密碼學…電子時代的新顯學

知己知彼，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。

許志農／臺灣師大數學系

從人類學會溝通後，便不斷尋找更為巧妙複雜的方式來隱藏訊息，以防敵人識破。例如：古代中國會用明礬水寫保密書信；義大利人則發現用明礬調配出來的墨水，可以滲透蛋殼，在裡面的熟蛋白留下痕跡，但是從蛋殼外表卻看不出來；甚至遠在波斯王朝時，剃光信差的頭髮，將訊息刺在信差的光頭上，等頭髮長出來了，就派他去傳遞秘密訊息。事實上，語言與文字就是最早的秘語與暗碼，使用不同語言或文字的兩個人是很難溝通的，除非比手劃腳。在比賽場上，特別是雙打，要溝通時，經常發現隊友會用手遮住嘴巴講話，用意是怕被對方識破，但若知道對手不懂我隊的語言，遮住嘴巴的動作就可以免了。上述這些隱匿法都是古代傳遞秘密訊息的方法，算是密碼學的早期雛形，而密碼學的歷史就是幾世紀以來編碼者與解碼者之間的戰爭史。

古代也會在文字上做文章，大搞隱藏訊息手法，例如破譯「青鵝」兩字的故事是說「唐朝時，武則天稱帝，地方官員徐敬業準備起兵造反，中書令裴炎給徐敬業等人寫了一封書信，只有『青鵝』兩個字，被人告發了，朝中大臣誰都不知道這是什麼意思。武則天說：『青』字可以拆成『十二月』，『鵝』字可以拆成『我自與』，這說的是『十二月我自與』。馬上殺掉了裴炎，徐敬業等人的造反也很快失敗了」。凱撒在高盧戰爭期間使用凱撒移位法與將領們通訊，他們的作法是把每個字母順移同樣的數目，例如：順移的數目為 3，a 就變成 d ，b 就變成 e 。有時候還採取比較複雜的調換字母順序來作為隱藏訊息的方法。當我們無法得知這調換順序時，就很難破解密碼。因此在一段很長的時期內，這種隱藏訊息的方法是很管用的，直到伊斯蘭先知穆罕默德的可蘭經出現，解密的工作才出現大幅度的進步。事情是這樣的，伊斯蘭神學家仔細計算可蘭經各個單字在每一篇啟示出現的頻率，發現這頻率有很高的穩定性。這項看似無關緊要的觀察結果，日後卻造成了密碼分析學的第一次大突破。

我們無法確知是誰先意識到字母出現頻率的差異可以用來破解密碼，就目前所知，這項技術的說明最早見於西元 9 世紀的科學家津帝：「倘若我們知道加密訊息所使用的語言，有一種破解它的方法是：找出一篇至少一頁長的相同語言的明文文章，數算每個字母的出現次數。把最常出現的字母稱為『1 號』，次常出現的字母稱為『2 號』，再次常出現的字母稱為『3 號』，以此類推，直到這篇明文樣本的所有字母都如此整理完畢。接下來，就輪到我們要解密的密碼文了，我們也將它的符號如此分類。找到最常出現的符號後，將它替換成明文範本的『1 號』字母，次常出現的符號換成『2 號』字母，再次常出現的符號依例換成『3 號』字母，以此類推，直到密碼文的所有符號都替換完畢為止」。

津帝的說明，以英文字母為例比較容易解釋。首先，為了確立每個英文字母的出現頻率，我們必須分析一篇或甚至數篇普通的英文文章。英文字母出現頻率最高的是 e ，接下來是 t ，然

後是 a ，……。再來，檢視我們要處理的密碼文件，也把每個字母出現的頻率整理出來。假設密碼文件內出現頻率最高的字母是 j ，那麼它很可能是 e 的替身；如果密碼文件內出現頻率次高的字母是 p ，那它可能就是 t 的替身，於此類推。這樣我們就可以破解密碼文件了。

很長一段時間，非洲下撒哈拉區使用鼓聲來傳遞資訊，鼓聲、號角和鐘聲一樣，有時能用來示意，傳遞簡單的訊息，例如：進攻、撤退和上教堂，但是我們無法想像鼓聲會說話，而且是非洲人利用鼓聲來傳遞資訊。非洲會說話的鼓就像華騷所勾勒的「鼓聲隆隆不息，響徹黑暗大陸，……，會說話的鼓，是莽林的無線電」。

高斯是第一位實驗電磁脈衝通訊的人，他架設了一條長一公里的電線，由位於哥廷根的韋伯實驗室連接到高斯居住的天文臺，用來互相傳遞訊息，這也開啟了電磁密碼的時代，直到 1838 年，美國人摩斯開發的電磁密碼最為成功，這套密碼和高斯及韋伯的密碼很像，只是把每個字母轉換為長短電波的組合。摩斯密碼擁有精簡、低成本與高效率的優點，所以在通訊科技昌明的今天，它仍然占有相當重要的地位。摩斯密碼的組成相當簡單，它是由點「・」（短音）與線段「－」（長音）所組成的，例如：數字 0、1、3、5，英文字母 Q 與運算符號 +、×的摩斯電碼分別為

