b) = p_1^{\max\{n_1,m_1\}} \cdots p_r^{\max\{n_r,m_r\}}.$$

Proof. 由於 $ab = p_1^{n_1+m_1} \cdots p_r^{n_r+m_r}$ 利用 Proposition 1.4.2 以及 Proposition 1.6.2 知

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)} = p_1^{n_1+m_1-\min\{n_1,m_1\}} \cdots p_r^{n_r+m_r-\min\{n_r,m_r\}}.$$

對任意二數 x,y, 不失一般性我們假設 $x \ge y$, 此時我們有 $\min\{x,y\} = y$ 且 $\max\{x,y\} = x$, 因此得 $x + y = \min\{x,y\} + \max\{x,y\}$. 所以對任意 $i \in \{1,\dots,r\}$ 我們皆有 $\max\{n_i,m_i\} = n_i + m_i - \min\{n_i,m_i\}$, 因此得證本定理. □

當我們有多於兩個的整數時, 我們就可以利用質因數分解以及 Proposition 1.4.6 和 Proposition 1.4.7 將他們的最大公因數和最小公倍數寫下. 例如若 $a = p_1^{n_1} \cdots p_r^{n_r}$, $b = p_1^{m_1} \cdots p_r^{m_r}$ 且 $c = p_1^{t_1} \cdots p_r^{t_r}$, 其中 $p_1,\dots,p_r$ 為相異質數且 $n_i, m_i, t_i \ge 0$, 則

$$\gcd(a,b,c) = p_1^{\min\{n_1,m_1,t_1\}} \cdots p_r^{\min\{n_r,m_r,t_r\}}, \quad \operatorname{lcm}(a,b,c) = p_1^{\max\{n_1,m_1,t_1\}} \cdots p_r^{\max\{n_r,m_r,t_r\}}.$$

Exercise 1.19. 給定 $n \in \mathbb{N}$ 且 $n > 1$, 令 $l(n)$ 表示 n 最小的質因數, 例如 $l(91) = 7$. 假設 n 是合成數且 $1 < n < 300$ 試問 $l(n)$ 最大可能值為何?

Exercise 1.20. 試找出可能的一組 $a,b \in \mathbb{N}$ 滿足 $\gcd(a,b) = 12$ 且 $\operatorname{lcm}(a,b) = 360$.

Exercise 1.21. 假設 $a,b,n \in \mathbb{N}$ 若已知 $ab = n^2$ 且 $\gcd(a,b) = 1$, 試證明存在 $c,d \in \mathbb{N}$ 滿足 $a = c^2$ 且 $b = d^2$.

Exercise 1.22. 假設 $m \in \mathbb{N}$ 且 p 是質數, 如果 $p^a \mid m$ 且 $p^{a+1} \nmid m$, 則我們稱 p^a 恰整除 m 且用 $p^a || m$ 表示之. 現假設 $p^a || m$ 且 $p^b || n$.

(1) 若已知 $a < b$, 試求 r 滿足 $p^r || m+n$.

(2) 試舉一個 $a=b$ 的例子使得 $p^r||m+n$ 且 $r>a$.

(3) 試求 s 滿足 $p^s||mn$.

(4) 試求 t 滿足 $p^t||m^n$.

(5) 假設 $m<p^{a+1}$, 試求 v 滿足 $p^v||m!$.

Exercise 1.23. 利用以下步驟找出所有大於 1 的相異整數 a,b 滿足 $a^b=b^a$.

(1) 假設 $a<b$, 證明 $a \mid b$.

(2) 假設 $b=ak$, 證明 $a^{k-1}=k$.

(3) 證明若 a,k 皆為大於 1 的整數滿足 $a^{k-1}=k$, 則 $k=2$.

(4) 說明 $a=2,b=4$ 以及 $a=4,b=2$ 是所有滿足 $a^b=b^a$ 的相異正整數.

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 函數之假設矛盾, 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 1.2.10), 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 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

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

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.

Question 2.1. $v : \mathbb{N} \to \mathbb{N}$ 是否為 completely multiplicative?

Question 2.2. 假設 $f : \mathbb{N} \to \mathbb{C}$ 是一個 completely 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 是否為 completely multiplicative?

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, σ 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 的所有正因數之和. 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 σ 為 multiplicative.

既然 σ 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 σ 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

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

Question 2.3. $\sigma : \mathbb{N} \to \mathbb{N}$ 是否為 completely multiplicative?

Exercise 2.1. 我們定義一個 arithmetic function ρ 為 $\rho(1) = 1$ 且對 $n > 1$ 定義 $\rho(n) = 2^m$ 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.

(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 $f(n)$.

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 $F(n) = 0$.