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 1

整數的基本性質

雖然有些同學已對整數的性質相當了解, 我們想利用這個大家較熟悉的東西來介紹一下如何用比較“數學”的方法來處理問題. 有些簡單的問題我們可能會故意繞遠路來處理, 主要原因是希望大家能熟悉表達數學的方法和形式以及邏輯推演的過程. 所以這一章會顯得較為冗長. 若大家對這些性質已很熟悉且認為表達數學的能力已很成熟, 可以略過此章, 直接進入下一章.

1.1. 因數與倍數

首先我們介紹幾個符號順便複習一下集合的概念. 要知道符號是數學上幫助我們能簡明表達事情的必要工具, 大家應該要學習如何適切的使用符號.

在本講義中我們用 $\mathbb{Z}$ 來表示所有整數所成的集合. 所以 0 在 $\mathbb{Z}$ 中, 2 也在 $\mathbb{Z}$ 中, 2007 和 -365 也在 $\mathbb{Z}$ 中. 這樣一來當我們要說一個數 a 是整數時, 我們只要說 a 在 $\mathbb{Z}$ 中就好了. 在數學上我們要說一個東西在一個集合中就用“$\in$”這個符號, 也就是“屬於”的意思. 所以以後我們要表達 a 是一個整數就直接說 $a \in \mathbb{Z}$ 即可. 我們也常只考慮正整數, 在本講義中我們用 $\mathbb{N}$ 表示所有正整數所成的集合. 所以我們用 $a \in \mathbb{N}$ 來表示 a 是一個正整數.

對於整數一開始是由自然數出發，利用數數的方法我們定義了加法，接著有了負的概念整個整數加法的體系就建立起來了。給定 $a \in \mathbb{Z}$, 我們用 $2a$ 表示. $a+a$ 一般來說若 $n \in \mathbb{N}$ 我們將 n 個 a 相加的結果表為 na. 我們也將 $(-n)a$ 看成 n 個 $-a$ 相加所得之值. 若我們再將 $0a$ 定為 0, 如此一來對任意的 $m \in \mathbb{Z}$, ma 都有了定義. 如此定義出來的乘法和加法之間所滿足的運算規則如交換率, 結合率和分配率等此處就不再贅述. 我們將可以寫成 ma 其中 $m \in \mathbb{Z}$ 的數稱為 a 的倍數 (multiple). 另一方面若 b 是 a 的倍數, 我們也稱 a 是 b 的因數 (divisor). 符號記為 $a|b$.

我們將 a 的倍數所成的集合用 $a\mathbb{Z}$ 來表示. 也就是說 $a\mathbb{Z}$ 中的元素都是 ma 這樣的形式其中 $m \in \mathbb{Z}$. 這樣的集合可用 $a\mathbb{Z} = \{ma \mid m \in \mathbb{Z}\}$ 來表示. 因此我們可以說 $b \in a\mathbb{Z}$ 和 b 是 a 的倍數 (或 a 是 b 的因數) 是一樣的意思.

接下來我們想用集合的角度處理因數倍數的一些性質. 要注意這些性質大家高中時都已證過, 我們用集合的角度處理並沒有比較方便，介紹這樣的處理方法僅是利用它讓大家熟悉一下集合的語言.

首先注意若 $a\in\mathbb{Z}$, $a\mathbb{Z}$ 這一個集合並不單單是一個集合. 由於整數在加法和乘法之下有所謂的封閉性, $a\mathbb{Z}$ 也有以下兩個重要的封閉性.

Proposition 1.1.1. 假設 $a\in\mathbb{Z}$ 且 $b,c\in a\mathbb{Z}$. 則我們有以下之性質.

(1) $b+c\in a\mathbb{Z}$.

(2) 對任意 $m\in\mathbb{Z}$ 皆有 $mb\in a\mathbb{Z}$.

Proof. 因為 $b,c\in a\mathbb{Z}$ 依定義知存在 $n,n'\in\mathbb{Z}$ 使得 $b=na$ 且 $c=n'a$.

(1) 由分配率知 $b+c=na+n'a=(n+n')a$. 又由於 $n,n'\in\mathbb{Z}$ 我們知 $n+n'\in\mathbb{Z}$, 故得 $b+c\in a\mathbb{Z}$.

(2) 由結合率知 $mb=m(na)=(mn)a$. 又由於 $m,n\in\mathbb{Z}$ 我們知 $mn\in\mathbb{Z}$, 故得 $mb\in a\mathbb{Z}$. □

結合 Proposition 1.1.1 的結果我們有以下之性質.

Corollary 1.1.2. 假設 $a\in\mathbb{Z}$ 且 $b,c\in a\mathbb{Z}$. 若 $m,n\in\mathbb{Z}$ 則 $mb+nc\in a\mathbb{Z}$. 換言之, 若 $a|b$ 且 $a|c$, 則對任意 $m,n\in\mathbb{Z}$ 皆有 $a|mb+nc$.

Proof. 因為 $b,c\in a\mathbb{Z}$ 以及 $m,n\in\mathbb{Z}$, 由 Proposition 1.1.1(2) 知 $mb,nc\in a\mathbb{Z}$. 再利用 Proposition 1.1.1(1) 知 $mb+nc\in a\mathbb{Z}$. 也就是說 $a|mb+nc$. □

大部分一個重要的性質我們都會用 Proposition 來稱呼再冠上編號以便以後引用. 而直接套用 Proposition 所得的性質我們都用 Corollary 來稱呼.

接著我們來看集合單純的性質. 若 A,B 是集合且 A 中的元素都在 B 中, 則我們就用 $A\subseteq B$ 來表示 (稱 A 包含於 B). 很容易有以下之性質:

(1) 若 $A\subseteq B$ 且 $B\subseteq A$ 則 $A=B$.

(2) 若 $A\subseteq B$ 且 $B\subseteq C$ 則 $A\subseteq C$.

結合這集合的性質以及前面提的封閉性我們有以下之結果.

Proposition 1.1.3. 假設 $a,b,c\in\mathbb{Z}$. 我們有以下之結果.

(1) $b\mathbb{Z}\subseteq a\mathbb{Z}$ 若且唯若 $a|b$.

(2) 若 $a|b$ 且 $b|a$ 則 $a=\pm b$.

(3) 若 $a|b$ 且 $b|c$ 則 $a|c$.

Proof. (1) 若 $b\mathbb{Z}\subseteq a\mathbb{Z}$, 由於 $b\in b\mathbb{Z}$, 我們得 $b\in a\mathbb{Z}$. 故知 $a|b$. 反之, 若 $a|b$, 我們要證明 $b\mathbb{Z}\subseteq a\mathbb{Z}$. 一般來說要證明一個集合 B 包含於另一個集合 A, 我們要證明的是 B 中任取一個元素都會在 A 中. 因此此處我們要證的是任取 $b\mathbb{Z}$ 中的一個元素 mb, 其中 $m\in\mathbb{Z}$ 都可以得

到 $mb \in a\mathbb{Z}$. 然而由 $a|b$ 的假設我們知 $b \in a\mathbb{Z}$. 接著我們就可利用 Proposition 1.1.1(2) 知對任意 $m \in \mathbb{Z}$ 皆有 $mb \in a\mathbb{Z}$. 也就是說 $b\mathbb{Z}$ 的元素都在 $a\mathbb{Z}$ 中. 故得證 $b\mathbb{Z} \subseteq a\mathbb{Z}$.

(2) 若 $a|b$ 且 $b|a$, 由 (1) 知 $b\mathbb{Z} \subseteq a\mathbb{Z}$ 且 $a\mathbb{Z} \subseteq b\mathbb{Z}$. 因此由集合性質知 $a\mathbb{Z} = b\mathbb{Z}$. 也就是說 $a\mathbb{Z}$ 和 $b\mathbb{Z}$ 是相同的集合. 由此, 很容易看出當 $a = 0$ 時 $b = 0$. 反之亦然. 因此我們只剩考慮 $a \neq 0$ 且 $b \neq 0$ 的情況. 此時 $a\mathbb{Z}$ 中最小的正數 a (當 $a > 0$) 或 $-a$ (當 $a < 0$) 會等於 $b\mathbb{Z}$ 中最小的正數 b 或 $-b$. 故得證 $a = \pm b$.

(3) 若 $a|b$ 且 $b|c$, 則由 (1) 知 $b\mathbb{Z} \subseteq a\mathbb{Z}$ 且 $c\mathbb{Z} \subseteq b\mathbb{Z}$. 因此由集合性質知 $c\mathbb{Z} \subseteq a\mathbb{Z}$. 故再由 (1) 的等價關係知 $a|c$. □

Question 1.1. 假設 $a, b \in \mathbb{Z}$ 試證明 $a\mathbb{Z} = b\mathbb{Z}$ 若且唯若 $a = \pm b$.

Remark 1.1.4. 對於整數有一個很重要的性質 "well-ordering principle". 這一個 principle 就是說給定一個非空的整數的子集合 S, 如果 S 有下界 (若有一數小於 S 中所有的數, 則稱 S 有下界), 則 S 中必含有一個最小的整數 (通常用 $\min S$ 來表示). 同理若整數的非空子集合 S 有上界 (若有一數大於 S 中所有的數, 則稱 S 有上界), 則此集合中必含有一個最大的整數 (通常用 $\max S$ 來表示). 例如剛才 Proposition 1.1.3(2) 的證明中我們考慮 $a\mathbb{Z}$ 中最小的正整數, 當 $a > 0$ 時 a 就是 $a\mathbb{Z}$ 中最小的正整數. 這裡因為我們確實知道 $a\mathbb{Z}$ 這個集合長什麼樣, 所以並不需這個性質直接可知 a 就是最小的. 以後我們常會碰到一些抽象的正整數子集合, 那時就得經常用到整數的這個性質來確知此集合存在一個最小的正數. 另外要注意此性質在其他的情況如有理數就不對了. 事實上正有理數是有下界的 (0 小於所有的正有理數), 但並沒有所謂最小的正有理數.