0 － － － － －
1 ・ － － － －
3 ・ ・ ・ － －
5 ・ ・ ・ ・ ・
Q － － ・ －
+ ・ － ・ － ・
× － ・ ・ －

電報與密碼的長期發展，促使人們對個人隱私的重視，例如：英國維多利亞時期的年輕情侶無法公然表達他們的愛意，甚至不能透過信函，因為他們的父母可能會攔截、閱讀信件內容。因此，有些情侶就透過報紙的個人啟事區傳送加密的訊息給對方。這些俗稱的「相思專欄」勾起解密專家的好奇心。有一次惠斯頓解譯了一名牛津學生刊在《泰晤士報》提議愛人與他一起私奔的啟示。幾天後，惠斯頓刊登他自己的啟事，也用同樣的密碼加密，勸告這對愛侶不要履行這項輕率、叛逆的計畫。稍後隨即出現第三則啟事，這次沒有加密，它是女方當事人發出的：「親愛的惠斯頓，不要再寫了。我們的密碼被發現了」。

每一本現代的書都有國際標準書碼（或稱 ISBN 碼），國際標準書碼一共有十碼，前九碼是 9 個數字，稱為「訊息碼」；第十碼可能是數字或是 × 這個記號，稱為「檢查碼」。檢查碼是由訊息碼所決定的，將訊息碼的每個數字依序分別乘上 1、2、3、……、9，再將其總和除以 11，當所得的餘數是 10 時，規定檢查碼為 ×，餘數不為 10 時，就以此餘數當檢查碼。例如《阿草的葫蘆》這本書的訊息碼為 957-990-882，又

$$1\times 9+2\times 5+3\times 7+4\times 9+5\times 9+6\times 0+7\times 8+8\times 8+9\times 2=259$$

除以 11 所得的餘數為 6，故檢查碼為 6，此書完整的 ISBN 碼為 957-990-882-6，如下圖的標籤所示：

婷婷從電腦上查得《幾何原本十三卷》這本書的 ISBN 碼，並用噴墨印表機將它印下。由於不小心觸摸，使得其中的第三碼數字模糊了，但是其他的數字還很清楚，書碼如下所示：

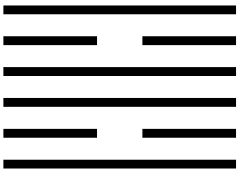
ISBN：04■-620-112-0

你能推得該書碼的第三碼應該是多少嗎？這是辦得到的，國際標準書碼具有神奇的功能：它會自我偵錯，而這偵錯的道理來自於 11 倍數的算術使用，算算看模糊的數字應該是多少。

由於書籍出版量龐大，ISBN 開始面臨無碼可用的局面，因此 2007 年 1 月 1 日起，ISBN 改為 13 碼，並將第 2、4、6、8、10 和 12 個數字相加後乘以 3，再加上第 1、3、5、7、9 和 11 個數字，最後選定第 13 個檢查碼，讓其總和為 10 的倍數，例如下圖所示：

就是一本書的國際標準書碼。

萊布尼茲發明了二進制，只用數字 0 和 1 表示數。當年他與在清朝的傳教士來往，世上至今仍然留有那時他們的書信。歷史記載，萊布尼茲在德國見過邵雍的方圓圖，他曾經用放大鏡仔細觀察八卦，發現八卦是由陽爻（實線）和陰爻（中斷的線）兩種符號組成。萊布尼茲的天才在於，他以數解卦。這個方法開闢了溝通算術與易經的道路。按照他的觀點，所謂陰陽可以數字化，陽爻用數字 1 表示，陰爻用數字 0 表示。這樣每個卦都成了由 0 和 1 構成的六位數。特別的，他認為採用二進制來計算是最簡單的，例如：下圖是《易經》六十四卦中的第三十卦（離為火），由下往上讀可以得到二進位表示的 101101：

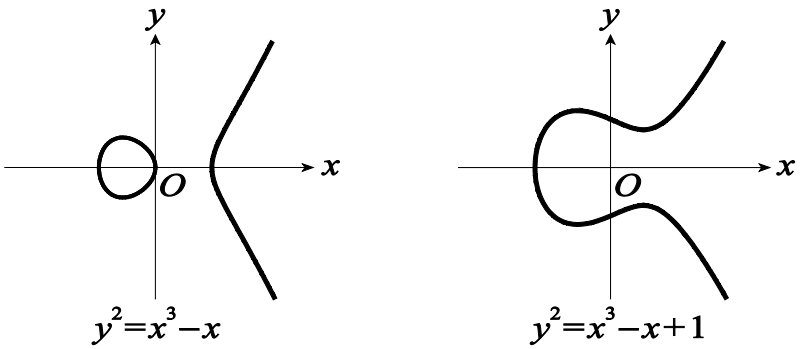


無論訊息加密與否，都需要找出由一地傳遞至另一地的方法。中國長城上的狼煙，水手使用的旗號系統，輪船打出的燈光訊號，一般書信傳遞，這些都是為了將訊息傳遞出去所想到的方法。身處 21 世紀的今日，網際網路無遠弗屆，幾乎取代一切傳遞訊息的方法。

