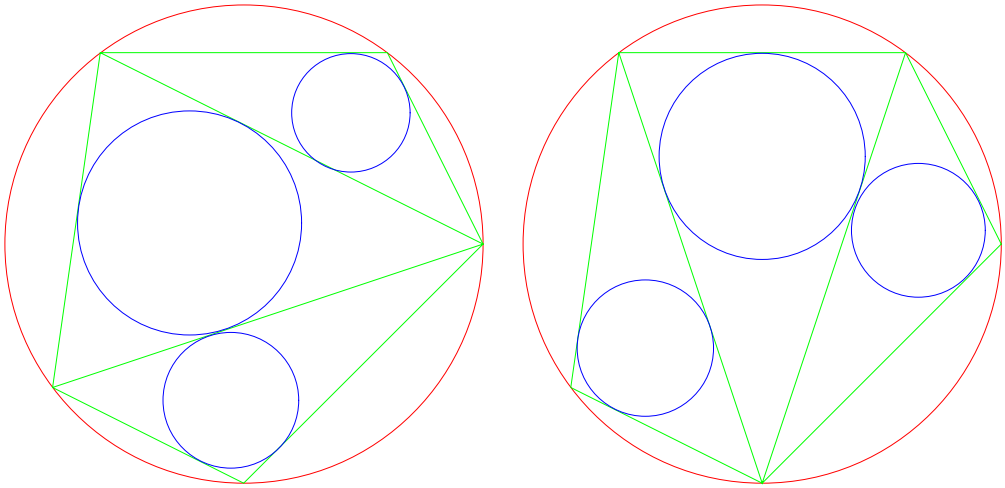
算術講義

許 志 農

國立台灣師範大學數學系

December 26, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

目 錄

1 歐基里得輾轉相除法

如果我們將一則數學問題的證明或解答中的邏輯推理及語文給剔除，所剩下的部份不是數學公式就是數學演算法。所謂數學公式是指所要求的值可以用一個公式給表達出來，例如三角形的面積公式、一元二次方程式的根的公式解、餘弦定理、正弦定理等。但並不是所有所要求的值都可以用一個公式給表示出來，例如求最大公因數就不能用一個公式來表示，而只能根據歐基里得輾轉相除法的過程來求兩數的最大公因數（或者將兩數個別作因數分解，求它們最大的共同因數）。像這樣的方法就叫做數學演算法。另兩個耳熟能詳的數學演算法就是判別一個正整數是否為質數的方法及第 ?? 節的一次因式檢驗法。我們習慣稱前種方法為埃拉托塞尼篩法（一種篩選質數的方法）。因為演算法是比數學公式較有深度的數學方法，所以歐基里得的輾轉相除法與埃拉托塞尼篩法是歷史上很早且很有名的兩則數學演算法。本節的目的就是要介紹歐基里得的輾轉相除法。

1.1 輾轉相除法求最大公因數

設 a,b 為整數，用符號 (a,b) 代表 a 與 b 的最大公因數。因為最大公因數 (a,b) 不能用一個數學公式來表示，所以我們需要尋找一種有效而且快速的方法來求最大公因數。歐基里得是第一位給最大公因數演算法的數學家，他的方法就是現今有名的歐基里得輾轉相除法。

定理 **1.1** **(**歐基里得算法**)** 設 m 為整數，n 為正整數。若 n 除以 m 所得的商及餘數分別為 q 與 r；即

$$m = nq + r, \quad 0 \le r < n,$$

則 $(m,n) = (n,r)$。

【証明】設 $d = (m,n), h = (n,r)$ 則因為

$$\begin{aligned} d \mid m, d \mid n \quad &\Rightarrow d \mid m - nq \Rightarrow d \mid r, d \mid n \Rightarrow d \mid h, \\ h \mid n, h \mid r \quad &\Rightarrow h \mid nq + r \Rightarrow h \mid m, h \mid n \Rightarrow h \mid d, \end{aligned}$$

所以 $d = h$。 ⊠

例題 **1.1** 試求 $(851, 299)$ 的值，並找一組整數 x, y 使得

$$851x + 299y = (851, 299).$$

【解】因為

$$\begin{aligned} 851 &= 299 \cdot 2 + 253 \\ 299 &= 253 \cdot 1 + 46 \\ 253 &= 46 \cdot 5 + 23 \\ 46 &= 23 \cdot 2 + 0, \end{aligned}$$

所以 $(851,299)=(299,253)=(253,46)=(46,23)=(23,0)=23$。如果將上式的前三式反代回去，則我們可以得到

$$\begin{aligned}23 &= 253-46\cdot 5 = 253-(299-253)\cdot 5 = 253\cdot 6-299\cdot 5\\ &= (851-299\cdot 2)\cdot 6-299\cdot 5 = 851\cdot 6-299\cdot 17.\end{aligned}$$

