漫談最大公因數

許介彥

大葉大學　通訊與計算機工程學系

某天，小明帶著兩個空桶子到河邊提水，兩個桶子上都沒有刻度，不過容量已知分別為 15 公升和 27 公升；小明想要取得不多不少正好 6 公升的河水，他該怎麼做？

歐幾里得演算法

以上所述是一個與最大公因數（greatest common divisor，簡稱 g.c.d.）有關的問題。我們在中學學過，任意兩個正整數的最大公因數可以利用「輾轉相除法」求得。舉例來說，以下所示為以輾轉相除法求出 477 與 138 的最大公因數（等於 3）的過程：

3	477	138	2
	414	126	
5	63	12	4
	60	12	
	3	0	

其中的各個階段可以用數學式來表示：

$$\begin{aligned} 477 &= 3 \cdot 138 + 63 \\ 138 &= 2 \cdot 63 + 12 \\ 63 &= 5 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

或者再換個方式：

階段	被除數	除數	餘數	商
1	477	138	63	3
2	138	63	12	2
3	63	12	3	5
4	12	3	0	4

由上表很明顯可以看出，除了第一個階段外，其他各階段的被除數與除數分別是來自前一個階段的除數與餘數，而當某個階段的餘數為 0 時整個計算即告結束，而且該階段的除數就是原來的兩數的最大公因數。為什麼會這樣呢？

對任意正整數 a 與 b，如果我們將 a 除以 b 的商及餘數分別記作 q 及 r（餘數 r 的值須滿足 $0 \le r < b$），也就是

$$a = q \cdot b + r$$

那麼不難証明，a 與 b 的最大公因數會等於 b 與 r 的最大公因數。要証明這個性質可依下列三個步驟來完成：

1. 說明 a 與 b 的公因數必是 r 的因數。
2. 說明 b 與 r 的公因數必是 a 的因數。
3. 由以上 1 與 2 可知 a 與 b 所有的公因數和 b 與 r 所有的公因數相同，因此 a 與 b 和 b 與 r 有相同的「最大」公因數。

以前面的例子為例，如果我們將 a 與 b 的最大公因數記作 $\gcd(a,b)$，那麼前面的運算過程其實是持續地在簡化用來求最大公因數的兩個整數：

$$\begin{aligned} \gcd(477,138) &= \gcd(138,63) \\ &= \gcd(63,12) \\ &= \gcd(12,3) \\ &= 3 \end{aligned}$$

一般而言，對任意正整數 a 與 b，我們可以將輾轉相除法的各個階段以數學式子表示：

$$\begin{aligned} a &= q_1 \cdot b + r_1 && (0 < r_1 < b) \\ b &= q_2 \cdot r_1 + r_2 && (0 < r_2 < r_1) \\ r_1 &= q_3 \cdot r_2 + r_3 && (0 < r_3 < r_2) \\ r_2 &= q_4 \cdot r_3 + r_4 && (0 < r_4 < r_3) \\ &\vdots \end{aligned}$$

並且讓計算一直持續到餘數為 0 為止。經由審視各階段的餘數間的大小關係，我們發覺必然會在某個階段出現餘數為 0 的情形，因為除了最後一個階段以外，各階段的餘數都是正數而且越來越小：

$$b > r_1 > r_2 > r_3 > r_4 > \cdots > 0$$

因此頂多經過 b 個階段，必定會出現餘數為 0 的情形：

$$\begin{aligned} &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \quad (0 < r_n < r_{n-1}) \\ r_{n-1} &= q_{n+1} \cdot r_n \end{aligned}$$

這時候我們就知道 a 與 b 的最大公因數等於 r_n，也就是當餘數為 0 時的除數，亦即這一系列計算中的最後一個大於 0 的餘數，因為

$$\begin{aligned} \gcd(a,b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &= \cdots \\ &= \gcd(r_{n-1}, r_n) \\ &= r_n \end{aligned}$$

上述做法一般認為是由西元前三世紀的希臘大數學家歐幾里得（Euclid）發明的，因此常被稱為歐幾里得演算法（Euclidean algorithm），其運算步驟可以簡潔地表達成以下的遞迴演算法：

```
GCD( a, b)
   if b = 0
      return a
   else
      return GCD( b, a mod b)
```