來趟時空旅行，無論是回到過去，或者前往未來，總是令人嚮往與期待，如此我們就可以改變歷史或者讓預測未來變成簡單。在時空旅行尚未成熟之前，人類一直利用數學在偷窺未來，也利用數學在探知過去。既然偷窺，探知與揭開秘密的衝動是人類的天性，所以把重要的資料與訊息加密，不被盜取變為相當重要。所謂道高一尺魔高一丈，以其人之道，還治其人之身，我們也只能利用數學來防堵與加密，進行反制。維多利亞時代的密碼分析大師巴貝吉指出「解密技術最特別的一點，在於每個人都深信自己能設計出一套無人能解的暗碼，就連略懂皮毛的人也不例外。我還觀察到，愈聰明的人愈相信這一點」。

不管訊息如何加密，最終還是得把解密鑰匙送至對方，對方才能正確解讀訊息，運送解密鑰匙的過程出了差錯，再好的加密技術也沒用。如何不必運送解密鑰匙成為密碼學的一大難題，解決的方法是這樣的：「愛麗絲將一則極私密的訊息，加密之後送給巴伯，此時巴伯沒有解開它的密碼，但沒有關係，巴伯再將這訊息加第二道密碼，然後送還給愛麗絲，愛麗絲收到這加了兩道密碼的訊息之後，將第一道她所設的密碼解開，僅留下第二道密碼，然後再將訊息寄給巴伯，此時巴伯就可以解開他所設的第二道密碼，進而得知愛麗絲的私密訊息內容為何了」。在整個傳遞過程中，即使私密訊息被攔截，也無法解開訊息，這是近代密碼學加密而不必傳遞解密鑰匙的基本原理，妙不可言吧！

過去的密碼學需要大家先面對面協商，用於網路交易是行不通的，幸好數學提供了解決的辦法。利用大質數、費馬小定理及橢圓曲線（非高中的橢圓）是近年來有效傳遞密碼的方法。



有人說，首度運用芥子氣與氯氣的第一次世界大戰，可稱之為化學家的戰爭，以原子彈結束的第二次世界大戰，可稱之為物理學家的戰爭。以此類推，有人相信第三次世界大戰將是數學家的戰爭，因為數學家將掌控下一場大戰的重要武器—資訊。

約翰・查威克在《線形文字 *B* 的解譯》中說道「揭開秘密的衝動是人類根深蒂固的天性。就是最不好奇的心，也會為即將得知他人的秘密而悸動。有些幸運的人能以解謎為業，我們大部分的人卻得靠解開那些供消遣之用的矯造謎語來滿足這種慾望。對一般人而言，偵探故事或縱橫字謎便已足夠，極少數人則是以破解玄密的符號為志業」。

現在就讓密碼學家耍一道需要一點解密過程的《讀心術遊戲》，來滿足一般讀者的好奇心，也當成本章科學家餘興節目的內容：下圖中的左圖縱橫各六行列，一共有 36 位小朋友，每位小朋友只有站立或蹲下兩種情形，每按電腦的亂碼鈕一次，這 36 位小朋友會隨機設定成站立或蹲下。雖然是隨機，但是還是有某一種「特色」存在，請讀者從圖中解讀出這關鍵的「特色」是

什麼？當我們點選圖中一位小朋友時，此小朋友及其前、後、左、右共 5 位小朋友的狀態都會改變，即站立者變成蹲下者，而蹲下者卻變成站立者。例如：點選左圖中坐標為$(4,3)$的小朋友之後，就會變成右圖的小朋友站、蹲分布狀態。

讀心術遊戲是這樣進行的「讀心專家先閉上眼睛，被讀心的人在電腦上隨意的按電腦的亂碼鈕，按愈多次愈好，這樣小朋友的站蹲分布才會很亂。然後，從圖中選定 1 位小朋友，並點選他，舉例來說，下圖中 36 位小朋友的站蹲分布就是某位被讀心人操作的結果」。接著讀心專家張開他的雙眼，看著 36 位小朋友的分布圖及傾聽被讀心人的心跳，讀心專家可以辨識出剛剛被點選的小朋友的坐標，你相信嗎？理由又為何呢？

最後，感謝臺灣商務印書館翻譯的科普書籍《碼書》（賽門・辛著，劉燕芬譯），讓我對密碼學的歷史有基本的認識，也謝謝我的研究生陳裕錫幫我撰寫 Flash 版的《許教授的讀心術》遊戲，關於密碼學的科普書籍也可以參閱天下文化出版的《數學小魔女》（夫蘭納里著，葉偉文譯）與衛城出版的《資訊》（詹姆斯・葛雷易克著，賴盈滿譯）。