再次強調一下前面我們用集合較抽象的方法證明整除的性質主要是要大家習慣集合的語言以及學習一些抽象的論證方法. 它並不是什麼特別的好方法. 比方說大家熟知的 $a|b$ 則 $ma|mb$ 就很難用類似上面集合的方法來處理. 總之, 要處裡一個問題並沒有說一定要用什麼方法. 你只要使用一個你認為可行且正確的方法處理. 所以學習數學絕不要僅是背誦定理的證明. 如何將繁瑣的證明整理成你自己習慣且能理解的語言才是重點. 接下來我們就回歸定義來證明前述之性質.

Lemma 1.1.5. 假設 $a, b \in \mathbb{Z}$ 且 $a|b$, 我們有以下之性質.

(1) 若 $m \in \mathbb{Z}$, 則 $ma|mb$.

(2) 若 $d|a$ 且 $d|b$, 則 $(a/d)|(b/d)$.

Proof. 由假設 $a|b$ 知存在 $n \in \mathbb{Z}$ 使得 $b = na$.

(1) 將等式兩邊同乘以 m 可得 $mb = mna = n(ma)$ 故知 $ma|mb$.

(2) $d|a$ 且 $d|b$ 即表示存在 $a', b' \in \mathbb{Z}$ 使得 $a = a'd$ 且 $b = b'd$. 故由 $b = na$ 得 $b'd = na'd$. 因為 $d \neq 0$, 兩邊同除以 d 可得 $b' = na'$, 即 $a'|b'$. 因為 $a/d = a'$ 且 $b/d = b'$ 故得證 $(a/d)|(b/d)$. □

Lemma 1.1.5 是一個簡單的性質. 它本身並不算什麼重大的性質, 但是以後討論許多性質時都要用到它, 我們便用 Lemma 稱呼之以方便引用.

在 Lemma 1.1.5(2) 中 $d|a$ 且 $d|b$ 的假設就是說 d 同時是 a 和 b 的因數, 我們簡稱之為 a,b 的 *common divisor* (公因數). 討論一些整數之間的關係時公因數和最大公因數以及公倍數和最小公倍數是很重要的工具. 接下來我們給它們下定義.

Definition 1.1.6. 令 $a_1,a_2,\ldots,a_n \in \mathbb{Z}$ 且皆不等於 0.

(1) 若 $c \in \mathbb{Z}$, 且 $c|a_1, c|a_2, \ldots, c|a_n$, 則稱 c 為 $a_1,a_2,\ldots,a_n$ 的 *common divisor* (公因數).

(2) 若 $d \in \mathbb{N}$ 是 $a_1,a_2,\ldots,a_n$ 的公因數中最大的, 則稱 d 為 $a_1,a_2,\ldots,a_n$ 的 *greatest common divisor* 最大公因數, 通常我們會用 $\gcd(a_1,a_2,\ldots,a_n)$ 來表示之.

(3) 若 $m \in \mathbb{Z}$, 且 $a_1|m, a_2|m, \ldots, a_n|m$, 則稱 m 為 $a_1,a_2,\ldots,a_n$ 的 *common multiple* (公倍數).

(4) 若 $l \in \mathbb{N}$ 是 $a_1,a_2,\ldots,a_n$ 的正的公倍數中最小的, 則稱 l 為 $a_1,a_2,\ldots,a_n$ 的 *least common multiple* 最小公倍數, 通常我們會用 $\mathrm{lcm}(a_1,a_2,\ldots,a_n)$ 來表示之.

通常當有一個符號或名詞需要介紹時, 為了方便找到我們會特別用 Definition 來標示之.

當要下一個定義時要注意是否合理. 不要給的定義的東西根本不存在或沒有用. Definition 1.1.6 中就要注意最大公因數及最小公倍數是否存在: 因為 1 整除所有的整數, 所以若 $a_1,a_2,\ldots,a_n \in \mathbb{Z}$ 則其公因數必存在. 又因為當 $a \neq 0$ 時, a 的任意因數皆小於等於 $|a|$, 故 $a_1,a_2,\ldots,a_n$ 的公因數所成的集合有上界, 所以我們知 $a_1,a_2,\ldots,a_n$ 的最大公因數必存在. 不過 $a_1,a_2,\ldots,a_n$ 的最大公因數有可能是 1. 若如此 (即 $\gcd(a_1,a_2,\ldots,a_n)=1$), 則稱 $a_1,a_2,\ldots,a_n$ 互質 (*relatively prime*). 另一方面因為 $a_1a_2\cdots a_n$ 是 $a_1,a_2,\ldots,a_n$ 的公倍數, 所以適當的乘上正負號可知 $a_1,a_2,\ldots,a_n$ 正的公倍數必存在, 因此由 well-ordering principle 知 $a_1,a_2,\ldots,a_n$ 的最小公倍數必存在.

接下來我們探討公因數及最大公因數的基本性質. 由於 a 和 $-a$ 的因數是一樣的, 所以不失一般性, 在討論因數時我們僅討論正整數的情形. 我們就從兩個正整數的情形開始討論.

Proposition 1.1.7. 假設 $a,b \in \mathbb{N}$ 且 d 是 a 和 b 的公因數. 若 d' 是 a/d 和 b/d 的公因數, 則 dd' 是 a 和 b 的公因數.

Proof. 首先注意, 由於 d 是 a,b 的公因數, 故存在 $m,n \in \mathbb{Z}$ 使得 $a=dm$ 且 $b=dn$. 也就是說 $a/d=m$ 和 $b/d=n$ 皆為整數. 又 d' 是 m,n 的公因數故存在 $m',n' \in \mathbb{Z}$ 使得 $m=d'm'$ 且 $n=d'n'$. 整理得 $a=dd'm'$ 且 $b=dd'n'$ 故知 dd' 是 a 和 b 的公因數. □

若 Proposition 1.1.7 中我們取 $d=\gcd(a,b)$, 則利用最大公因數的定義我們可得以下之性質.

Corollary 1.1.8. 假設 $a,b \in \mathbb{N}$ 且 $d=\gcd(a,b)$. 則 a/d 和 b/d 互質.

Proof. 要證明 a/d 和 b/d 互質就是證 $\gcd(a/d,b/d)=1$. 然而要說明 $\gcd(a/d,b/d)=1$ 就得說明若 d' 是 a/d 和 b/d 的一個正的公因數, 則 $d'=1$. 事實上若 d' 是 a/d 和 b/d 的一個的公因數, 則由 Proposition 1.1.7 知 dd' 是 a,b 的公因數. 然而已知 d 是 a,b 公因數中最

大的, 故知 $d \geq dd'$. 也就是說 $d' \leq 1$. 因此結合當初假設 d' 是 a,b 的一個正的公因數 (即 $d' \geq 1$) 得證 $d' = 1$. □

注意一般要證明 $d = \gcd(a,b)$ 我們要證明兩件事. 首先要證明 d 是 a,b 的公因數, 再來就是證明 d 是 a 和 b 的公因數中最大的. 前面 Corollary 1.1.8 中我們要證明 $\gcd(a/d, b/d) = 1$. 由於 1 必為 $a/d, b/d$ 的公因數, 所以只要證明任意 a/d 和 b/d 的公因數皆小於等於 1 就可.

Proposition 1.1.7 和 Corollary 1.1.8 都可以推廣到一般 n 個正整數的情形.

Question 1.2. 假設 $a_1, \ldots, a_n \in \mathbb{N}$. 試證明

(1) 若 d 是 $a_1, \ldots, a_n$ 的公因數且 d' 是 $a_1/d, \ldots, a_n/d$ 的公因數, 則 dd' 是 $a_1, \ldots, a_n$ 的公因數.

(2) 若 $d = \gcd(a_1, \ldots, a_n)$. 則 $\gcd(a_1/d, \ldots, a_n/d) = 1$.

等下一節探討除法原理之後, 我們再進一步談論最大公因數及最小公倍數其他的性質.

1.2. 除法原理與最大公因數

整數中最基本的定理應該就是整數的除法原理 *Division Algorithm*, 幾乎所有整數的基本性質都是由它推導出來.

Theorem 1.2.1 (Division Algorithm)**.** 給定一正整數 n, 對任意的 $m \in \mathbb{Z}$, 皆存在 $h, r \in \mathbb{Z}$, 其中 $0 \leq r < n$, 滿足 $m = h \cdot n + r$.

這是一個很重要的性質, 重要到我們以 Theorem 來稱呼它. 這個定理我們習慣稱為除法原理, 如此稱它當然就包含 "除" 這個概念. 首先觀察, 當我們在小學時處理 36 除以 7 的問題時, 我們會先嘗試 $36-7$, 發現所餘大於 7, 所以再考慮 $36-2\times 7$. 所餘還是太大, 因此再考慮 $36-3\times 7$, 這樣一直下去到 $36-5\times 7$ 夠小了, 我們便確定 36 除以 7 的商為 5 餘數為 1. 大家可以看出來, 這裡我們事實上是考慮 $\{36-7t \mid t \in \mathbb{Z}\}$ 這個集合中最小的非負整數, 便會是 36 除以 7 的餘數了. 利用這個想法, 我們便可以證明 Theorem 1.2.1 了.

