*Chapter 1*

# 整數的基本性質

開始的第一章, 為了完整性, 我們從整數的基本性質出發. 若同學已對整數的性質相當了解, 可以略過此章, 直接進入下一章.

## 1.1. 因數與倍數

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 $2a$ 來表示 $a+a$. 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律, 結合律和分配律等此處就不再贅述.

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 $a \mid b$.

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.

接下來我們要處理因數倍數的一些性質. 考慮 $a,b,c \in \mathbb{Z}$. 首先若 $b$ 是 $a$ 的倍數且 $c$ 是 $b$ 的倍數, 表示存在 $r,s \in \mathbb{Z}$ 使得 $b = ra$ 且 $c = sb$. 此時由乘法的結合律我們有

$$c = sb = s(ra) = (sr)a.$$

由於 $sr \in \mathbb{Z}$, 可知 $c$ 為 $a$ 的倍數. 這一個結果是用結合律得到的, 事實上整數的加法與乘法間有分配律. 利用分配律, 我們可以進一步得到以下的性質.

現假設 $b,c$ 皆為 $a$ 的倍數. 這表示存在 $r,s \in \mathbb{Z}$ 使得 $b = ra$ 且 $c = sa$. 此時對任意 $m,n \in \mathbb{Z}$, 由分配律得

$$mb + nc = m(ra) + n(sa) = (mr + ns)a.$$

也就是說 $mb+nc$ 仍為 $a$ 的倍數.

**Question 1.1.** 假設 $a \in \mathbb{Z}$, 試說明對任意 $b,c \in a\mathbb{Z}$ 以及 $m,n \in \mathbb{Z}$ 皆有 $mb+nc \in a\mathbb{Z}$.

整數的乘法中有一個重要的性質，即：若 $a,b$ 皆不為 0，則 $ab \neq 0$。另一個重要的性質, 就是有乘法單位元素 1. 也就是說 1 乘上任意的整數 $a$ 仍為 $a$ (即 $1\cdot a = a$), 這個大家都知道. 其實更重要的是 1 是唯一的整數有這個性質的. 事實上若 $a$ 為非 0 的整數且 $x$ 滿足 $x\cdot a = a$ 則 $x$ 一定是 1.

**Question 1.2.** 上面的敘述為何要假設 $a \neq 0$ 呢? 試說明為何若 $a \neq 0$ 且 $x$ 滿足 $x\cdot a = a$ 則 $x = 1$.

1 還有一個特性, 也就是若 $x,y \in \mathbb{Z}$ 滿足 $x\cdot y = 1$, 則 $x = 1, y = 1$ 或 $x = -1, y = -1$.

**Question 1.3.** 試說明上述的性質為何成立.

利用這些有關 1 的特性. 我們可以得到若 $b$ 是 $a$ 的倍數且 $a$ 是 $b$ 的倍數, 則 $b = a$ 或 $b = -a$. 這是因為存在 $r,s \in \mathbb{Z}$ 滿足 $b = ra$ 且 $a = sb$, 故

$$a = sb = s(ra) = (sr)a.$$

現若 $a = 0$, 則 $b = ra = 0 = a$ 成立, 而若 $a \neq 0$, 則由前述 1 的性質可得 $r = 1$ 或 $r = -1$, 亦即 $b = a$ 或 $b = -a$. 我們將前面提的這些性質用以下的數學方法表示.

**Lemma 1.1.1.** 假設 $a,b,c \in \mathbb{Z}$. 我們有以下之結果.

(1) 若 $a \mid b$ 且 $b \mid c$ 則 $a \mid c$.

(2) 若 $a \mid b$ 且 $a \mid c$ 則對任意 $m,n \in \mathbb{Z}$ 皆有 $a \mid mb + nc$.

(3) 若 $a \mid b$ 且 $b \mid a$ 則 $a = \pm b$.

我們再試著由倍數的定義以及整數的加法乘法運算性質來證明以下之性質.

**Lemma 1.1.2.** 假設 $a,b,m \in \mathbb{Z}$ 且 $m \neq 0$. 則 $a \mid b$ 若且唯若 $ma \mid mb$.

**Proof.** 首先假設 $a \mid b$, 知存在 $n \in \mathbb{Z}$ 使得 $b = na$. 故將等式兩邊同乘以 $m$ 可得 $mb = mna = n(ma)$, 因此得 $ma \mid mb$.

反之, 若已知 $ma \mid mb$, 則存在 $n \in \mathbb{Z}$ 滿足 $mb = n(ma)$, 亦即 $m(b - na) = 0$. 故由 $m \neq 0$ 的假設知 $b - na = 0$. 得證 $a \mid b$. □

當我們碰到兩整數 $a,b$ 皆很大無法判別其是否有倍數關係時, 若知道 $a,b$ 有共同的因數 $d$ (即 $a = da', b = db'$，其中 $a', b' \in \mathbb{Z}$), 通常會將共同因數約去得到較小的兩個數, 為了方便起見我們用 $a/d, b/d$ 表示 (即 $a/d = a', b/d = b'$), 再判別其是否有倍數關係. 我們有以下的結果.