阿基米德的胃痛拼圖…數大就是美

數缺形時少直覺，形少數時難入微。

許志農／臺灣師大數學系

西元前 287 年，阿基米德出生在古希臘西西里島東南端的敘拉古。在當時古希臘的輝煌文化已經逐漸衰退，經濟、文化中心逐漸轉移到埃及的亞歷山卓城。9 歲時，阿基米德到埃及的亞歷山卓城唸書，在這裡跟隨許多著名的數學家學習，包括有名的幾何學大師—歐幾里得。在經過許多年的求學歷程後，回到故鄉—敘拉古。據說阿基米德經常為了研究而廢寢忘食，走進他的住處，隨處可見數字和方程式，地上則是畫滿了各式各樣的圖形，牆上與桌上也無法倖免，都成了他的計算板，由此可知他旺盛的研究精神。

阿基米德的科學以惡作劇、謎題及走捷徑而聞名，他也喜歡答案超大的數學問題，其中有兩個問題跟我們這個時代有密切的關連，《牛群問題》是上世紀中葉才得到完整的答案，而《胃痛拼圖》卻是上世紀末才被重新挖掘出來的遊戲。在阿基米德死後的 2200 多年的今日，我們有幸與這兩個數大就是美的問題邂逅，算是緣分也是福氣。

根據傳說，西元前 3 世紀時，阿波羅尼亞斯（Apollonius）找到一個圓周率的近似值，比阿基米德的結果還要準確，而且，還寫了一篇批評阿基米德的文章，使得他很生氣。為了報復，阿基米德設計了一道計算題，必須計算到相當大的數字才能找到答案，在寫給當時亞歷山卓城圖書館館長艾拉塔斯西尼茲（Eratosthenes）的一封信中，提出他的牛群問題。到底阿基米德有沒有寫這封信，以及他是不是牛群問題的發明人，仍是一個疑問，倒是牛群問題被流傳下來了，這是阿基米德做過最遊戲式的計算。

朋友，為了計算太陽神的牛隻有多少，假如你擁有智慧，你還必須勤快，西西里島平原上有多少隻牛在吃草，特麗納西亞島上有四種顏色的牛，即乳白、黑、黃色和花紋，每一種中公牛比母牛多，並滿足下列九個條件：

1. 白公牛數 $=$ 黃公牛數 $+\left(\frac{1}{2}+\frac{1}{3}\right)$ 黑公牛數；

2. 黑公牛數 $=$ 黃公牛數 $+\left(\frac{1}{4}+\frac{1}{5}\right)$ 花公牛數；

3. 花公牛數 $=$ 黃公牛數 $+\left(\frac{1}{6}+\frac{1}{7}\right)$ 白公牛數；

4. 白母牛數 $=\left(\frac{1}{3}+\frac{1}{4}\right)$ 黑牛數；

5. 黑母牛數 $=\left(\frac{1}{4}+\frac{1}{5}\right)$ 花牛數；

6. 花母牛數 $=\left(\frac{1}{5}+\frac{1}{6}\right)$ 黃牛數；

7. 黃母牛數$=\left(\frac{1}{6}+\frac{1}{7}\right)$白牛數；

8. 白公牛數＋黑公牛數＝平方數；

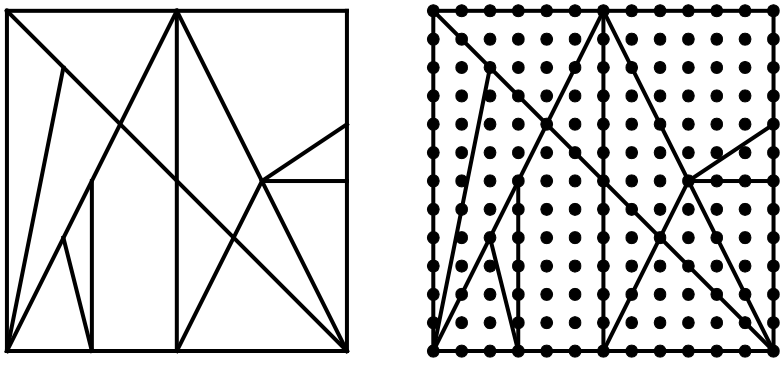
9. 花公牛數＋黃公牛數＝三角形數。

要證明滿足前 7 個約束條件的最小牛群總數是 50,389,082 並不難，但加上最後兩個條件以後就不同了。一直到 1880 年才有重大的進展，這一年，德國人安索爾（A. Amthor）證明最小牛群的總數，是一個由 7766 開頭的 206,545 位數字，真是個天文數字，全世界有這麼多牛嗎？牛群問題有 10 個未知數（為何 10 個呢？想想看），但只有 9 個方程式，根據數學經驗，答案可能有許多組，甚至無窮多組。

在 1981 年 7 月的《科學的美國人》雜誌透露，最近勞侖斯國家實驗室的尼爾遜，利用這個問題來測驗該實驗室那部新計算機克雷（CRAY）一號的性能，又把答案找出，並把結果發表在最新一期的《趣味數學》季刊上。他表示，用克雷一號只花了約 10 分鐘。由於時間太短，不足以測驗計算機的性能，所以又繼續用同一程式找出 5 個新的解答，最大的數目超過 100 萬位數。

《牛群問題》是上個世紀末才被解決的大數字問題，很難相信阿基米德本身可以解這問題。接下來要介紹的也是上個世紀末才被重新找到的阿基米德問題《胃痛拼圖》，這失蹤 2000 多年的拼圖遊戲被重新找到的過程是既有趣又離奇。