Proof. 給定 $n \in \mathbb{N}$ 且 $m \in \mathbb{Z}$. 首先考慮 $W = \{m - t \cdot n \mid t \in \mathbb{Z}\}$ 這一個集合. 也就是收集 m, $m-n$, $m-2n, \ldots$ 以及 $m+n$, $m+2n, \ldots$ 等元素所得集合. 因為 t 可取任何整數, 很容易就看出 W 一定包含一些非負的整數. 換言之, 若考慮 W' 為 W 中非負的元素所成的集合, 則 W' 是一個非空的整數的子集合. 故由整數的 well-ordering principle 知 W' 中存在最小的整數 r. 即 r 是 W 中最小的非負的整數. 因為 $r \in W$, 由定義知存在 $h \in \mathbb{Z}$ 滿足 $r = m - h \cdot n$. 我們最主要的目的就是要證明 $0 \leq r < n$.

假設 r 不合我們的條件, 也就是說 $r \geq n$ (別忘了 r 是非負整數的假設). 若如此, 我們可將 r 寫成 $r = n + r'$, 其中 $r' \geq 0$. 因此利用

$$m = h \cdot n + r = h \cdot n + (n + r') = (h+1) \cdot n + r',$$

我們得到 $r' = m - (h+1) \cdot n \in W$. 但 $0 \leq r' < r$, 這和 r 是 W 中最小的非負整數相矛盾. 故得證本定理. □

要注意 Theorem 1.2.1 的證明我們用到整數上可以排序的 *well-ordering principle*, 因此雖然證明很簡單, 但並不能直接套用到其他的數系.

Division Algorithm 是整數論中一個重要的性質, 它可以幫助我們處理一個整數是否可以被另一個整數整除的問題. 底下我們就是要利用 Theorem 1.2.1 將 $\mathbb{Z}$ 中有哪些子集合可以寫成 $a\mathbb{Z}$ 這樣的形式確認出來.

回顧一下, 在上一節中我們知道當 $a\in\mathbb{Z}$, $a\mathbb{Z}$ 這一個集合有所謂的封閉性 (Proposition 1.1.1), 即若 $b,c\in a\mathbb{Z}$ 則對任意 $m,n\in\mathbb{Z}$ 皆有 $mb+nc\in a\mathbb{Z}$. 現在我們要說明, 反過來也成立. 也就是說若 S 是 $\mathbb{Z}$ 的一個非空子集且有封閉性 (即滿足若 $b,c\in S$ 則對任意 $m,n\in\mathbb{Z}$ 皆有 $mb+nc\in S$), 我們要證明存在 $a\in\mathbb{Z}$ 使得 $S=a\mathbb{Z}$.

首先觀察因 S 為非空, 故必存在 $b\in S$, 因此由封閉性的假設知 $b+(-1)b=0\in S$. 也就是說 0 一定在 S 中. 現若 $S=\{0\}$, 則令 $a=0$, 我們自然有 $S=a\mathbb{Z}$. 因此我們僅剩下 $S\neq\{0\}$ 的情形要考慮. 要怎樣找到 $a\in\mathbb{Z}$ 使得 $S=a\mathbb{Z}$ 呢? 我們知道若 $S=a\mathbb{Z}$, 那麼 S 中最小的正整數就是 a 或 $-a$. 所以要找到 a 滿足 $S=a\mathbb{Z}$, 我們自然也會考慮 S 中最小的正整數了. 令 S' 為 S 中的正整數所成的集合, 即 $S'=S\cap\mathbb{N}$. 我們先說明 S' 不是空集合. 這是因為由 $S\neq\{0\}$ 知存在 $b\in S$ 且 $b\neq 0$. 若 $b>0$, 則知 $b\in S'$; 而若 $b<0$, 由 $0\in S$ 以及封閉性知 $0-b=-b\in S$, 因此由 $-b>0$, 得知 $-b\in S'$. 最後由 S' 為非空集合且有下界知存在 $a\in S'$ 且是 S' 中最小的元素. 我們要說明此時 $S=a\mathbb{Z}$. 回顧一下, 當我們要說兩個集合相等時, 便要說明這兩個集合互相有包含關係. 因為 $a\in S$, 故由封閉性知對任意 $m\in\mathbb{Z}$, $ma\in S$, 因此得證 $a\mathbb{Z}\subseteq S$. 最後我們剩下要證明 $S\subseteq a\mathbb{Z}$ 了. 也就是要證明對任意 $b\in S$, 皆滿足 $b\in a\mathbb{Z}$. 換言之, 我們要證明 S 中的任意元素 b 皆可被 a 所整除. 這就是我們要用到 division algorithm 的時機了. 由於 $a\in\mathbb{N}$, 由 Theorem 1.2.1 知存在 $h,r\in\mathbb{Z}$ 使得 $b=ha+r$, 且 $0\leq r<a$. 要注意此時 $r=b-ha$, 而 a,b 皆屬於 S, 故由封閉性知 $r\in S$. 現若 $r\neq 0$, 表示 $r\in\mathbb{N}$, 故由 $r\in S$ 得 $r\in S'$. 然而 $r<a$, 這便和 a 是 S' 中的最小元素相矛盾了. 故知 $r=0$, 也因此得證 $b=ha\in a\mathbb{Z}$. 我們將上面討論的結果整理如下.

Theorem 1.2.2. 假設 $S\subseteq\mathbb{Z}$ 為非空集合且 S 滿足對於任意 $b,c\in S$ 以及 $m,n\in\mathbb{Z}$ 皆有 $mb+nc\in S$, 則存在 $a\in\mathbb{Z}$ 使得 $S=a\mathbb{Z}$. 特別的, 當 $S\neq\{0\}$, 令 a 為 $S\cap\mathbb{N}$ 中最小的元素, 此時可得 $S=a\mathbb{Z}$.

Question 1.3. 考慮 $S=\{4x+6y\mid x,y\in\mathbb{Z}\}$. 試證明 S 滿足對任意 $b,c\in S$ 以及 $m,n\in\mathbb{Z}$ 皆有 $mb+nc\in S$. 試找出 $a\in\mathbb{Z}$ 使得 $S=a\mathbb{Z}$.

接下來我們利用 Theorem 1.2.2 來探討有關最大公因數重要的性質. 我們還是從兩個正整數的情況開始探討. 給定 $a,b\in\mathbb{N}$, 如果我們能找到一個集合 S 滿足 $a,b\in S$ 且具有封閉性, 則由 Theorem 1.2.2 便可知存在 $d\in\mathbb{Z}$ 使得 $S=d\mathbb{Z}$. 此時由於 $a,b\in S=d\mathbb{Z}$, 故知 a,b 皆為 d 的倍數, 也就是說 d 會是 a,b 的公因數. 然而現若有另一集合 S' 亦滿足 $a,b\in S'$ 且具有封閉性, 同理知存在 $d'\in\mathbb{Z}$ 使得 $S'=d'\mathbb{Z}$, 此時 d' 亦為 a,b 的公因數. 現若又假設 $S\subseteq S'$, 亦即 $d\mathbb{Z}\subseteq d'\mathbb{Z}$, 則由 Proposition 1.1.3(1) 知 $d'\mid d$. 從這裡我們可以知道, 當我們找的 S 越小, 可得到 a,b 的公因數就越大. 所以現在的目標便是要找到一個最小的集合 S 滿足 $a,b\in S$ 且具有封閉性.

怎樣的集合 S 會是包含 a,b 且具有封閉性的最小的集合呢? 依封閉性的要求, 由 $a,b\in S$ 我們得對任意 $m,n\in\mathbb{Z}$ 皆需 $ma+nb\in S$. 因此 S 的最小的可能就是 $S=\{ma+nb\mid m,n\in\mathbb{Z}\}$. 我們將證明這樣定出的 S 確實有封閉性, 也因此得到以下的性質.

Proposition 1.2.3. 假設 $a,b\in\mathbb{N}$, 令 d 為集合 $S=\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中最小的正整數. 則 $\gcd(a,b)=d$.

Proof. 首先注意由於這裡 m,n 是任意的整數, 所以我們知道集合 $S=\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中必存在正整數. 因此我們套用 well-ordering principle 知 S 中必有最小的正整數. 也就是說敘述中的 d 一定存在.

接著我們要先說明 S 是封閉的然後按照前面提的兩個步驟證明 d 為 a,b 的最大公因數. 任取 $u,v\in S$, 由 S 的定義我們知存在 $r,r',s,s'\in\mathbb{Z}$ 使得 $u=ra+sb$, $v=r'a+s'b$. 現對任意 $m,n\in\mathbb{Z}$, 我們有

$$mu+nv=m(ra+sb)+n(r'a+s'b)=(mr+nr')a+(ms+ns')b.$$

因此由 $mr+nr',ms+ns'\in\mathbb{Z}$ 得 $mu+nv\in S$, 證明了 S 的封閉性. 所以由 Theorem 1.2.2 知 $S=d\mathbb{Z}$. 也因此由 $a\in S$ 以及 $b\in S$ 得證 $a\in d\mathbb{Z}$ 以及 $b\in d\mathbb{Z}$. 也就是說 $d|a$ 且 $d|b$, 亦即 d 是 a,b 的公因數.