因此 $x=6, y=-17$ 為所要的一組整數解。 ⊠

1.2 二元一次不定方程式的整數解

由前節的例題可以得到底下的定理。

定理 **1.2** (二元一次不定方程式的整數解通解) 設 m,n 是互質的整數，則可以找到整數 x_0, y_0 滿足

$$mx_0+ny_0=1.$$

而且二元一次不定方程式 $mx+ny=1$ 的整數解通解為

$$\begin{cases}x=x_0+nt,\\ y=y_0-mt,\end{cases}$$

其中 t 為整數。

【証明】關於整數 x_0, y_0 的存在性：由輾轉相除法所得的式子反代回去可以得到。至於通解部分，令整數 x, y 滿足方程式 $mx+ny=1$ 則

$$mx+ny=1=mx_0+ny_0.$$

因此 $m(x-x_0)=n(y_0-y)$。由整數 m,n 互質可知

$$\begin{cases}x=x_0+nt,\\ y=y_0-mt,\end{cases}$$

其中 t 為整數。 ⊠

例題 **1.2** 試求 $23x+4y=1$ 的整數解 x 與 y。

【解】因為

$$\begin{aligned}23 &= 4\cdot 5+3,\\ 4 &= 3\cdot 1+1,\\ 3 &= 1\cdot 3+0,\end{aligned}$$

所以反代回去可以得到

$$1=4-3\cdot 1=4-(23-4\cdot 5)\cdot 1=23\cdot(-1)+4\cdot 6.$$

由上定理可以得到 $23x+4y=1$ 的整數解為

$$\begin{cases}x=-1+4t,\\ y=6-23t,\end{cases}$$

其中 t 為整數。 ⊠

習題 **1.1** 試求 $(299, 481) =?$ 並求二元一次不定方程式

$$299x + 481y = (299, 481)$$

的整數解。

習題 **1.2** 設 n 為正整數且 $233 \cdot n$ 被 377 除之，餘數為 1。試問 n 的最小值為何？

習題 **1.3** 第 n 個費馬數定義為 $F_n = 2^{2^n} + 1$。若正整數 m 與 n 不相同，則證明 F_m 與 F_n 互質。

習題 **1.4** 設 m, n 為正整數，試求最大公因數

$$(2^m - 1, 2^n - 1) = \ ?$$

並證明之。

習題 **1.5** 設整數 a，正整數 n 及質數 p 滿足

$$a^n \equiv 1 \pmod{p}.$$

若正整數 d 是滿足 $a^d \equiv 1 \pmod{p}$ 的最小正整數，則證明

$$d | n.$$

習題 **1.6** 設 a, b 為互質的正整數，並考慮方程式 $ax + by = n$。

(1) 若 n 為大於 $ab - a - b$ 的正整數，則可以找到非負整數解 x, y。

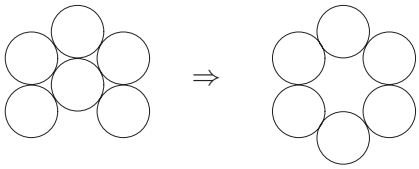
(2) 若 $n = ab - a - b$，則沒有非負整數解 x, y。[1]

(3) 某郵局僅剩 m 元及 n 元兩種郵票，其中 m 與 n 互質。試問該郵局所無法提供的整數郵資之最大值是多少？並說明之。

動手玩數學

準備七枚十元硬幣，先將一枚放在桌子上，然後將其餘的六枚放在此枚的四周（不可以重疊），這六枚的中心剛好構成一個正六邊形，再將六枚中的任意一枚拿掉。這時桌上只剩下六枚硬幣，每次操作只能在桌子上滑動六枚硬幣中的一枚，使其與至少兩枚硬幣相外切，而且滑動過程不能動到其餘的五枚硬幣。你是否有辦法在有限次的滑動之後，使這六枚硬幣的中心剛好構成一個正六邊形（如果可以的話，至少需多少次操作才能完成）。

[1] 若 $n \in \{0, 1, 2, \cdots, ab - a - b\}$，則讓 $ax + by = n$ 有非負整數解的 n 共有多少個。這是一個可以研究清楚的問題。



挑戰題

“蹴鞠”是唐宋時代一種類似今日足球的運動，在宮廷裡很是盛行（宋徽宗是當時的蹴鞠高手）。當時規定，踢進一球得 a 分；罰進一球得 b 分（那時 $a > b$）。從出土的成績紀錄表上發現：2 分及 13 分從來沒有出現過；而且 14 分至 100 分皆曾出現過。你是否可以據此推得：當時的蹴鞠運動，踢進一球及罰進一球的分數是多少呢？

歐基里得

希臘數學家，生於西元前 350 年，曾任教於亞力山大學院，是歐基里得幾何原本的作者，著作共有十三冊。輾轉相除法出現在第七冊；第四冊則有著名的“質數有無窮多個”的證明。

給定正整數 a 與 b，歐基里得輾轉相除法告訴我們，在有限且規律的步驟裡，可以算出它們的最大公因數。一則很自然的問題便發生了，到底需要多少步驟呢？已經知道的結果有

(1) 拉梅的結果：所需的步驟數小於或等於

$$5 \times \min\{a \text{ 的位數}, b \text{ 的位數}\},$$

這裡的符號 $\min\{x, y\}$ 代表 x 與 y 的較小值。

(2) 在 1970 年，狄克遜進一步證明 [2]：所需的步驟數小於或等於

$$2.078 \times \{1 + \log(\max\{a, b\})\},$$

這裡的符號 $\max\{x, y\}$ 代表 x 與 y 的較大值。

[2] 參考 Journal of Number Theory 2 (1970), pp. 414-422.