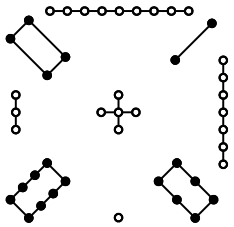
在加州史丹福大學同步輻射實驗室，古文物復原專家運用紫外光與數位圖像電腦處理技術，讓阿基米德發明的一道遊戲重現天日。在 1998 年 10 月 30 日，《紐約時報》頭版登了一則報導：紐約佳士得拍賣會上，有一本其貌不揚的古書，以美金 200 萬的高價成交。從外表看，這本書就像是中世紀某位修士的祈禱書，磨損不堪，布滿燒焦、水漬、發霉的痕跡。然而在祈禱文的下方，隱約可看見幾乎被擦拭掉的、傳抄自古代科學家阿基米德的抄本。這祈禱書是教士約翰・麥隆納斯於西元 1229 年 4 月 14 日抄寫，想在耶穌復活周年日，當作禮物獻給教會。羊皮紙從古代中世紀開始使用，由於價值極為貴重，通常經過皮面刮削後，重新書寫，被稱為再生羊皮紙，麥隆納斯將祈禱文書寫在再生羊皮紙上。透過高科技的掃描，祈禱書最後一頁原本是阿基米德稱為《胃痛拼圖》的一篇文章。該文章並非談身體的疼痛，而是在論述一道組合學的問題，而且附了一個正方形的插圖：



阿基米德的《胃痛拼圖》

在這再生羊皮書上，阿基米德所給的答案是 17152 種！這答案經過電腦科學家比爾・卡特勒驗證無誤，卡特勒也指出：將旋轉或者鏡射視為同一種的話，仍然有 536 種不同的拼法。事實上，幾位鼎鼎有名的數學家，如隆・格拉罕及金芳蓉夫婦檔，都只靠紙與筆就算出這個數字。

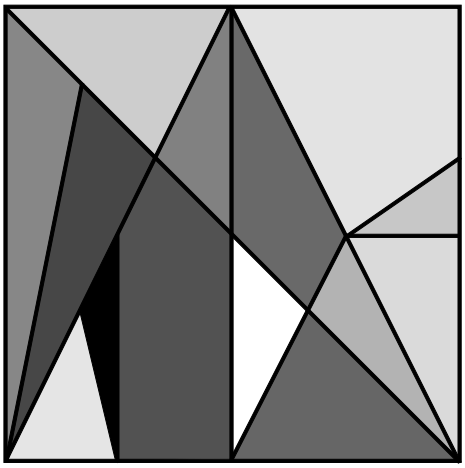
相傳在西元前 23 世紀大禹治水的時候，在黃河支流洛水中，浮現出一隻大烏龜，背甲上有 9 種花點的圖案，人們將圖案中的花點數了一下，竟驚奇地發現 9 種花點數正巧是 1～9 這 9 數，各數位置的排列也相當奇妙，後來人們稱這個圖案為洛書。



洛書給出的 9 個數所排成的方陣具有絕妙的性質，橫的 3 行、縱的 3 列以及兩對角線上各自的數字之和都是 15。人們因它的性質之獨特而大感興趣，對其進行了多方面的研究。中國把這「縱橫圖」或西方稱為「幻方」的精巧結構當作組合數學的濫觴。再生羊皮書的出現，西方似乎也把組合數學的歷史往前推算到阿基米德的《胃痛拼圖》。

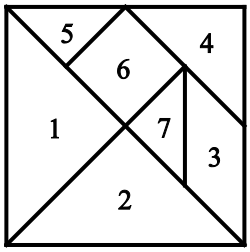
洛書、幻方都是組合學古老的例子，如今加入了胃痛拼圖這道啟蒙例子，讓組合學的內涵更多采多姿。從這些例子不難發現，組合學就是在處理離散的情形；而今日的電腦也是以處理離散情形為核心。計算機的使用讓組合學研究一日千里，同樣的，組合學的訓練也使計算機軟體產業得到好的基礎。

現在讓我們動手做一道練習吧！拿剪刀或美工刀將阿基米德的胃痛拼圖沿著黑線剪開，讓它變成 14 塊，然後將這 14 塊填滿底下阿基米德的正方形圖片 ，並要求轉動後的縫隙不得與原來的圖形一樣：



拼成正方形的方法有 17152 種，如果一位老師每天到學校的第一件事情就是拼出新的正方形，那麼在他退休時，也無法完成所有的拼法。這是否意味著隨便拼都會成功呢？試試看吧！