最後我們要證明 d 是 a,b 的公因數中最大的數. 也就是要證明若 d' 是 a,b 的公因數, 則 $d'\le d$. 今由於 $d\in S$, 由 S 的定義知存在 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$. 然而 $d'|a$ 且 $d'|b$, 由 Corollary 1.1.2 知 $d'|ma+nb$. 即 $d'|d$, 也就是說存在 $l\in\mathbb{Z}$ 使得 $d=d'l$. 因此由已知 $d>0$ 當然得 $d'\le d$. □

或許大家會奇怪, 一般來說找 a,b 的最大公因數只要在 a,b 有限多個公因數中找最大的就好了為什麼要自討苦吃在 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 這個有無窮多個元素的集合中找? 沒有錯, 如果 a,b 很具體的知道是什麼當然直接找. 然而當我們要討論一般的情形, a,b 是任何可能的整數, 不能用幾個具體例子代一代就了事. 所以雖然 Proposition 1.2.3 在實際操作時並不實用但要用到理論的推演時它卻是很好用來表達最大公因數的工具. 直接利用 Proposition 1.2.3 我們馬上有以下之性質.

Corollary 1.2.4. 假設 $a,b\in\mathbb{N}$ 且 $d=\gcd(a,b)$ 則存在 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$. 而且對任意 $d'\in\mathbb{Z}$, d' 是 a,b 的公因數若且唯若 $d'|d$.

Proof. 由 Proposition 1.2.3 我們知 d 在集合 $S=\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中, 故依定義存在 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$.

注意這裡“若且唯若”的意思就是說如果 d' 是 a,b 的公因數那麼 d 必整除 a,b 的最大公因數 d, 反之若 d' 整除 a,b 的最大公因數, 那麼 d' 一定是 a,b 的公因數. 由 Proposition 1.2.3 的證明我們知若 d' 是 a,b 的公因數則 $d'|d$. 反之若 $d'|d$, 則由於 $d|a$ 且 $d|b$, 利用 Proposition 1.1.3(3) 知 $d'|a$ 且 $d'|b$. 即 d' 為 a,b 的公因數. □

一般來說有的性質可以從甲可推得乙, 但這並不表示從乙可推得甲. 如果兩個性質可以互推, 我們就用 "若且唯若" 表示之. 特別要注意 Corollary 1.2.4 並不是說若有一個正整數 d 可找到 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$, 則 d 就是 a,b 的公因數. 這是一開始大家在學習邏輯推論時常犯的錯誤. 其實 d 可以寫成 $ma+nb$ 僅表示 d 會在集合 $S=\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中, 並不表示 d 會是 S 中最小的正整數. 所以當然 d 就未必是 a,b 的最大公因數. 因此當要證明 d 是 a,b 的最大公因數時, 還是得按部就班如前面所提的兩步驟進行, 千萬不要找到兩個整數 m,n 使得 $d=ma+nb$ 就說 d 就是 a,b 的最大公因數. 當然了如果你要證明 a,b 互質 (即 $\gcd(a,b)=1$) 時可以利用找到 m,n 使得 $ma+nb=1$ 來處理. 這是因為此時 1 在 S 中, 故當然是 S 中最小的正整數了. 因此我們將此特殊情況列出.

Corollary 1.2.5. 假設 $a,b\in\mathbb{N}$. 則 $\gcd(a,b)=1$ 若且唯若存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$.

Proof. 再強調一次, 要證明若且唯若必需兩個方向都證明.

若 $\gcd(a,b)=1$, 由 Corollary 1.2.4 知存在 $m,n\in\mathbb{Z}$ 使得 $1=ma+nb$. 反之, 若存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$, 則 1 必為集合 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中最小的正整數, 故由 Proposition 1.2.3 知 $\gcd(a,b)=1$. □

以上的性質並沒有告訴我們怎麼找到 m,n 使得 $ma+nb=\gcd(a,b)$, 我們將會在下節介紹完輾轉相除法後給一個方法來求 m,n. 雖然目前我們不知如何求得 m,n, 不過從下一個探討 a,b 互質時的重要的性質我們可以看到僅僅知道它們的存在性在理論的推演就很管用了.

Proposition 1.2.6. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$. 我們有以下的性質:

(1) 若 $k\in\mathbb{Z}$ 且 $a|bk$, 則 $a|k$.

(2) 若 $l\in\mathbb{Z}$ 且 $a|l$ 及 $b|l$, 則 $ab|l$.

Proof. 因為 $\gcd(a,b)=1$, 由 Corollary 1.2.5 我們知存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$.

(1) 將 $ma+nb=1$ 等式兩邊乘上 k 可得 $mak+nbk=k$. 然而假設 $a|bk$ 故利用 $a|ak$ 以及 Corollary 1.1.2 知 $a|mak+nbk$, 即 $a|k$.

(2) 由 $a|l$ 以及 $b|l$ 知存在 $r,s\in\mathbb{Z}$ 使得 $l=ar=bs$. 因為 $a|ar$ 故得 $a|bs$. 再由 $\gcd(a,b)=1$ 的假設利用 (1) 可得 $a|s$. 換言之存在 $t\in\mathbb{Z}$ 使得 $s=at$. 將之帶回 $l=bs$ 得 $l=b(at)=(ab)t$, 得證 $ab|l$. □

要注意 Proposition 1.2.6 的條件. 一般來說若沒有 a,b 互質的假設 $a|bc$ 並不能保證 $a|b$ 或 $a|c$. 就拿 $12|6\times4$ 來說吧, 很明顯的 $12\nmid6$ (這裡 $\nmid$ 表示不整除的意思) 而且 $12\nmid4$. 同樣的若 a,b 不互質 $a|c$ 且 $b|c$ 也不能保證 $ab|c$. 例如 $4|12$ 且 $6|12$ 但是 $4\times6\nmid12$.

接下來我們來看看 a,b 的最小公倍數. 若 l 是 a,b 的最小公倍數, 則由於 $\gcd(a,b)|l$, 我們自然知存在 $m,n\in\mathbb{Z}$ 使得 $l=ma+nb$. 不過這個表示法對 l 就沒有什麼幫助了. 主要原因是 l 在 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 這個集合中不像 $\gcd(a,b)$ 有如 Proposition 1.2.3 所述一樣特殊的地位. 不過沒關係, 下一個定理告訴我們一般來說只要了解 a,b 的最大公因數就能掌握 a,b 的最小公倍數.

讓我們先來看看要怎樣知道 l 是 a,b 的最小公倍數. 就如同最大公因數的情形一樣我們要證明兩件事. 首先證明 l 是 a,b 的正的公倍數, 再來就是證明 l 是 a 和 b 的正的公因數中最小的. 如此一來就能擔保 l 是 a,b 的最小公倍數.

Proposition 1.2.7. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=d$ 及 $\operatorname{lcm}(a,b)=l$, 則 $l=ab/d$. 而且 $m\in\mathbb{Z}$ 是 a,b 的公倍數若且唯若 $l|m$.

Proof. 由假設 $d=\gcd(a,b)$ 知存在 $a',b'\in\mathbb{N}$ 使得 $a=a'd$, $b=b'd$ 且 $\gcd(a',b')=1$ (Proposition 1.1.8). 現在我們依上述兩個步驟證明 $ab/d=a'b=b'a$ 是 a,b 的最小公倍數.

首先由 $ab/d=b'a$ 知 $a|(ab/d)$ 同理知 $b|(ab/d)$, 也就是說 ab/d 為 a 和 b 的公倍數. 又因為 a,b,d 皆為正數, 所以 ab/d 為 a,b 之正的公倍數.

接著證明若 m 為 a,b 之正的公倍數, 則 $(ab/d)\le m$. 由假設知存在 $m',n'\in\mathbb{N}$ 使得 $m=m'a=n'b$. 換言之 $m=m'a'd=n'b'd$, 故消掉 d (因 $d\neq 0$) 得 $m'a'=n'b'$. 也就是說 $a'|n'b'$. 但由於 $\gcd(a',b')=1$, 故由 Proposition 1.2.6(1) 知 $a'|n'$. 也就是說存在 $h\in\mathbb{N}$ 使得 $n'=a'h$. 代回 $m=n'b$ 得 $m=ha'b$, 故得知 $a'b=(ab/d)|m$. 由於 ab/d 及 m 皆為正數, 得證 $(ab/d)\le m$. 也就是說 $ab/d=\operatorname{lcm}(a,b)=l$.

既然 $ab/d=l$ 由上面的證明我們知若 m 為 a,b 的公倍數, 則 $l=(ab/d)|m$. 反之, 若 $l|m$, 則由 $a|l$ 且 $b|l$, 得知 $a|m$ 且 $b|m$, 故 m 為 a,b 之公倍數. □

要注意雖然 Proposition 1.2.7 中假設 $a,b\in\mathbb{N}$, 但其目的僅是利用其為正數方便描述最小公倍數. 若 $a,b\in\mathbb{Z}$ 不一定為正時, 我們只要適當的加上負號仍可利用 Proposition 1.2.7 的式子寫下最小公倍數. 另外和 Corollary 1.2.4 中所述公因數為最大公因數之因數相輝映 Proposition 1.2.7 告訴我們公倍數為最小公倍數之倍數.

接下來讓我們來看看有關多個 (多於兩個) 整數的最大公因數性質. 我們試著著推廣前面的方法, 看看前面的結果對多個整數是否適用.

Proposition 1.2.8. 假設 $a_1,\dots,a_n\in\mathbb{N}$, 令 d 為集合 $S=\{m_1a_1+\cdots+m_na_n\mid m_1,\dots,m_n\in\mathbb{Z}\}$ 中最小的正整數. 則 $\gcd(a_1,\dots,a_n)=d$.