其中的 **mod** 是取餘數的運算，a **mod** b 的結果為 a 除以 b 的餘數。

歐幾里得演算法的應用

(一)將 a/b 表為連分數

歐幾里得演算法可以用來將兩個正整數相除的結果表示成連分數（continued fractions），也就是形如

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

的分數，其中除了 a_0 之外，所有的 a_n 都是正整數。以我們前面看過的求 gcd(477,138) 的例子為例，$477/138$ 的值很容易可以被表示成連分數：

$$\frac{477}{138} = 3 + \frac{63}{138} = 3 + \cfrac{1}{\cfrac{138}{63}}$$

$$= 3 + \cfrac{1}{2 + \cfrac{12}{63}} = 3 + \cfrac{1}{2 + \cfrac{1}{\cfrac{63}{12}}}$$

$$= 3 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{3}{12}}} = 3 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{\cfrac{12}{3}}}}$$

$$= 3 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{4}}}$$

很明顯，最後結果的整數部份 a_0、a_1、a_2、a_3、…（此例中的 3、2、5、4）正好是歐幾里得演算法的計算過程中各階段的商。

連分數的用途之一是用來做為兩數相除結果的近似值。以 477 /138 （分子與分母約掉公因數 3 後成為 159 / 46）為例，在以上將其表為連分數的過程中，如果我們在各階段將還沒算完的部分捨棄，可分別得到一個 159 / 46 的「近似值」：

階段	近似值
1	3
2	$3 + \frac{1}{2} = \frac{7}{2}$
3	$3 + \cfrac{1}{2 + \cfrac{1}{5}} = \frac{38}{11}$
4	$3 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{4}}} = \frac{159}{46}$

其中，

$$3 < \frac{159}{46}$$
$$\frac{7}{2} > \frac{159}{46}$$
$$\frac{38}{11} < \frac{159}{46}$$
$$\frac{159}{46} = \frac{159}{46}$$

一般而言，第一個階段的近似值會比實際值小，第二個階段的近似值會比實際值大，第三個階段的近似值又較小，第四個階段的近似值又較大……，與實際值相比，大小關係是交替的，所有奇數階段都比實際值小，偶數階段都比實際值大，直到最後一個階段才與實際值相等。因此，以 159 / 46 為例，如果我們想要取一個比實際值稍大且數字較簡單的值來做為近似值，可以取 7 / 2（誤差約為 1.3%），而如果想要取一個比實際值小的近似值，可以取 38/11 （誤差約為 0.057%）。

(二)求 $ax + by = c$ 的整數解

歐幾里得演算法的另一個應用是可以求得形如 $ax + by = c$ 的方程式的整數解，其中的 a、b、c 都是已知的正整數而 x 與 y 為未知整數；這種方程式在數學上稱為 linear Diophantine equation（Diophantus 為西元三世紀的希臘數學家，一般譯為丟番圖）；當它有解時，必有無窮多組解，不過也可能沒有任何整數解。

在說明如何求解之前，讓我們先看一個相關的性質：如果 $d = \gcd(a, b)$，那麼方程式 $ax + by = d$ 必定存在整數解，也就是說，d 必可表示成 a 與 b 的線性組合（linear combination）。歐幾里得演算法可以幫助我們很容易地找到 $ax + by = d$ 的一組解；而有了一組解後，再找其他解就不難了。

用前面看過的 $3 = \gcd(477,138)$ 為例，上面的性質是說 $477x + 138y = 3$ 一定有整數解。我們在前面曾經將求 477 與 138 的最大公因數的各個階段以數學式表示；如果我們將各式的餘數寫在等號左邊，其他項移到等號右邊，將得

$$63 = 477 - 3 \cdot 138$$
$$12 = 138 - 2 \cdot 63$$
$$3 = 63 - 5 \cdot 12$$

前面提過，歐幾里得演算法的計算過程是在將數字持續簡化，而我們現在要做的工作則是相反，是要由最大公因數 3 開始「反推」回去，讓數字由簡單而複雜，直到能將 3 用最初的 477 與 138 表示為止：

$$\begin{aligned}3&=63-5\cdot12\\&=63-5\cdot(138-2\cdot63)\\&=11\cdot63-5\cdot138\\&=11\cdot(477-3\cdot138)-5\cdot138\\&=11\cdot477-38\cdot138\end{aligned}$$