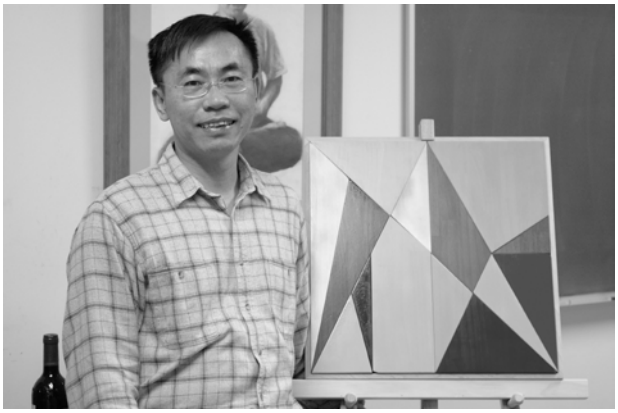
阿基米德的羊皮紙手稿，由丹麥學者海伯格於 1906 年在今之伊斯坦堡發現，1920 年再度失蹤，1998 年出現在紐約佳士得拍賣會上。該次拍賣，希臘代表競標至美金 190 萬才退出，而最後的得標者，是一位不願意透露姓名的美國收藏家，這位收藏家說，將來學者可以借閱該手稿。阿基米德的 14 塊拼圖，除了拼成正方形的遊戲之外，也可以玩類似中國七巧板的遊戲，拼各種動物。



七巧板

胃痛拼圖最早出現在中世紀的阿拉伯文譯本上，大家都把它視為類似中國七巧板的遊戲，直到再生羊皮書的出現，才了解阿基米德是在研究拼成正方形的組合方法數，並不是拼圖遊戲或是七巧板之類的益智遊戲。也因為這樣，阿基米德也成為西方組合學的老祖先。

胃痛拼圖是滑板遊戲的一種，可以用木板切割出精確的 14 塊，然後在正方形盒子內擺放，下圖是一個邊長 60 公分大小的木頭材質胃痛拼圖。從圖片中不難想像，把五顏六色的木板所拼出來的胃痛拼圖擺在辦公室或者住家牆壁上，肯定是不錯的裝飾。

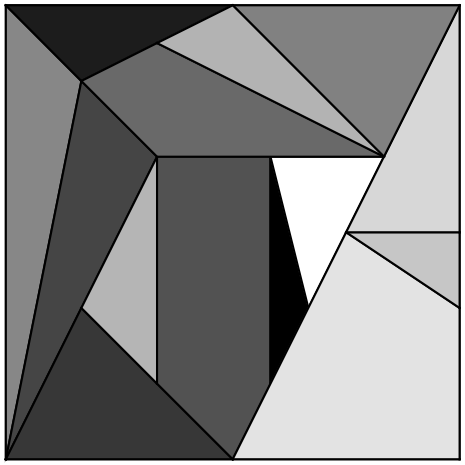


在尋找木工製作胃痛拼圖的過程，也有一段插曲，一般的木工師傅會告訴你「從正方形木板用鋸子切割，因為每鋸一段，都會產生 0.2 釐米的耗損，等 14 片都鋸完，再拼回去，肯定跟正方形有很大的落差，這樣的拼圖你不會滿意，所以沒辦法接這生意」，講究一點的師傅會說「這拼圖必須 14 塊逐一切割，才能在拼的過程完全密合，但這樣既耗木材，又浪費時間，價錢會很高，你應該不會接受」。這些都反映出幾何學中「尺規作圖」的重要性，國內木工師傅顯然在這方面的素養不是很夠，這恐怕是我國中學幾何教育一道待克服的問題。但是，也有例外，在景美女中教授生活科技的施妙佳老師，在聽完胃痛拼圖後，把它當成每位高二學生的一件工藝作品，他們也畫出精密準確的切割圖，沒有浪費太多材料，而且容易切割，完成之後的密合也很棒。

西元 1 世紀的希臘傳記作家普盧塔克描述阿基米德生前的最後一刻「他獨自一人，靠著圖形的輔助，正要求解問題，而把整個心思及雙眼，貫注在他的研究之上。他沒注意到羅馬人的入侵，或城市的淪陷。突然來了一名士兵，命令他隨同去見馬歇勒斯，他拒絕前往，要士兵等他解出問題，完成證明。士兵受不了而被激怒，抽出他的劍把阿基米德殺死了」。

在此要感謝三位對這篇文章有幫助的人，關於牛群問題，感謝林克瀛教授在《科學月刊》上的一篇文章，刊在 1982 年 3 月，第 147 期。關於胃痛拼圖，主要參考來源是天下文化出版的科普書籍《阿基米德寶典—失落的羊皮書》，由曹亮吉教授翻譯。在一次高雄的演講會上，曹教授對該書的內容及阿基米德的作品對我做了相當清楚的單獨講解，謝謝他的解釋。關於阿基米德的故事，大都是以少量的史實，加上大量的傳奇故事，所揉合而成的綜合體，其真實性，有賴讀者自行判斷。但是值得注意的是：阿基米德能在 22 個世紀以前，用十分有限的工具做出那麼多的成果，光是這點就值得把阿基米德邀請到我們的課堂裡，使講課內容更加豐富，並能擴大啟蒙學生的功效。關於阿基米德的作品也可以參考天下文化出版的《阿基米德幹了什麼好事！》（斯坦著，陳可崗譯）。

同時，也感謝我的研究生陳裕錫，他花了整個暑假的時間完成了胃痛拼圖的 Flash 版，原始程式長達 40 來頁，各位如果有這個免費的版本，也應該要感謝他的付出。最後，附上胃痛拼圖眾多解答中的一種，也是個人覺得很漂亮的一種拼法：