Proof. 和前面的情形相同, 利用 well-ordering principle 知 S 中必有最小的正整數. 也就是說敘述中的 d 一定存在. 接著和前面一樣, 我們知 S 是封閉的, 故由 Theorem 1.2.2 得 $S=d\mathbb{Z}$. 因此可按照前面證明最大公因數的步驟證明 d 為 $a_1,\dots,a_n$ 的最大公因數.

首先檢查對所有 $i\in\{1,\dots,n\}$, 皆有 $d|a_i$. 由於 $a_i\in S=d\mathbb{Z}$, 故知 $d|a_i$. 也就是說 d 為 $a_1,\dots,a_n$ 的公因數.

接著我們要證明 d 是 $a_1,\dots,a_n$ 的公因數中最大的數. 也就是要證明若 d' 是 $a_1,\dots,a_n$ 的公因數, 則 $d'\le d$. 依定義, 存在 $m_1,\dots,m_n\in\mathbb{Z}$ 使得 $d=m_1a_1+\cdots+m_na_n$. 今由於對任意 $i\in\{1,\dots,n\}$, 皆有 $d'|a_i$ 故知 $d'|m_1a_1+\cdots+m_na_n$. 即 $d'|d$, 因此由已知 $d>0$ 當然得 $d'\le d$. □

有了 Proposition 1.2.8 我們當然可以和前面的方法一樣得到以下之結果, 證明就不再贅述.

Corollary 1.2.9. 假設 $a_1,\dots,a_n \in \mathbb{N}$ 且 $d = \gcd(a_1,\dots,a_n)$ 則存在 $m_1,\dots,m_n \in \mathbb{Z}$ 使得 $d = m_1a_1+\cdots+m_na_n$. 而且對任意 $d' \in \mathbb{Z}$, d' 是 $a_1,\dots,a_n$ 的公因數若且唯若 $d'|d$.

要注意並不是所有有關兩個整數的最大公因數的性質都可以推廣到多個整數的情形. 例如 Proposition 1.2.6(2) 告訴我們若 $\gcd(a,b)=1$ 且 $a|l$ 及 $b|l$, 則 $ab|l$. 此性質在兩個以上整數的情形就不一定對. 主要原因就是依多個整數互質的定義 $a_1,a_2,\dots,a_n$ 互質是表示這些數除了 ±1 之外沒有共同的因數, 但不表示任取其中兩個數都互質. 其實有可能任意 a_i,a_j 都不互質但是 $a_1,\dots,a_n$ 仍互質. 例如 $a_1=6$, $a_2=15$ 以及 $a_3=10$ 的情形. 我們有 $\gcd(a_1,a_2)=3$, $\gcd(a_2,a_3)=5$ 以及 $\gcd(a_1,a_3)=2$ 但是 $\gcd(a_1,a_2,a_3)=1$. 所以有些情形僅假設 $a_1,\dots,a_n$ 互質是不夠的, 我們須用到任取兩個都互質 (即對任意 $i,j\in\{1,\dots,n\}$ 且 $i\neq j$, 皆有 $\gcd(a_i,a_j)=1$) 這一個較強的互質性才行. 這種較強的互質性我們稱之為 "兩兩互質" (*pairwise relatively prime*). 當然了若 $a_1,\dots,a_n$ 兩兩互質, 則 $a_1,\dots,a_n$ 必互質. 大家一定要清楚這兩種互質性之不同. Proposition 1.2.6(2), 在多個整數的情形之下若改為兩兩互質就會成立. 由於這裡牽涉到任意多個整數, 所以得用到數學歸納法來證明. 數學歸納法的原理我們假設大家已了解, 此處不再贅述.

Proposition 1.2.10. 假設 $a_1,\dots,a_n \in \mathbb{N}$ 且這些 a_i 兩兩互質. 若令 $M = a_1\cdots a_n$, 則我們有以下之性質.

(1) 對任意 $i\in\{1,\dots,n\}$ 皆有 $\gcd(a_i,M/a_i)=1$.

(2) 若對所有 $i\in\{1,\dots,n\}$ 皆有 $a_i|l$, 則 $M|l$.

Proof. 由於僅在多於一個整數時才談最大公因數, 所以我們數學歸納法從 $n=2$ 開始.

(1) 此處由於和 $a_1,\dots,a_n$ 的排序無關, 我們僅處理 $i=1$ 的情形. 首先看 $n=2$ 的情形. 此時 $M=a_1a_2$ 故由假設 $\gcd(a_1,a_2)=1$ 知 $\gcd(a_1,M/a_1)=1$. 再來由數學歸納法假設 $n=k-1$ 時成立, 即 $\gcd(a_1,a_2\cdots a_{k-1})=1$. 此時存在 $m',n'\in\mathbb{Z}$ 使得

$$m'a_1+n'(a_2\cdots a_{k-1})=1. \tag{1.1}$$

現考慮 $n=k$ 之情形, 此時 $M=a_1a_2\cdots a_k$. 將式子 (1.1) 兩邊乘以 a_k 得

$$m'a_1a_k+n'(a_2\cdots a_{k-1}a_k)=m'a_ka_1+n'(M/a_1)=a_k. \tag{1.2}$$

又由兩兩互質的假設知 $\gcd(a_1,a_k)=1$, 即存在 $r,s\in\mathbb{Z}$ 使得 $ra_1+sa_k=1$. 以式子 (1.2) 之 a_k 代入上式得

$$1=ra_1+s(m'a_ka_1+n'(M/a_1))=(r+sm'a_k)a_1+sn'(M/a_1).$$

因為 $r+sm'a_k\in\mathbb{Z}$ 且 $sn'\in\mathbb{Z}$ 故由 Corollary 1.2.5 知 $\gcd(a_1,M/a_1)=1$.

(2) 首先考慮 $n=2$ 的情形, 此時 $M=a_1a_2$ 且 $\gcd(a_1,a_2)=1$ 故 Proposition 1.2.6(2) 告訴我們若 $a_1|l$ 且 $a_2|l$, 則 $M|l$. 再來由數學歸納法假設 $n=k-1$ 時成立, 即若令 $M'=a_1\cdots a_{k-1}$,

則 $M'|l$. 現考慮 $n=k$ 之情形, 此時 $M=a_1\cdots a_{k-1}a_k=M'a_k$. 由 (1) 知 $\gcd(a_k,M')=\gcd(a_k,M/a_k)=1$, 故由假設 $a_k|l$ 且 $M'|l$ 以及 Proposition 1.2.6(2) 知 $M'a_k=M|l$. □

接下來我們來看, 若我們會求兩個整數的最大公因數 (參見下一節之輾轉相除法) 那麼我們就可以兩個兩個地求得多個整數的最大公因數. 也就是說可以先求 $d_1=\gcd(a_1,a_2)$ 求得 $d_2=\gcd(a_1,a_2,a_3)=\gcd(d_1,a_3)$, 這樣一直下去以求得 $\gcd(a_1,a_2,\cdots,a_n)$. 我們的證明方法還是利用前述證明最大公因數方法進行.

Proposition 1.2.11. 若 $a_1,\ldots,a_n\in\mathbb{N}$ $(n>2)$, 則

$$\gcd(a_1,\ldots,a_{n-1},a_n)=\gcd(\gcd(a_1,\ldots,a_{n-1}),a_n).$$

Proof. 令 $d=\gcd(\gcd(a_1,\ldots,a_{n-1}),a_n)$ 首先我們要證明 d 是 $a_1,\ldots,a_n$ 的公因數. 由於 $d|\gcd(a_1,\ldots,a_{n-1})$ 由 Corollary 1.2.9 知 d 是 $a_1,\ldots,a_{n-1}$ 的公因數. 再加上 $d|a_n$, 故知 d 是 $a_1,\ldots,a_{n-1},a_n$ 的公因數.

現假設 d' 是 $a_1,\ldots,a_{n-1},a_n$ 的公因數. 當然 d' 是 $a_1,\ldots,a_{n-1}$ 的公因數, 故由 Corollary 1.2.9 知 $d'|\gcd(a_1,\ldots,a_{n-1})$. 再加上 $d'|a_n$, 故知 d' 是 $\gcd(a_1,\ldots,a_{n-1})$ 和 a_n 的公因數, 故再由 Corollary 1.2.4 知 $d'|\gcd(\gcd(a_1,\ldots,a_{n-1}),a_n)=d$. 得證 d 是 $a_1,\ldots,a_n$ 的公因數中最大的數, 故為 $a_1,\ldots,a_n$ 的最大公因數. □

最後我們看看多個整數的最小公倍數的性質. 首先要注意的是 Proposition 1.2.7 中 $\operatorname{lcm}(a,b)=ab/\gcd(a,b)$ 這個性質在多個整數時並不一定對. 例如前面所提 $a_1=6$, $a_2=15$ 以及 $a_3=10$ 的例子, 我們有 $a_1a_2a_3=900$, $\gcd(a_1,a_2,a_3)=1$ 但是 $\operatorname{lcm}(a_1,a_2,a_3)=30$. 雖然如此, 我們仍有公倍數為最小公倍數之倍數的性質, 而且求多個整數之最小公倍數也可如最大公因數一樣兩個兩個進行. 底下我們將利用數學歸納法同時證明這兩個性質. 這種重要的證明技巧大家或許沒有見過, 不過其原理如同一般的數學歸納法原理, 大家應能理解.