因此我們找到了方程式 $477x+138y=3$ 的一組整數解：$x_0=11$ 及 $y_0=-38$，或者寫為 $(x_0,y_0)=(11,-38)$。

其他的整數解要怎麼求呢？假設 (x_1,y_1) 是任意另外一組解，由

$$\begin{cases}ax_1+by_1=d\\ax_0+by_0=d\end{cases}$$

兩式相減，得

$$a(x_1-x_0)+b(y_1-y_0)=0$$

因此 (x_1-x_0,y_1-y_0) 必為 $ax+by=0$ 的解；又由於方程式 $ax+by=0$ 的解必可寫為

$$x=\frac{b}{d}n,\quad y=\frac{-a}{d}n$$

（n 為任意整數），因此我們可以讓

$$x_1-x_0=\frac{b}{d}n,\quad y_1-y_0=\frac{-a}{d}n$$

而得

$$x_1=x_0+\frac{b}{d}n,\quad y_1=y_0-\frac{a}{d}n$$

因此方程式 $ax+by=d$ 的一般解為

$$x=x_0+\frac{b}{d}n,\quad y=y_0-\frac{a}{d}n$$

方程式 $477x+138y=3$ 的一般解因此為 $(x,y)=(11+46n,-38-159n)$。

接著我們回到原來的方程式 $ax+by=c$。假設 $d=\gcd(a,b)$，由於 $ax+by$ 一定是 d 的倍數，因此 c 一定也是 d 的倍數，否則 $ax+by=c$ 不可能有整數解。另一方面，是不是只要 c 是 d 的倍數，$ax+by=c$ 就一定有整數解呢？答案是肯定的，因為如果 (x_0,y_0) 是 $ax+by=d$ 的一組解，而且 c 是 d 的 m 倍（$c=md$），則

$$\begin{aligned}&ax_0+by_0=d\\\Rightarrow\ &a(mx_0)+b(my_0)=c\\\Rightarrow\ &(mx_0,my_0)\text{ 是 }ax+by=c\text{ 的一組解}\end{aligned}$$

因此，我們有了以下的結論：$ax+by=c$ 有整數解「若且唯若」c 是 d 的整數倍。如果 c 是 d 的 m 倍且 (x_0,y_0) 是 $ax+by=d$ 的一組解，那麼 $ax+by=c$ 的一般解為

$$x=mx_0+\frac{b}{d}n,\quad y=my_0-\frac{a}{d}n$$

舉例來說，$477x+138y=9$ 的一般解為 $(x,y)=(33+46n,-114-159n)$。

歐幾里得演算法的擴充

由已知的 a 與 b 想求得方程式 $ax+by=d$（d 等於 $\gcd(a,b)$）的一組解，除了前述分為兩個階段（先由歐幾里得演算法求出 d，再由 d 反推回 a 與 b）的方法外，其實只要將歐幾里得演算法稍作修改，我們不難讓求最大公因數與求解可以同時進行，使得在求出最大公因數的同時也求得了 $ax+by=d$ 的一組解。

一開始，我們先寫下如下兩個恆等式：

$$a = 1 \cdot a + 0 \cdot b$$
$$b = 0 \cdot a + 1 \cdot b$$

也就是將 a 和 b 分別用 a 與 b 表示，接著就如同一般歐幾里得演算法的步驟，設法經由兩式之間的算術運算使得等號左邊成為 a 與 b 的最大公因數；由於運算過程的每個階段等號左邊的數都被表示成 a 與 b 的線性組合，因此當等號左邊為 a 與 b 的最大公因數時，自然就有了 $d = ax + by$ 的一組解。

舉例來說，假設 $a = 477$，$b = 138$，我們用下面兩個式子為起點：

$$477 = 1 \cdot 477 + 0 \cdot 138 \quad (1)$$
$$138 = 0 \cdot 477 + 1 \cdot 138 \quad (2)$$

由 $(1) - 3 \times (2)$ 得

$$63 = 1 \cdot 477 - 3 \cdot 138 \quad (3)$$

由 $(2) - 2 \times (3)$ 得

$$12 = -2 \cdot 477 + 7 \cdot 138 \quad (4)$$

由 $(3) - 5 \times (4)$ 得

$$3 = 11 \cdot 477 - 38 \cdot 138 \quad (5)$$

等號左邊的 3 很明顯是 12 的因數，因此 $\gcd(477,138) = 3$，此時由(5)式的等號右邊可知 $(x, y) = (11, -38)$ 為方程式 $477x + 138y = 3$ 的一組解。

