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 $m\in\mathbb{Z}$, 皆存在唯一的 $h,r\in\mathbb{Z}$, 其中 $0\le r<n$, 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 $36-2\times7$. 所餘還是太大, 因此再考慮 $36-3\times7$, 這樣一直下去到 $36-5\times7$ 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 $m\in\mathbb{Z}$. 首先我們證明存在性. 考慮 $W=\{m-t\cdot n\,|\,t\in\mathbb{Z}\}$ 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 $0\le r<n$.

假設 r 不合我們的條件, 也就是說 $r\ge n$ (別忘了 r 是非負整數的假設). 若如此, 我們可將 r 寫成 $r=n+\tilde{r}$, 其中 $\tilde{r}\ge0$. 因此利用

$$m=h\cdot n+r=h\cdot n+(n+\tilde{r})=(h+1)\cdot n+\tilde{r},$$

我們得到 $\tilde{r}=m-(h+1)\cdot n\in W$. 但 $0\le\tilde{r}<r$, 這和 r 是 W 中最小的非負整數相矛盾. 因此證明了 $0\le r<n$.

至於唯一性, 我們假設 $h',r'\in\mathbb{Z}$, 也滿足 $0\le r'<n$ 以及 $m=h'\cdot n+r'$. 此時因 $h\cdot n+r=m=h'\cdot n+r'$, 知 $n(h-h')=r'-r$. 但由於 $0\le r,r'<n$, 我們有 $n\cdot|h-h'|=|r-r'|<n$. 此式會成立只有在 $h-h'=0$, 故得 $h=h'$ 以同時得 $r=r'$. 我們證明了唯一性故得證本定理. □

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, Lemma 1.1.1 (2) 告訴我們若 $a\in\mathbb{Z}$, 則 $a\mathbb{Z}$ 這一個集合有所謂的封閉性, 即若 $b,c\in a\mathbb{Z}$ 則對任意 $m,n\in\mathbb{Z}$ 皆有 $mb+nc\in a\mathbb{Z}$ (參見 Question 1.1). 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 1.4. 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 $d\in d\mathbb{Z}$ 得 $d\in d'\mathbb{Z}$, 亦即 $d'\mid d$. 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 $d\mid a$ 且 $d\mid b$, 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 $d'\mid a$ 且 $d'\mid b$, 由 Corollary 1.1.1 知 $d'\mid ma+nb$. 即 $d'\mid d$, 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 $d'\mid d$.

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 $d'\mid d$. 反之若 $d'\mid d$, 則由於 $d\mid a$ 且 $d\mid b$, 利用 Proposition 1.1.1(1) 知 $d'\mid a$ 且 $d'\mid b$. 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 未必會是 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 $a\mid bk$, 則 $a\mid k$.

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

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 $a\mid bk$ 故利用 $a\mid ak$ 以及 Corollary 1.1.1 知 $a\mid mak+nbk$, 即 $a\mid k$.

(2) 由 $a\mid l$ 以及 $b\mid l$ 知存在 $r,s\in\mathbb{Z}$ 使得 $l=ar=bs$. 因為 $a\mid ar$ 故得 $a\mid bs$. 再由 $\gcd(a,b)=1$ 的假設利用 (1) 可得 $a\mid s$. 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 $ab\mid l$. □

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

由於 Corollary 1.2.5 是互質的充要條件, 所以如我們已知兩數是互質可用它, 而且也可以用它來證明兩數是互質的. 下面這個 Lemma 就是很好的例子.

Lemma 1.2.7. 假設 $\gcd(a,b)=1$ 以及 $\gcd(a,c)=1$, 則 $\gcd(a,bc)=1$.