Proposition 1.2.12. 若 $a_1,\ldots,a_n\in\mathbb{N}$ $(n>2)$, 則

$$\operatorname{lcm}(a_1,\ldots,a_{n-1},a_n)=\operatorname{lcm}(\operatorname{lcm}(a_1,\ldots,a_{n-1}),a_n).$$

而且 $m\in\mathbb{Z}$ 是 $a_1,\ldots,a_n$ 的公倍數若且唯若 $\operatorname{lcm}(a_1,\ldots,a_n)|m$.

Proof. 應用數學歸納法, 當 $n=3$ 時令 $l=\operatorname{lcm}(\operatorname{lcm}(a_1,a_2),a_3)$. 因為 l 為 $\operatorname{lcm}(a_1,a_2)$ 和 a_3 之公倍數, 知 l 為 $\operatorname{lcm}(a_1,a_2)$ 之倍數, 故由 Proposition 1.2.7 得知 l 為 a_1,a_2 的公倍數. 故 l 為 a_1,a_2,a_3 之公倍數. 現假設 m 為 a_1,a_2,a_3 之公倍數. 當然 m 是 a_1,a_2 之公倍數, 故由 Proposition 1.2.7 知 $\operatorname{lcm}(a_1,a_2)|m$. 又因 m 為 a_3 之倍數, 故知 m 為 $\operatorname{lcm}(a_1,a_2)$ 和 a_3 之公倍數. 因此再由 Proposition 1.2.7 知 $l=\operatorname{lcm}(\operatorname{lcm}(a_1,a_2),a_3)|m$. 我們證得了 l 是 a_1,a_2,a_3 的正公因數中最小的數, 故得 $l=\operatorname{lcm}(a_1,a_2,a_3)$. 我們也同時證得 l 整除所有 a_1,a_2,a_3 的公倍數. 反之, 若 $l|m$, 則由 $a_1|l$, $a_2|l$ 以及 $a_3|l$ 知 m 為 a_1,a_2,a_3 的公倍數. 因此 $n=3$ 的情形證明完成.

現依數學歸納法假設 $n=k-1$ 時成立: 即

$$\operatorname{lcm}(a_1,\ldots,a_{k-1})=\operatorname{lcm}(\operatorname{lcm}(a_1,\ldots,a_{k-2}),a_{k-1})$$

且 $m\in\mathbb{Z}$ 是 $a_1,\dots,a_{k-1}$ 的公倍數若且唯若 $\operatorname{lcm}(a_1,\dots,a_{k-1})|m$. 現考慮 $n=k$ 之情形. 令 $l'=\operatorname{lcm}(a_1,\dots,a_{k-1})$ 且 $l=\operatorname{lcm}(l',a_k)$ 我們要證明 l 是 $a_1,\dots,a_k$ 的最小公倍數.

由於 $l=\operatorname{lcm}(l',a_k)$ 是 $l'=\operatorname{lcm}(a_1,\dots,a_{k-1})$ 的倍數, 故由數學歸納法假設 ($n=k-1$ 之情況) 知 l 為 $a_1,\dots,a_{k-1}$ 的公倍數. 再加上 l 也是 a_k 的倍數, 故得知 l 是 $a_1,\dots,a_k$ 的公倍數. 另一方面若 m 是 $a_1,\dots,a_{k-1},a_k$ 的公倍數, 當然 m 是 $a_1,\dots,a_{k-1}$ 的公倍數. 故由數學歸納法假設知 $l'=\operatorname{lcm}(a_1,\dots,a_{k-1})|m$. 再加上 $a_k|m$, 知 m 為 l' 和 a_k 之公倍數. 故由 Proposition 1.2.7 知 $l=\operatorname{lcm}(l',a_k)|m$. 因而得知 l 確為 $a_1,\dots,a_k$ 的正公倍數中最小者, 也就是說 $l=\operatorname{lcm}(a_1,\dots,a_k)$. 我們也同時證得若 m 為 $a_1,\dots,a_k$ 的公倍數, 則 $l|m$. 反之若 $l|m$, 則由對所有 $i\in\{1,\dots,k\}$ 皆有 $a_i|l$, 得證 $a_i|m$. 也就是說 m 為 $a_1,\dots,a_k$ 的公倍數. □

1.3. 輾轉相除法

輾轉相除法是求最大公因數很有效率的方法. 首先我們介紹輾轉相除法的原理.

Lemma 1.3.1. *若 $a,b\in\mathbb{N}$ 且 $a=bh+r$, 其中 $h,r\in\mathbb{Z}$, 則 $\gcd(a,b)=\gcd(b,r)$.*

Proof. 假設 $d_1=\gcd(a,b)$ 且 $d_2=\gcd(b,r)$. 我們證明 $d_1|d_2$ 且 $d_2|d_1$, 因而可利用 Proposition 1.1.3(2) 以及 d_1,d_2 皆為正數得證 $d_1=d_2$.

因 $d_1|a$ 且 $d_1|b$ 利用 Corollary 1.1.2 我們知 $d_1|a-bh=r$. 因為 $d_1|b$, $d_1|r$ 且 $d_2=\gcd(b,r)$ 故由 Proposition 1.2.4 知 $d_1|d_2$. 另一方面, 因為 $d_2|b$ 且 $d_2|r$ 故 $d_2|bh+r=a$. 因此可得 $d_2|d_1$. □

Lemma 1.3.1 告訴我們當 $a>b>0$ 時, 要求 a,b 的最大公因數我們可以先將 a 除以 b 所得餘數若為 r, 則 a,b 的最大公因數等於 b 和 r 的最大公因數. 因為 $0\le r<b<a$, 所以當然把計算簡化了. 接著我們就來看看輾轉相除法. 由於 $\gcd(a,b)=\gcd(-a,b)$ 所以我們只要考慮 a,b 都是正整數的情況.

Theorem 1.3.2 (The Euclidean Algorithm)**.** 假設 $a,b\in\mathbb{N}$ 且 $a>b$. 由除法原理我們知存在 $h_0,r_0\in\mathbb{Z}$ 使得

$$a=bh_0+r_0,\quad \text{其中 } 0\le r_0<b.$$

若 $r_0>0$, 則存在 $h_1,r_1\in\mathbb{Z}$ 使得

$$b=r_0h_1+r_1,\quad \text{其中 } 0\le r_1<r_0.$$

若 $r_1>0$, 則存在 $h_2,r_2\in\mathbb{Z}$ 使得

$$r_0=r_1h_2+r_2,\quad \text{其中 } 0\le r_2<r_1.$$

如此繼續下去直到 $r_n=0$ 為止. 若 $n=0$ (即 $r_0=0$), 則 $\gcd(a,b)=b$. 若 $n\ge1$, 則 $\gcd(a,b)=r_{n-1}$.

Proof. 首先注意若 $r_0\neq0$, 由於 $r_0>r_1>r_2>\dots$ 是嚴格遞減的, 因為 r_0 和 0 之間最多僅能插入 r_0-1 個正整數, 所以我們知道一定會有 $n\le r_0$ 使得 $r_n=0$.

若 $r_0=0$, 即 $a=bh_0$, 故知 b 為 a 之因數, 得證 b 為 a,b 的最大公因數. 若 $r_0>0$, 則由 Lemma 1.3.1 知

$$\gcd(a,b)=\gcd(b,r_0)=\gcd(r_0,r_1)=\cdots=\gcd(r_{n-1},r_n)=\gcd(r_{n-1},0)=r_{n-1}.$$

□

現在我們來看用輾轉相除法求最大公因數的例子.

Example 1.3.3. 我們求 $a=481$ 和 $b=221$ 的最大公因數. 首先由除法原理得 $481=2\cdot 221+39$, 知 $r_0=39$. 因此再考慮 $b=221$ 除以 $r_0=39$ 得 $221=5\cdot 39+26$, 知 $r_1=26$. 再以 $r_0=39$ 除以 $r_1=26$ 得 $39=1\cdot 26+13$, 知 $r_2=13$. 最後因為 $r_2=13$ 整除 $r_1=26$ 知 $r_3=0$, 故由 Theorem 1.3.2 知 $\gcd(481,221)=r_2=13$.

在利用輾轉相除法求最大公因數時, 大家不必真的求到 $r_n=0$. 例如在上例中可看出 $r_0=39$ 和 $r_1=26$ 的最大公因數是 13, 利用 Lemma 1.3.1 馬上得知 $\gcd(a,b)=13$.

在上一節 Corollary 1.2.4 告訴我們若 $\gcd(a,b)=d$, 則存在 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$. 當時我們沒有提到如何找到此 m,n. 現在我們利用輾轉相除法來介紹一個找到 m,n 的方法. 我們沿用 Theorem 1.3.2 的符號. 首先看 $r_0=0$ 的情形, 此時 $d=\gcd(a,b)=b$ 所以若令 $m=0$, $n=1$, 則我們有 $d=b=ma+nb$. 當 $r_0\neq 0$ 但 $r_1=0$ 時, 我們知 $d=\gcd(a,b)=r_0$. 故利用 $a=bh_0+r_0$ 知, 若令 $m=1$, $n=-h_0$, 則 $d=r_0=ma+nb$. 同理若 $r_0\neq 0$, $r_1\neq 0$ 但 $r_2=0$, 則知 $d=\gcd(a,b)=r_1$. 故利用 $a=bh_0+r_0$ 以及 $b=r_0h_1+r_1$ 知

$$r_1=b-r_0h_1=b-(a-bh_0)h_1=-h_1a+(1+h_0h_1)b.$$

因此若令 $m=-h_1$ 且 $n=1+h_0h_1$, 則 $d=r_1=ma+nb$. 依照此法, 當 r_0,r_1 和 r_2 皆不為 0 時, 由於 $d=\gcd(a,b)=r_{n-1}$ 故由 $r_{n-3}=r_{n-2}h_{n-1}+r_{n-1}$ 知 $d=r_{n-3}-h_{n-1}r_{n-2}$. 利用數學歸納法我們知存在 $m_1,m_2,n_1,n_2\in\mathbb{Z}$ 使得 $r_{n-3}=m_1a+n_1b$ 且 $r_{n-2}=m_2a+n_2b$ 故代入得

$$d=(m_1a+n_1b)-h_{n-1}(m_2a+n_2b)=(m_1-h_{n-1}m_2)a+(n_1-h_{n-1}n_2)b.$$

因此若令 $m=m_1-h_{n-1}m_2$ 且 $n=n_1-h_{n-1}n_2$, 則 $d=ma+nb$.