一個簡單的遊戲

以下是一個與最大公因數有關的遊戲，在教室裡很容易就可以進行。首先，老師先在黑板上寫下兩個正整數，然後請兩位同學上台，輪流在黑板上寫下更多數字。每位同學每次所寫的數必須是當時黑板上的某兩個數的差（大數減去小數），而且不能與黑板上已有的數重覆。此遊戲一直持續到有一方無法寫出新數為止，此人就是遊戲的輸家。

如果某位參賽者有權決定遊戲是由自己或對方開始的話，他其實一定可以贏得這場遊戲；在往下看之前，請讀者想一想，他的致勝之道是什麼？

假設最初由老師提供的兩數為 a 與 b 且 a 大於 b，讀者不難看出，參賽的同學所寫下的每個數一定都是 $\gcd(a,b)$ 的倍數，而且隨著遊戲的進行，所有小於 a 的 $\gcd(a,b)$ 的倍數都能陸續出現在黑板上。因此，當 a 與 b 的值確定後，參賽的兩方總共會在黑板上寫下多少個數其實就已經確定了，總共有

$$\frac{a}{\gcd(a,b)} - 2$$

個數。因此如果某位參賽者有權決定遊戲是由自己或對方開始的話，整場遊戲的輸贏當然已經在他的掌握之中。

結語

對任意正整數 a 與 b 而言，由於所有可以表示成 $ax + by$ 的正整數一定是 $\gcd(a,b)$ 的倍數，因此 $\gcd(a,b)$ 其實是可以表示成形如 $ax + by$ 的所有正整數中最小的整數，這可以看成是最大公因數的另一個定義。

最後我們來看這篇文章一開始小明所面臨的問題。經由河水在桶子間的倒進倒出，小明希望能剩下不多不少正好 6 公升的河水；這個問題相當於在求 $15x + 27y = 6$ 的整數解。由於 $\gcd(15,27) = 3$ 而 6 是 3 的倍數，因此我們可以肯定此問題有解。首先由歐幾里得演算法求出最大公因數：

$$27 = 1 \cdot 15 + 12$$
$$15 = 1 \cdot 12 + 3$$
$$3 = 4 \cdot 12$$

再由最大公因數 3 反推回去：

$$\begin{aligned} 3 &= 15 - 12 \\ &= 15 - (27 - 15) \\ &= 2 \cdot 15 - 27 \end{aligned}$$

我們得到 $15x + 27y = 3$ 的一組解 $(x, y) = (2, -1)$，因此 $15x + 27y = 3$ 的一般解為

$$(x, y) = (2 + 9n, -1 - 5n)$$

而 $15x + 27y = 6$ 的一般解為

$$(x, y) = (4 + 9n, -2 - 5n)$$

所以，小明有無窮多種做法來解決他所面臨的問題。以 $(x, y) = (4, -2)$ 為例，他可以這麼做：將容量為 15 公升的桶子裝滿河水 4 次，每當裝滿了就往容量為 27 公升的桶子裡倒，而每當容量 27 公升的桶子滿了就將桶中的河水倒回河中；在大桶子第二次倒滿時，小桶子中的河水將不多不少正好是 6 公升。

練習題

以下是幾個和本文相關的問題，提供讀者參考：

1. 某人用 1000 元買了 100 隻雞。已知雞分成三種，公雞每隻 50 元，母雞每隻 30 元，而小雞每三隻才 10 元。請問此人總共買了公雞、母雞、小雞各幾隻？（請列出所有可能的組合）
2. 小明和小華都剛找到工作，今天是他們上班的第一天。小明每上班三天就會休息一天，小華每上班七天就會休息三天。在未來的 1000 天中，有多少天他們兩人同時都不上班？
3. 對任意兩個正整數 a 與 b 而言，如果 $ax + by = 2$ 有整數解，是否 $ax^2 + by^2 = 2$ 也一定有整數解？
4. 在所有小於 2002 的正整數中，會使得 $(n^2 + 7)/(n + 4)$ 不是最簡分數的正整數 n 有幾個？

參考資料

1. 許介彥（2001），遞迴演算法簡介，科學教育月刊，第 245 期。
2. Donald E. Knuth, *The Art of Computer Programming*, Vol. 1, 3rd edition, Addison-Wesley, 1997.
3. Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, 4th edition, McGraw-Hill, 1999.

作者信箱：chsu@mail.dyu.edu.tw