現在我們回到探討最大公因數. 為了方便起見, 不失一般性, 我們只需討論 $a,b\in\mathbb{N}$ 的情形. 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. 而要說 d 是 a,b 是公因數裡最大的, 由 Corollary 1.2.4 我們知道就是要證明若 d' 是 a,b 的公因數, 則 $d'\mid d$. 要證明這一點, 最好的方法就是證明存在 $m,n\in\mathbb{Z}$ 使得 $d=ma+nb$ (參見 Exercise 1.5).

一般來說要找到整數 a,b 的最大公因數, 我們會嘗試先找到一個公因數 d_1, 然後再看看是否能再找到 $a_1=a/d_1, b_1=b/d_1$ 這兩個比較小的整數的公因數 d_2, 這樣一直下去直到看出 a_n,b_n 的最大公因數為止. 這樣做真的就可以得到 a,b 的最大公因數嗎? 換句話說我們必須證明, 若 $d_1\mid a$, $d_1\mid b$ 且 $d=\gcd(a/d_1,b/d_2)$, 則 $d_1d=\gcd(a,b)$. 要證明這件事, 首先我們需驗證 d_1d 確實是 a,b 的公因數. 我們有以下的性質.

Proposition 1.2.9. 假設 $a,b\in\mathbb{N}$ 且 d_1 是 a 和 b 的公因數. 若 d_2 是 a/d_1 和 b/d_1 的公因數, 則 d_1d_2 是 a 和 b 的公因數.

Proof. 首先注意, 由於 d_1 是 a,b 的公因數, 故存在 $m,n\in\mathbb{Z}$ 使得 $a=d_1m$ 且 $b=d_1n$. 也就是說 $a/d_1=m$ 和 $b/d_1=n$ 皆為整數. 又 d_2 是 m,n 的公因數故存在 $m',n'\in\mathbb{Z}$ 使得 $m=d_2m'$ 且 $n=d_2n'$. 整理得 $a=d_1d_2m'$ 且 $b=d_1d_2n'$ 故知 d_1d_2 是 a 和 b 的公因數. □

Question 1.5. 假設 $a,b,d,d'\in\mathbb{Z}$ 且 dd' 是 a 和 b 的公因數. 試證明 d 是 a 和 b 的公因數, 且 d' 是 a/d 和 b/d 的公因數.

若 Proposition 1.2.9 中剛好有 $d_1=\gcd(a,b)$, 則利用最大公因數的定義我們可得以下之性質.

Corollary 1.2.10. 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, 等同於證明存在整數 x,y 使得 $x(a/d)+y(b/d)=1$ (Corollary 1.2.5). 然而已知 $d=\gcd(a,b)$, 故存在 $m,n\in\mathbb{Z}$ 滿足 $ma+nb=d$. 因此得 $m(a/d)+n(b/d)=1$. 故令 $x=m,y=n$ 即為所求. □

接下來我們就可以證明以下性質.

Theorem 1.2.11. 假設 $a,b\in\mathbb{N}$ 且 $d_1\mid a, d_1\mid b$. 若 $d=\gcd(a/d_1,b/d_1)$, 則 $d_1d=\gcd(a,b)$.

Proof. 由 Proposition 1.2.9, 我們知 d_1d 會是 a,b 的公因數. 所以我們僅要證明存在 $x,y\in\mathbb{Z}$ 使得 $xa+yb=d_1d$, 就證明了 $d_1d=\gcd(a,b)$. 已知 $d=\gcd(a/d_1,b/d_1)$, 故存在 $m,n\in\mathbb{Z}$ 滿足 $m(a/d_1)+n(a/d_1)=d$. 兩邊同乘以 d_1, 得 $ma+nb=dd_1$. 因此若取 $x=m,y=n$, 可得 $xa+yb=d_1d$. 得證 $d_1d=\gcd(a,b)$. □

Theorem 1.2.11 告訴我們, 當兩個數很大時, 若可找到一個大於 1 的公因數, 就可以除掉這個公因數, 將問題轉換成求較小的兩個數的公因數. 不過即使兩個數不大, 使用這一節找 $\{ma+nb : m,n\in\mathbb{Z}\}$ 這個集合中最小的非負整數的方法找 a,b 的最大公因數並不是一個有效率的方法. 下一節中, 我們將介紹一個很有效地找最大公因數的方法.