上面的說明看似好像當 $r_0\neq 0$ 時對每一個 $i\in\{0,1,\ldots,n-2\}$ 要先將 r_i 寫成 $r_i=m_ia+n_ib$, 最後才可將 $d=r_{n-1}$ 寫成 $ma+nb$ 的形式. 其實這只是論證時的方便, 在實際操作時我們其實是將每個 r_i 寫成 $m_i'r_{i-2}+n_i'r_{i-1}$ 的形式慢慢逆推回 $d=ma+nb$. 請看以下的例子.

Example 1.3.4. 我們試著利用 Example 1.3.3 的結果找到 $m,n\in\mathbb{Z}$ 使得 $13=481m+221n$. 首先我們有 $13=r_2=39-26=r_0-r_1$. 而 $r_1=221-5\cdot 39=b-5r_0$, 故得 $13=r_0-(b-5r_0)=6r_0-b$. 再由 $r_0=481-2\cdot 221=a-2b$, 得知 $13=6(a-2b)-b=6a-13b$. 故得 $m=6$ 且 $n=-13$ 會滿足 $13=481m+221n$.

要注意這裡找到的 m,n 並不會是唯一滿足 $d=ma+nb$ 的一組解. 雖然上面的推演過程好像會只有一組解, 不過只能說是用上面的方法會得到一組解, 並不能擔保可找到所有的解. 比方說若令 $m'=m+b$, $n'=n-a$, 則 $m'a+n'b=(m+b)a+(n-a)b=ma+nb=d$. 所以 m',n' 也會是另一組解. 因此以後當要探討唯一性時, 若沒有充分的理由千萬不能說由前

面的推導過程看出是唯一的就斷言是唯一. 一般的作法是假設你有兩組解, 再利用這兩組解所共同滿足的式子找到兩者之間的關係. 我們看看以下的作法.

Proposition 1.3.5. 假設 $a,b\in\mathbb{N}$ 且 $d=\gcd(a,b)$. 若 $x=m_0,y=n_0$ 是 $d=ax+by$ 的一組整數解, 則對任意 $t\in\mathbb{Z}$, $x=m_0+bt/d,y=n_0-at/d$ 皆為 $d=ax+by$ 的一組整數解, 而且 $d=ax+by$ 的所有整數解必為 $x=m_0+bt/d,y=n_0-at/d$ 其中 $t\in\mathbb{Z}$ 這樣的形式.

Proof. 假設 $x=m,y=n$ 是 $d=ax+by$ 的一組解. 由於已假設 $x=m_0,y=n_0$ 也是一組解, 故得 $am+bn=am_0+bn_0$. 也就是說 $a(m-m_0)=b(n_0-n)$. 由於 $d=\gcd(a,b)$, 我們可以假設 $a=a'd$, $b=b'd$ 其中 $a',b'\in\mathbb{Z}$ 且 $\gcd(a',b')=1$ (參見 Corollary 1.1.8). 因此得 $a'(m-m_0)=b'(n_0-n)$. 利用 $b'|a'(m-m_0)$, $\gcd(a',b')=1$ 以及 Proposition 1.2.6(1) 得 $b'|m-m_0$. 也就是說存在 $t\in\mathbb{Z}$ 使得 $m-m_0=b't$. 故知 $m=m_0+b't=m_0+bt/d$. 將 $m=m_0+bt/d$ 代回 $am+bn=am_0+bn_0$ 可得 $n=n_0-at/d$, 因此得證 $d=ax+by$ 的整數解都是 $x=m_0+bt/d,y=n_0-at/d$ 其中 $t\in\mathbb{Z}$ 這樣的形式. 最後我們僅要確認對任意 $t\in\mathbb{Z}$, $x=m_0+bt/d,y=n_0-at/d$ 皆為 $d=ax+by$ 的一組整數解. 然而將 $x=m_0+bt/d,y=n_0-at/d$ 代入 $ax+by$ 得 $a(m_0+bt/d)+b(n_0-at/d)=am_0+bn_0=d$, 故得證本定理. □

利用 Proposition 1.3.5 我們就可利用 Example 1.3.4 找到 $13=481x+221y$ 的一組整數解 $x=6,y=-13$ 得到 $x=6+17t,y=-13-37t$ 其中 $t\in\mathbb{Z}$ 是 $13=481x+221y$ 所有的整數解.

1.4. 質數

這一節我們要談整數的分解中最基本的元素: 質數. 大家都知道一個質數 p 就是正因數只有 1 和本身的數. 我們仍給一個正式的定義.

Definition 1.4.1. 若 $p\in\mathbb{Z}$, $p>1$ 且 p 的正公因數只有 p 和 1 則稱 p 是一個質數 (prime number). 若一正整數有其他的正因數則稱為合成數 (composite number).

簡單來說質數就是無法分解成兩個較小的正整數乘積的數. 質數這一種不可分解的特性讓它有很多特殊性質. 例如給定一質數 p 以及一整數 $a\in\mathbb{Z}$, 我們很容易判定 $\gcd(a,p)$ 為何. 若 $d=\gcd(a,p)$ 則因 $d|p$, 知 $d=1$ 或 $d=p$. 然而 $d=p$ 表示 $p|a$, 因此若已知 $p\nmid a$, 則可得 $d=1$. 所以利用 Proposition 1.2.6(1) 我們有以下之結論.

Lemma 1.4.2 (Euclid)**.** 假設 p 是一個質數, 且 $a,b\in\mathbb{Z}$. 若 $p|ab$, 則 $p|a$ 或 $p|b$.

Proof. 這裡我們要證明 $p|a$ 或 $p|b$. 如果 $p|a$ 當然就可以了 (不必擔心是否 $p|b$); 但若 $p\nmid a$, 那麼我們就得證明 $p|b$. 不過由前知 $p\nmid a$ 表示 $\gcd(p,a)=1$, 故利用 Proposition 1.2.6(1) 得證 $p|b$. □

Euclid 這一個 Lemma 告訴我們一個質數若是 ab 的因數那它一定是 a,b 其中之一的因數. 事實上這個性質並不只適用在兩個整數相乘的情況, 我們很容易推廣至更多數相乘之情況.

Corollary 1.4.3. 假設 p 是一個質數, 且 $a_1,a_2,\ldots,a_n\in\mathbb{Z}$. 若 $p|a_1a_2\cdots a_n$, 則存在 $i\in\{1,\ldots,n\}$ 滿足 $p|a_i$.

Proof. 我們依然用數學歸納法證明. 當 $k=2$ 時由 Lemma 1.4.2 知若 $p|a_1a_2$, 則 $p|a_1$ 或 $p|a_2$. 假設 $k=n-1$ 時成立, 即若有 $n-1$ 個整數 $a_1,\ldots,a_{n-1}$ 滿足 $p|a_1\cdots a_{n-1}$, 則存在 $i\in\{1,\ldots,n-1\}$ 使得 $p|a_i$. 現考慮 $k=n$ 的情形, 若 $a_1,\ldots,a_n$ 是 n 個整數滿足 $p|a_1\cdots a_n$, 則令 $a=a_1\cdots a_{n-1}$, $b=a_n$. 此時由 $p|ab$ 及 Lemma 1.4.2 知 $p|a$ 或 $p|b$. 若 $p|a$, 則由數學歸納法假設知存在 $i\in\{1,\ldots,n-1\}$ 使得 $p|a_i$, 而若 $p|b$ 即 $p|a_n$, 故得證本定理. □

若一質數 p 是一整數 a 的因數, 則我們稱 p 是 a 的一個質因數. 當然了質數 p 本身就是 p 的質因數, 而一個合成數會不會有質因數呢? 大家很自然的覺得一定有, 我們還是給一個正式的證明.

Lemma 1.4.4. 假設 $a\in\mathbb{Z}$ 且 $a>1$. 則必存在一質數 p 使得 $p|a$.

Proof. 我們用數學歸納法. 首先若 $a=2$, 則由於 2 是質數我們得 $p=2$ 為所求. 現假設對任意 $b\in\mathbb{Z}$ 滿足 $2\le b\le n$ 的數皆存在質數 p 使得 $p|b$, 我們考慮 $a=n+1$ 的情形. 若 a 本身是質數那當然 $p=a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b\in\mathbb{Z}$ 且 $2\le b<a$ 使得 $b|a$. 故由數學歸納法假設知存在一質數 p 滿足 $p|b$. 因此利用 Proposition 1.1.3(2) 得證 $p|a$. □

雖然正整數有無窮多個而 Lemma 1.4.4 告訴我們每一個大於 1 的正整數都有質因數, 但這並不代表會有無窮多個質數. 接著我們就是要探討質數確有無窮多個. 一般來說要證明質數有無窮多個或許會有的想法是希望利用現有的質數創造更大的質數. 不過這個想法是不可行的, 主要的原因是到目前為止我們沒有一個判別一個數是否為質數好的方法. 另類的思考是用反證法, 假設只有有限個質數而得到矛盾. 這個方法就不會碰到判別質數的問題, 相信由此大家更能體會到反證法的妙用.

