1.3. 輾轉相除法

Theorem 1.2.12 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. 這一節中, 我們介紹一個很有效地找最大公因數的方法“輾轉相除法”. 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 $d = \gcd(a,b)$. 利用 Proposition 1.2.9, 我們僅需證明 d 是 b,r 的公因數且 $d = xb+yr$ 存在整數解 x,y, 便可證得 $d = \gcd(b,r)$.

首先由 $d = \gcd(a,b)$ 知 $d \mid a$ 且 $d \mid b$. 故由 Corollary 1.1.1 知 $d \mid a-bh$, 得證 $d \mid r$. 因此 d 是 b,r 的公因數.

現因 d 是 a,b 的最大公因數, 故存在 $m,n \in \mathbb{Z}$ 滿足 $d = ma+nb$. 因此得 $d = m(bh+r)+nb = (mh+n)b+mr$. 故 $x = mh+n$, $y = m$ 就是 $d = xb+yr$ 的一組整數解. □

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 $13 = m481 + n221$. 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 $13 = 481m + 221n$.

Example 1.3.4 所介紹找到 $m,n \in \mathbb{Z}$ 使得 $ma + nb = \gcd(a,b)$ 的方法，有點繁瑣. 事實上，輾轉相除法的運算和矩陣（Type 3）基本列運算相似（只能乘上整數），我們可以利用其概念化簡“回推”求 m,n 的程序。簡單回顧一下（詳情請參閱『線性代數初步』講義）：當 A 為 $m \times n$ 矩陣，我們考慮增廣矩陣 $[A \mid I_m]$，若用一連串基本列運算將之化為

$[B \mid E]$，則 $EA = B$。同樣的若我們先寫下 $\left[\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right]$，然後利用輾轉相除法轉換成基本列運算形式（將除數與商的乘積乘上負號加到被除數），最後化為 $\left[\begin{array}{c|cc} d & m & n \\ 0 & * & * \end{array}\right]$，就可利用 $\begin{bmatrix} m & n \\ * & * \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$ 得知 $ma+nb=d$。我們將 Example 1.3.3 的輾轉相處法利用這個方式驗證與 Example 1.3.4 的結果一致。

Example 1.3.5. 要找到 $m,n \in \mathbb{Z}$ 使得 $13 = m481 + n221$. 首先寫下增廣矩陣 $\left[\begin{array}{c|cc} 481 & 1 & 0 \\ 221 & 0 & 1 \end{array}\right]$，接著將第二個 row 乘上 -2 加到第一個 row 得到 $\left[\begin{array}{c|cc} 39 & 1 & -2 \\ 221 & 0 & 1 \end{array}\right]$。再將第一個 row 乘上 -5 加到第二個 row 得到 $\left[\begin{array}{c|cc} 39 & 1 & -2 \\ 26 & -5 & 11 \end{array}\right]$，然後將第二個 row 乘上 -1 加到第一個 row 得到 $\left[\begin{array}{c|cc} 13 & 6 & -13 \\ 26 & -5 & 11 \end{array}\right]$。最將第一個 row 乘上 -2 加到第二個 row 得到 $\left[\begin{array}{c|cc} 13 & 6 & -13 \\ 0 & -17 & 37 \end{array}\right]$。因此由 $\begin{bmatrix} 6 & -13 \\ -17 & 37 \end{bmatrix}\begin{bmatrix} 481 \\ 221 \end{bmatrix} = \begin{bmatrix} 13 \\ 0 \end{bmatrix}$ 得知 $6\cdot 481 + (-13)\cdot 221 = 13$。

我們也可將這個矩陣列運算的程序用以下方式表示：$\left[\begin{array}{c|cc} 481 & 1 & 0 \\ 221 & 0 & 1 \\ 39 & 1 & -2 \\ 26 & -5 & 11 \\ 13 & 6 & -13 \\ 0 & -17 & 37 \end{array}\right]$.

Question 1.7. Example 1.3.5 中，請由矩陣 $\left[\begin{array}{c|cc} 13 & 6 & -13 \\ 26 & -5 & 11 \end{array}\right]$ 得到整數 $m,n \in \mathbb{Z}$ 使得 $26 = m481 + n221$。

要注意滿足 $d = ma+nb$ 的 m,n 並不會僅有唯一的一組解. 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 1.3.6. 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 1.2.11). 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 1.3.6 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.

附註：當 $a,b\in\mathbb{Z}$，使用輾轉相除法找出 $d=\gcd(a,b)$ 的過程中，若從基本列運算和 elementary matrix 的關聯，可以馬上讓我們得到 $ax+by=d$ 的所有整數解。事實上若將增廣矩陣 $\left[\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right]$ 運用輾轉相除（Type 3 基本列運算）變成 $\left[\begin{array}{c|cc} d & m & n \\ 0 & r & s \end{array}\right]$。由此式得 $\begin{bmatrix} m & n \\ r & s \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} d \\ 0 \end{bmatrix}$，亦即 $ma+nb=d$ 且 $ra+sb=0$。我們將說明：事實上 $r=-b/d$ 且 $s=a/d$，所以可由 Proposition 1.3.6，馬上寫下 $ax+by=d$ 的所有整數解為 $x=m+rt$, $y=n+st$, $t\in\mathbb{Z}$。以下論證若不了解基本列運算與 elementary matrix 可忽略，只要記下結果就好！

Proof. 因為矩陣 $\begin{bmatrix} m & n \\ r & s \end{bmatrix}$ 是由一些 type 3 elementary matrix 相乘所得，而且 type 3 的 elementary matrix 其行列式值為 1，所以 $\begin{bmatrix} m & n \\ r & s \end{bmatrix}$ 的行列式值亦為 1。因此知 $\begin{bmatrix} m & n \\ r & s \end{bmatrix}$ 的反矩陣為 $\begin{bmatrix} s & -n \\ -r & m \end{bmatrix}$。故由 $\begin{bmatrix} m & n \\ r & s \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} d \\ 0 \end{bmatrix}$ 兩邊乘上反矩陣得 $\begin{bmatrix} s & -n \\ -r & m \end{bmatrix}\begin{bmatrix} d \\ 0 \end{bmatrix}=\begin{bmatrix} a \\ b \end{bmatrix}$。乘開後得 $sd=a$ 且 $-rb=d$，亦即 $s=a/d$ 且 $r=-b/d$。 □

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 1.3.7. 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 $ax+by=c$ 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 1.3.6 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 1.3.8. 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.

Exercise 1.9. 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（請不要列出一個一個數）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 1.10. 試寫出以下 diophantine equations 的所有整數解.

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

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