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 $d=\gcd(b,r)$. 我們證明 $d=\gcd(a,b)$, 也就是說證明 d 是 a,b 的公因數且是所有 a,b 的公因數中最大的.

首先由 $d=\gcd(b,r)$ 知 $d\mid b$ 且 $d\mid r$. 故由 Corollary 1.1.1 知 $d\mid bh+r$, 得證 $d\mid a$ 且 $d\mid b$.

現若 d' 是 a,b 的公因數, 即 $d'\mid a$ 且 $d'\mid b$, 此時再由 Corollary 1.1.1 知 $d'\mid a-bh$, 即 $d'\mid r$. 也就是說 d' 也會是 b,r 的公因數. 因此由 d 是 b,r 的最大公因數, 得證 $d'\le d$. □

Question 1.6. 假設 $a,b\in\mathbb{N}$ 且 $a=bh+r$, 其中 $h,r\in\mathbb{Z}$.

(1) 是否 $\gcd(a,b)=\gcd(a,r)$?

(2) 試證明 $\{ma+nb:m,n\in\mathbb{Z}\}=\{m'b+n'r:m',n'\in\mathbb{Z}\}$.

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 $n\ge 1$, 則 $\gcd(a,b)=r_{n-1}$.

Proof. 首先注意若 $r_0\neq 0$, 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 1.2.10). 因此得 $a'(m-m_0)=b'(n_0-n)$. 利用 $b'\mid a'(m-m_0)$, $\gcd(a',b')=1$ 以及 Proposition 1.2.6(1) 得 $b'\mid m-m_0$. 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.

在數論中找整係數方程式的整數解是一個重要的課題. 這類的問題稱為解 *diophantine equation*. 我們可以利用前面的結果, 處理最簡單的一次的 diophantine equations.

Proposition 1.3.6. 假設 $a,b,c\in\mathbb{Z}$ 且 $d=\gcd(a,b)$. 考慮 *linear diophantine equation* $ax+by=c$. 我們有以下的結果.

(1) 方程式 $ax+by=c$ 有整數解若且唯若 $d\mid c$.

(2) 假設 $d\mid c$ 且 $x=m_0,y=n_0$ 是 $ax+by=d$ 的一組整數解, 則 $ax+by=d$ 的所有整數解為 $x=m_0(c/d)+(b/d)t,y=n_0(c/d)-(a/d)t$ 其中 $t\in\mathbb{Z}$.

Proof. 首先我們證明 $ax+by=c$ 有整數解若且唯若 $d\mid c$. 假設 $x=m,y=n$ 是 $ax+by=c$ 的一組整數解. 因 $d=\gcd(a,b)$, 故知 $d\mid a$ 且 $d\mid b$. 所以由 $m,n\in\mathbb{Z}$ 知 $d\mid am+bn$, 亦即 $d\mid c$. 現假設 $d\mid c$ 且令 $k=c/d$. 由於 $d=\gcd(a,b)$ 故存在 $m_0,n_0\in\mathbb{Z}$ 滿足 $am_0+bn_0=d$. 等式兩邊乘上 k, 得 $am_0k+bn_0k=dk=c$, 得證 $x=m_0k,y=n_0k$ 會是 $ax+by=c$ 的一組整數解, 亦即 $ax+by=c$ 有整數解.

接著當 $d\mid c$ 時我們要找到 $ax+by=c$ 的所有整數解. 同樣的令 $k=c/d$, 由前我們知若 $x=m_0,y=n_0$ 是 $ax+by=d$ 的一組整數解, 則 $x=m_0k,y=n_0k$ 會是 $ax+by=c$ 的一組整數解. 現假設 $x=m,y=n$ 是 $ax+by=c$ 的任一組整數解. 由於已知 $x=m_0k,y=n_0k$ 也是一組解, 故得 $am+bn=am_0k+bn_0k$. 故利用和 Proposition 1.3.5 相同的證明方法, 知存在 $t\in\mathbb{Z}$ 使得 $m=m_0k+bt/d,n=n_0k-at/d$, 亦即 $ax+by=c$ 的任一組整數解必為為 $x=m_0k+(b/d)t,y=n_0k-(a/d)t$ 其中 $t\in\mathbb{Z}$ 這樣的形式. 反之, 對任意 $t\in\mathbb{Z}$ 令 $x=m_0k+(b/d)t,y=n_0k-(a/d)t$ 可得 $ax+by=c$, 因此得證本定理. □