Theorem 1.4.5 (Euclid)**.** 質數有無窮多個.

Proof. 我們用反證法假設只有有限個質數. 既然只有有限個我們可以將之一一列出, 就假設 $p_1,\ldots,p_n$ 是所有的質數. 現考慮 $a=p_1\cdots p_n+1$, 由 Lemma 1.4.4 知必有一質數 p_i, $i\in\{1,\ldots,n\}$ 滿足 $p_i|a$. 然而 p_i 本身整除 $p_1\cdots p_n$ 故由 Corollary 1.1.2 知 $p_i|a-p_1\cdots p_n$, 也就是說 $p_i|1$ 而得到矛盾. 故知不可能僅有有限多個質數, 而得證有無窮多個質數. □

質數雖然有無窮多個不過他們的分布不是非常稠密的. 例如給定任意大的整數 n 我們可以找到 n 個連續整數都不是質數. 我們的找法是考慮

$$(n+1)!+2,(n+1)!+3,\ldots,(n+1)!+n+1$$

這 n 個連續整數. 很容意看出它們都不是質數. 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 1.4.6. 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 p 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 1.4.4 知存在質數 p 使得 $p|a$. 既然 $p|a$ 我們得 $p\le a\le\sqrt{n}$ 且 $p|n$. □

Proposition 1.4.6 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 1.4.6 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.

質數既然有無窮多個, 接下來我們可以問是否有些特定形式的質數也會有無窮多個? 例如我們知道偶數中只有 2 是質數, 因此可以將所有奇數分類, 分成 $4n+1$ 和 $4n+3$ 這兩類然後問哪一類會有無窮多個質數. 要注意 $4n+1$ 這一類的數有一重要特性就是兩個 $4n+1$ 形式的數相乘仍然是 $4n+1$ 的形式. 因此任意有限多個 $4n+1$ 形式的數相乘仍是 $4n+1$ 的形式, 也就是說這一類的數有乘法封閉性. 另一方面 $4n+3$ 的形式的數就沒有這個特性, 事實上兩個 $4n+3$ 形式的數相乘會變成 $4n+1$ 的形式. 利用這兩類數的特性以及類似 Lemma 1.4.4 的證明, 我們有以下之結果.

Lemma 1.4.7. 假設 $a=4n+3$ 其中 $n\in\mathbb{N}\cup\{0\}$, 則必存在一質數 $p=4n'+3$ 其中 $n'\in\mathbb{N}\cup\{0\}$ 滿足 $p|a$.

Proof. 我們利用數學歸納法證明. 首先若 $a=3$, 則由於 3 是質數我們得 $p=3$ 為所求. 現假設對任意 $b=4k+3\in\mathbb{Z}$ 滿足 $0\le k\le n-1$ 的數皆存在質數 $p=4k'+3$ 使得 $p|b$, 我們考慮 $k=n$ 的情形. 若 $a=4n+3$ 本身是質數那當然 $p=a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b,c\in\mathbb{N}$ 其中 $b<a$ 且 $c<a$ 使得 $a=bc$. 注意 b, c 中必有一個元素是 $4k+3$ 形式, 否則 b,c 都是 $4k+1$ 形式會造成 $bc=a$ 也是 $4k+1$ 形式的矛盾現象. 就假設 $b=4k+3$ 吧! 此時 $0\le k\le n-1$ (因 $b<a$), 故由歸納假設知存在 $p=4k'+3$ 使得 $p|b$, 因而得證 $p|a$. □

注意 $4n+1$ 形式的數並不一定有 $4n+1$ 形式的質因數. 9 就是最簡的的例子. 觀察由 Lemma 1.4.4 推得 Theorem 1.4.5 的關係, 同樣的我們也可利用 Lemma 1.4.7 推得 $4n+3$ 形式的質數有無窮多個.

Proposition 1.4.8. 集合 $S=\{4n+3\mid n\in\mathbb{Z},n\ge0\}$ 中有無窮多個質數.

Proof. 我們依然用反證法假設 S 中只有有限多個質數並令 $p_0=3,p_1,\ldots,p_n$ 是 S 中所有的相異質數. 現考慮 $a=4(p_1\cdots p_n)+3$. 由於 $a\in S$ 利用 Lemma 1.4.7 知必有一質數 $p\in S$ 滿足 $p|a$, 故由假設知存在 $i\in\{0,\ldots,n\}$ 使得 $p=p_i$, .

若 $p=p_0=3$, 則由 $3|a$, $3|3$ 以及 $a-3=4(p_1\cdots p_n)$ 得知 $3|4(p_1\cdots p_n)$, 故由 Corollary 1.4.3 得到 $3|4$ 或者 $3|p_i$, $i\in\{1,\ldots,n\}$ 這樣的矛盾.

若 $p=p_i$ 其中 $i\in\{1,\ldots,n\}$, 則由 p_i 本身整除 $p_1\cdots p_n$ 知 $p_i|a-4(p_1\cdots p_n)$, 也就是說 $p_i|3$ 而得到矛盾. 故得證 S 中不可能僅有有限多個質數. □

因為 Lemma 1.4.7 並不適用於 $4n+1$ 形式的整數, 所以 Proposition 1.4.8 的方法不能用來討論 $4n+1$ 形式的質數, 不過 $4n+1$ 形式的質數仍有無窮多個. 事實上數論一個很重要的定理 (Dirichlet Theorem) 告訴我們對任意互質的兩整數 a,b 皆有無窮多個 $an+b$ 形式的質數. 這個定理的證明超出本講義範圍, 我們就不再多談了.

1.5. 算數基本定理

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

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

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 $p_i=q_i$, $n_i=m_i$, $\forall i\in\{1,\ldots,r\}$.

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. 如果 a 本身是個質數, 則 $a=p_1$ (即 $r=1,n_1=1$), 得證存在性. 如果 a 不是質數呢? 由定義知存在 $a_1,b_1\in\mathbb{N}$ 且 $a_1\neq 1$, $b_1\neq 1$ 滿足 $a=a_1\cdot b_1$. 接下來就是看 a_1,b_1 是不是質數了. 如果其中有一個不是質數, 我們就繼續分解下去直到得到質數為止. 這個過程一定會停下來因為每次分解後得的數越來越小. 當然最後就可以將 a 寫成一些質數的乘積了. 這樣的證明方式, 相信大家會有一種說不清楚的感覺, 所以我們還是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.

我們依然用歸納法證唯一性, 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. 由於 p_1 是質數, 故由 $p_1 \mid a = q_1^{m_1} \cdots q_s^{m_s}$ 以及 Corollary 1.4.3 知存在某個 $j \in \{1,\ldots,s\}$ 滿足 $p_1 \mid q_j$. 變換一下順序我們可以假設 $p_1 \mid q_1$. 由於 q_1 是質數, q_1 的因數只能是 ± 1 或 $\pm q_1$. 故由 $p_1 \mid q_1$ 知 $p_1 = q_1$. 現在考慮

$$\frac{a}{p_1} = p_1^{n_1-1} p_2^{n_2} \cdots p_r^{n_r} = q_1^{m_1-1} q_2^{n_2} \cdots q_s^{m_s}.$$

由於 $a/p_1 < a$, 故利用唯一性的歸納法假設我們得 $r = s$ 且經過適當排序 $p_2 = q_2,\ldots,p_r = q_r$ 以及 $n_1 = m_1$, $n_2 = m_2,\ldots,n_r = m_r$, 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 1.5.2. 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. 為了方便起見, 對於所有 $i \in \{1,\ldots,r\}$, 我們令 $d_i = \min\{n_i, m_i\}$. 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 1.4.3 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 $p_i^{t_i} \mid p_1^{n_1} \cdots p_r^{n_r}$. 由於若 $i \neq j$ 則 $p_i \neq p_j$, 知此時 $\gcd(p_i^{t_i}, p_j^{n_j}) = 1$, 故由 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 $t_i \leq n_i$. 同理由 $d \mid b$ 可得 $t_i \leq m_i$, 故得證 $0 \leq t_i \leq d_i$.

接著我們探討 $\gcd(a,b)$. 首先說明 $p_1^{d_1} \cdots p_r^{d_r}$ 為 a,b 的公因數. 對於 $i \in \{1,\ldots,r\}$, 由於 $d_i \leq n_i$, 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 $i = 1,\ldots,r$ 皆成立又因為 $p_1^{d_1},\ldots,p_r^{d_r}$ 兩兩互質故由 Proposition 1.2.10 (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 $0 \leq t_i \leq d_i$, 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 1.5.2 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 1.5.2 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 1.2.7 將最小公倍數寫下.

Corollary 1.5.3. 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 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i\geq 0$, 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 1.2.7 以及 Proposition 1.5.2 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 $x\geq y$, 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 $i\in\{1,\ldots,r\}$ 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 1.2.11 和 Proposition 1.2.12 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 $p_1,\ldots,p_r$ 為相異質數且 $n_i,m_i,t_i\geq 0$, 則

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