科普好書推薦專欄

洪萬生／臺灣師大數學系退休教授

推薦

書名：《消失的天才》Perfect Rigor: A Genius and the Mathematical Breakthrough of the Century

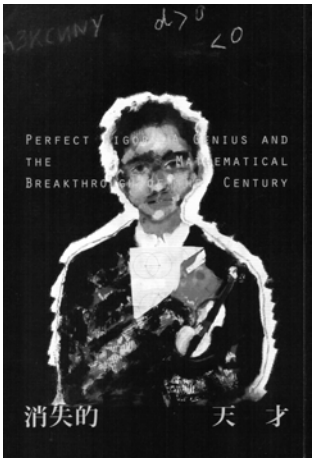
作者：瑪莎・葛森（Masha Gessen）

譯者：陳雅雲

出版社：臉譜出版社

出版日期：2012 年 4 月

關鍵詞：佩雷爾曼、龐加萊猜想、拓樸學、百萬美金難題、數學奧林匹亞



公元 2000 年，克雷研究所（Clay Mathematics Institute）在波斯頓舉辦的數學千禧年會議，擬定了七大百萬美金難題，作為 21 世紀數學的發展願景。顯然，這意在追隨希爾伯特（David Hilbert, 1862～1943）於 1900 年之壯舉，當年在巴黎舉行的國際數學家會議上，這位德國偉大數學家為 20 世紀數學，規劃了 23 道值得解決的難題，亦即後來所謂的「希爾伯特 23 問題」。現在，針對這七個世紀大難題，正如證明費馬最後定理的懷爾斯（Andrew Wiles）指出：「我們不知道它們會在何時解決：有可能要等 5 年，或者可能 100 年。但我們相信解決這些難題，可以為數學發現與景象開創全新的局面。」想不到言猶在耳，其中的「龐加萊猜想」（Poincare Conjecture）在 2002 年就獲得解決。至於貢獻這個證明的「最後一哩路」之天才，正是俄羅斯數學家格里高利・佩雷爾曼（Grigory Perelman）。

所謂「龐加萊猜想」，是由法國偉大數學家亨利・龐加萊（Henri Poincare, 1854～1912）—他與希爾伯特並稱為 20 世紀數學雙雄—在 1904 年所提出。他的原始版本是三維的情形：

> 如果一個三維流形（3-dimensional manifold）是平滑且為單連通，那麼，它與三維球 S^3 微分同胚（diffeomorphic）。

為了解決這個猜想，多位數學家在 1960 年代依序證明七維、五維、六維與更高維的情形。接著，證明的進展就完全停頓了下來，直到 1982 年，年僅 32 歲的美國數學家傅利曼（Michael Freedman）證明了四維的情形，而榮獲費爾茲獎（Fields Medal）。然而，所有這些證明與進路碰上三維本尊，全都束手無策。不過，卻也正是在此時，威廉・瑟斯頓（William Thurston）針對三維流形，

提出他的可能切割方式，亦即後來所謂的「幾何化猜想」(geometric conjecture)。然後，理查・漢米爾頓（Richard Hamilton）並緊接著據以擬定他的研究綱領（research programme）。可惜，漢米爾頓與他的團隊功敗垂成，最後利用他的工具與進路攻頂的，正是可畏的後生小輩佩雷爾曼。

佩雷爾曼將他的證明發表在數學網站上，而非一般數學家所習慣發表的期刊。儘管如此，2006 年在馬德里召開的國際數學家會議，還是頒給他數學界的最高榮譽費爾茲獎—這被視為數學界的諾貝爾獎，其獲獎條件甚至比諾貝爾獎還嚴苛，沒想到他竟然拒絕領獎。這種將自我從整個數學社群放逐的作風，甚至也波及克雷研究所所頒贈的百萬美金獎。

這究竟是怎麼回事？數學界一直眾說紛紜，始終無從理解他的內心世界。現在，有了瑪莎・葛森所寫的這一本佩雷爾曼傳記，我們多少可以想像在佩雷爾曼那柏拉圖式理想(Platonic ideal)的數學經驗遭嫉之後，他如何開始退縮，先是離開數學界，然後又從日常生活世界隱遁。

瑪莎・葛森是俄羅斯猶太人，後來，隨雙親移民美國，目前又回到莫斯科擔任新聞工作。她年輕時也曾參加前蘇聯（放學後的）數學俱樂部—那是將佩雷爾曼訓練成為一代數學奇才的課程，因此，她有很難得的機緣，可以從佩雷爾曼的師長、同事與朋友，述說一個相當引人但卻令人感傷的天才故事。這本傳記非常值得推薦，它的精彩敘事絕對超過約翰・納許(John Nash)的傳記—《美麗境界》(*A Beautiful Mind*)。