Example 1.3.7. 考慮兩個 diophantine equation $481x+221y=23$ 以及 $481x+221y=91$. 因 $\gcd(481,221)=13$ 故由 $13\nmid 23$ 以及 $13\mid 91$ 知 $481x+221y=23$ 無整數解, 而 $481x+221y=91$ 有整數解. 又由 Example 1.3.4 我們知 $x=6,y=-13$ 是 $481x+221y=13$ 的一組整數解, 故由 $91/13=7$ 得 $x=42+17t,y=-91-37t$ 是 $481x+221y=91$ 所有的整數解.

1.4. 最大公因數與最小公倍數

我們已經知道如何求得最大公因數, 接下來便是探討如何求得最小公倍數. 我們也會探討多個 (多於兩個) 整數的最大公因數與最小公倍數.

首先我們有以下最小公倍數的定義.

Definition 1.4.1. 令 $a,b\in\mathbb{Z}$ 且皆不等於 0.

(1) 若 $m\in\mathbb{Z}$, 且 $a\mid m, b\mid m$, 則稱 m 為 a,b 的 *common multiple* (公倍數).

(2) 若 $l\in\mathbb{N}$ 是 a,b 的正公倍數中最小的, 則稱 l 為 a,b 的 *least common multiple* (最小公倍數), 通常我們會用 $\operatorname{lcm}(a,b)$ 來表示之.

首先我們探討兩整數 a,b 的最小公倍數的性質. 若 l 是 a,b 的最小公倍數, 則由於 $\gcd(a,b)\mid l$, 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 1.4.2. 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 $l\mid m$.

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 1.2.10). 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 $a\mid(ab/d)$ 同理知 $b\mid(ab/d)$, 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 $d\neq0$) 得 $m'a'=n'b'$. 也就是說 $a'\mid n'b'$. 但由於 $\gcd(a',b')=1$, 故由 Proposition 1.2.6(1) 知 $a'\mid n'$. 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 $a'b=(ab/d)\mid m$. 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 $l=(ab/d)\mid m$. 反之, 若 $l\mid m$, 則由 $a\mid l$ 且 $b\mid l$, 得知 $a\mid m$ 且 $b\mid m$, 故 m 為 a,b 之公倍數. □

要注意雖然 Proposition 1.4.2 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 1.4.2 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 1.4.2 告訴我們公倍數為最小公倍數之倍數.

Exercise 1.8. 試利用數學歸納法證明以下性質.

(1) 若 $\gcd(a_1,a_i)=1$, $\forall i\in\{2,\dots,n\}$, 則 $\gcd(a_1,a_2\cdots a_n)=1$.

(2) 假設 $a_1,\dots,a_n$ 兩兩互質 (即對任意 $i,j\in\{1,\dots,n\}$ 且 $i\neq j$, 皆有 $\gcd(a_i,a_j)=1$) 且 $a_i\mid l$, $\forall i\in\{1,\dots,n\}$, 則 $a_1\cdots a_n\mid l$.

Exercise 1.9. 假設 $a,b\in\mathbb{Z}$ 且令 $d=\gcd(a+b,a-b)$.

(1) 試證明 $d\mid 2a$ 且 $d\mid 2b$.

(2) 若已知 $\gcd(a,b)=1$ 試證明當 a,b 同為奇數時 $d=2$; 而當 a,b 為一奇一偶時 $d=1$.

Exercise 1.10. 試利用輾轉相除法原理 (Lemma 1.3.1) 處理以下問題.

(1) 已知在 1 到 100 間共有 40 個整數和 100 互質. 試算出 (請不要用數的) 在 1 到 1000 間共有多少個整數和 100 互質.

(2) 給定 $a,d\in\mathbb{N}$, 已知共有 k 個整數 b 滿足 $0<b\leq na$, $(n\in\mathbb{N})$ 且 $\gcd(a,b)=d$. 試證明 $n\mid k$.

Exercise 1.11. 試寫出以下 diophantine equations 的所有整數解.

(1) $18x+27y=15$.

(2) $17x+29y=10$.