Proof. 由 Corollary 1.2.5, 我們知存在 $m,n\in\mathbb{Z}$ 以及 $m',n'\in\mathbb{Z}$ 使得 $ma+nb=1$ 以及 $m'a+n'c=1$. 兩式相乘得

$$1=(ma+nb)(m'a+n'c)=(mam'+mn'c+nbm')a+(nn')bc=1.$$

由於 $mam'+mn'c+nbm'\in\mathbb{Z}$ 且 $nn'\in\mathbb{Z}$, 故再由 Corollary 1.2.5, 得知 $\gcd(a,bc)=1$. □

利用 Lemma 1.2.7, 我們可以得到以下 Proposition 1.2.6 (2) 的推廣.

Proposition 1.2.8. 假設 a,b,c 兩兩互質 (即 $\gcd(a,b)=\gcd(a,c)=\gcd(b,c)=1$), 若 $a|l$, $b|l$ 及 $c|l$, 則 $abc|l$.

Proof. 因 $\gcd(b,c)=1$ 且 $b|l$, $c|l$, 由 Proposition 1.2.6 (2) 知 $bc|l$. 再因 $\gcd(a,b)=\gcd(a,c)=1$, 由 Lemma 1.2.7 得 $\gcd(a,bc)=1$. 因此再由 Proposition 1.2.6 (2) 得證 $abc|l$. □

Exercise 1.3. 以下我們介紹兩種不同形式的 division algorithm (除法原理). 這裡我們僅假設 $a,b\in\mathbb{Z}$ 且 $b\neq 0$ (不必假設 $b\in\mathbb{N}$).

(1) 證明存在唯一的 $h,r\in\mathbb{Z}$ 滿足

$$a=bh+r \text{ 且} 0\leq r<|b|.$$

(2) 證明存在唯一的 $h,r\in\mathbb{Z}$ 滿足

$$a=bh+r \text{ 且} -\frac{|b|}{2}<r\leq\frac{|b|}{2}.$$

Exercise 1.4. 假設 $a,m,n\in\mathbb{N}$ 且 $a>1$, 以下我們要證明 $a^m-1\mid a^n-1$ 若且唯若 $m\mid n$.

(1) 利用因式分解 $x^h-1=(x-1)(x^{h-1}+x^{h-2}+\cdots+x+1)$ (其中 $h\in\mathbb{N}$), 證明若 $m\mid n$, 則 $a^m-1\mid a^n-1$.

(2) 證明若 $a^m-1\mid a^{m'+r}-1$ (其中 m',r 為非負整數) 且 $a^m-1\mid a^{m'}-1$, 則 $a^m-1\mid a^r-1$. (參考 Exercise 1.1 (5))

(3) 假設 $a^m-1\mid a^n-1$, 證明 $m\mid n$. (利用除法原理將 m 除以 n 並利用題 (1)(2)).

Exercise 1.5. 假設 $a,b\in\mathbb{Z}$. 試證明 $d=\gcd(a,b)$ 若且唯若 $d\mid a$, $d\mid b$ 且存在 $m,n\in\mathbb{Z}$ 滿足 $ma+nb=d$.

Exercise 1.6. 假設 $a,b\in\mathbb{Z}$ 且 d 是集合 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中最小的正整數. 試證明若 $r\in\mathbb{N}$, 則 rd 是集合 $\{mra+nrb\mid m,n\in\mathbb{Z}\}$ 中最小的正整數. 依此證明 $\gcd(ra,rb)=r\gcd(a,b)$.

Exercise 1.7. 假設 $a,b,c\in\mathbb{Z}$, 試利用定理：「$\gcd(a,b)=1$ 若且唯若存在 $r,s\in\mathbb{Z}$ 使得 $ra+sb=1$」證明以下有關於互質的性質.

(1) 假設 $m,n\in\mathbb{N}$. 試證明 $\gcd(a,b)=1$ 若且唯若 $\gcd(a^m,b^n)=1$. (Hint: 利用二項式定理)

(2) 假設 $\gcd(a,b)=1$ 且 $c\mid a+b$. 試證明 $\gcd(a,c)=\gcd(b,c)=1$.