**Corollary 1.1.3.** 假設 $d \mid a$ 且 $d \mid b$, 則 $a \mid b$ 若且唯若 $(a/d) \mid (b/d)$.

**Proof.** 首先注意因為 $d \mid a$ 所以 $a/d$ 是整數, 同理 $b/d$ 也是整數, 因此我們才可以探討是否 $(a/d) \mid (b/d)$. 因為 $d \neq 0$, 依 Lemma 1.1.2 我們知道 $d(a/d) \mid d(b/d)$ (即 $a \mid b$) 若且唯若 $(a/d) \mid (b/d)$. 故得證本定理. □

在 Corollary 1.1.3 中 $d \mid a$ 且 $d \mid b$ 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). Corollary 1.1.3 告訴我們將兩個整數約掉其公因數仍會保持其倍數關係.

討論一些整數之間的關係時公因數和最大公因數很重要的工具. 接下來我們給它們下定義.

**Definition 1.1.4.** 令 $a,b \in \mathbb{Z}$ 且皆不等於 0.

(1) 若 $c \in \mathbb{Z}$, 且 $c \mid a, c \mid b$, 則稱 $c$ 為 $a,b$ 的 *common divisor* (公因數).

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

當要下一個定義時要注意是否合理. 不可定義的東西根本不存在或沒有用. Definition 1.1.4 中就要注意公因數以及最大公因數是否存在. 首先我們探討公因數的存在性: 因為 1 整除所有的整數, 所以若 $a,b \in \mathbb{Z}$ 則其公因數必存在 (至少 1 就是).

至於最大公因數的存在性, 就要用到整數的 "well-ordering principle" 這個性質了. 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 (即存在一個數小於等於 $S$ 中所有的數), 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 (即存在一個數大於等於 $S$ 中所有的數), 則此集合中必含有一個最大的整數 (通常用 $\max S$ 來表示). 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.

現在回到最大公因數的存在性. 因為當 $a \neq 0$ 時, $a$ 的任意因數皆小於等於 $|a|$, 故 $a,b$ 的公因數所成的集合有上界 (例如 $|a|$ 就是). 所以由 well-ordering principle 我們知 $a,b$ 的最大公因數必存在.

要注意的是 $a,b$ 的最大公因數有可能是 1. 若如此 (即 $\gcd(a,b) = 1$), 表示 $a$ 和 $b$ 除了 $\pm 1$ 外沒有其他的公因數, 我們稱 $a,b$ 互質 (*relatively prime*).

**Exercise 1.1.** 假設 $a,b,c,d \in \mathbb{Z}$ 皆不等於 0, 試證明以下有關於整除的性質.

(試著利用 Lemma 1.1.1, Lemma 1.1.2 不直接用定義證明).

(1) 若 $a \mid b$ 且 $c \mid d$, 則 $ac \mid bd$. (Lemma 1.1.2 & Lemma 1.1.1(1))

(2) 若 $a \mid b$, 則對任意 $n \in \mathbb{N}$ 皆有 $a^n \mid b^n$. (由題 (1) 以及數學歸納法)

(3) 若 $c \mid a+b$ 且 $c \mid a$, 則 $c \mid b$. (Lemma 1.1.1(2))

(4) 若 $a \mid bc-1$ 以及 $a \mid b-1$, 則 $a \mid c-1$. (由題 (3))

(5) 假設 $m,n \in \mathbb{N}$ 且 $a > 1$, 若 $a^m - 1 \mid a^{m+n} - 1$, 則 $a^m - 1 \mid a^n - 1$. (由題 (4))

**Exercise 1.2.** 假設 $a \in \mathbb{Z}$, 試證明 $3 \mid a^3 - a$.

## 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 $m, m-n, m-2n,\dots$ 以及 $m+n, m+2n,\dots$ 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.

**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 $b\neq0$ (不必假設 $b\in\mathbb{N}$).

(1) 證明存在唯一的 $h,r\in\mathbb{Z}$ 滿足

$$a=bh+r \text{ 且} 0\le r<|b|.$$

(2) 證明存在唯一的 $h,r\in\mathbb{Z}$ 滿足

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