不過，根據作者的訪談，沒有人形容佩雷爾曼才華橫溢，只是說他「非常、非常聰明，思考非常、非常精確」。事實上，儘管他揚名立萬的主題是幾何學的延伸—拓樸學（topology），然而，「他的幾何想像力也不曾令同事讚嘆，但他們幾乎都對他在解題時所展現百分百的精確度，感到印象深刻。他的大腦幾乎就像萬能的數學壓縮機，能把問題壓縮成本質。無論他的腦是怎麼構成的，最終數學俱樂部的同學暱稱它為『佩雷爾曼槌』(Perelman stick)，因為它就像一個巨大的想像工具，他總是靜坐著用它思考，然後揮出致命的一擊」。

另一方面，數學俱樂部的老師魯克辛除了引導學生學習數學之外，也介紹他們進入文學和音樂的領域，並以此為己任，但是，佩雷爾曼卻全神貫注數學。由於他的優異表現，在他十四歲時，佩雷爾曼被送進一所數學菁英學校就讀，那就是位於列寧格勒，鼎鼎大名的 239 號數學物理專業學校。這種學校的建制，可以說是前蘇聯一代數學大師柯莫哥洛夫(Andrey Nikolaevich Kolmogorov, 1903～1987)的珍貴遺產。他認為「一個人想要成為偉大的數學家，必須具有音樂、視覺藝術和詩方面的涵養」。事實上，他始終醉心研究偉大作家普希金（Pushkin）的詩之形式與結構。此外，他還認為強健的體魄也同等重要。他的一位學生在追思錄中指出：「柯莫哥洛夫曾經特別稱讚他很會摔角」。

由此觀之，前蘇聯的數學菁英教育，除了訓練超強的數學奧林匹亞的金牌選手之外，也有

相當可貴的教育過程，值得有意鼓勵子女走上這一條窄路的家長參考借鑑。其實，要不是數學奧林匹亞競賽，以佩雷爾曼的猶太人身分，根本被排除在前蘇聯菁英教育體制之外。當然，要是讀者想要了解前蘇聯數學社群的社會文化面向，那麼，作者在本書第一章〈逃入想像的世界〉就提供了一個不可或缺的觀察。譬如說吧，作者以她極為敏銳的眼光，看到她熟悉的蘇共體制下的俄羅斯數學：

> 俄羅斯孕育出 20 世紀一些最偉大的數學家，這件事本身就是一個奇蹟。數學跟前蘇聯時代的做法形成顯著的對比。數學提倡論證，研究胚騰，俄羅斯卻控制人民，迫使他們不斷接受變化、無法預測的現實；數學重視邏輯與一致性，當時的文化卻以華麗虛飾的語言和恐懼為成長的養分；數學要求高度專業的知識才能理解，所以對門外漢來說，數學就像密碼一樣難以解讀；更糟的是，數學主張單一、可知的真理，當時政體的合法性卻是建立在單方認定的真理上。

不過，儘管這種數學文化 vs.政治文化的強烈對比，「俄羅斯的數學之所以能逃過法令規章的摧殘，主要有三個幾乎毫無關聯的因素。第一，俄羅斯的數學原本可能受創最重，它卻剛好特別堅強。第二，數學太過艱澀，蘇聯領導人偏好的手法無從干涉。第三，它剛好證明在關鍵的時刻對蘇聯有用。」

因此，本書不僅是佩雷爾曼的傳記，同時，也是數學社會學（sociology of mathematics）的一種書寫，任何人想要了解前蘇聯如何有能力在數學研究上與美國爭霸，更是不可或缺的參考讀物。讀者若能與論述主要關乎歐美世界的《數學恩仇錄》（*Great Feuds in Mathematics: Ten of the Liveliest Disputes Ever*）併而觀之，一定可以得到意想不到的收穫。

最後，有關本書之敘事手法，作者的告白值得引述如下：

> 我撰寫本書的方式跟一般傳記的做法不同。我沒有深入訪談佩雷爾曼。事實上，我完全沒有與他交談過。等我開始撰寫本書時，他已經跟所有記者和大多數人斷絕聯繫。這使我的工作變得更加困難，因為我得想像一個未曾謀面的人，但這也讓這項工作變得更加有趣：就像進行一場研究。幸運的是，大多數曾經與佩雷爾曼親近且熟知「龐加萊猜想」故事的人，願意接受訪談。事實上，有時我覺得這比描繪一個合作的故事主人翁還容易，因為我想寫的並不是佩雷爾曼本人敘述的故事及他對自己的看法—而是想找出真相。

旨哉斯言！瑪莎・葛森真是太謙虛了，其實，數學史家撰寫數學家傳記不也是如此嗎？本書所以十足有趣，正是因為作者在「龐加萊猜想」的求解脈絡中，說明佩雷爾曼的數學經驗（mathematical experience），乃至於他與前蘇聯、國際數學社群的互動關係，如何地具有歷史意義。

利用單形法求線性規劃的問題

鍾國華／臺北市祐德高中

一、前言 》

在數亦優第 18 期的文章：「利用最小成本法求運輸問題」刊出後，引起學生們的興趣，上課中最常提問的兩個問題：「第一個問題是：線性規劃（linear programming）的問題除了圖解法（graph method）外，是否還有其他解法？第二個問題是：三個變數以上的線性規劃要如何求解？」，本文提出單形法（simplex method），以解答學生的學習問題。

二、單形法 》

1. 沿史：美國數學家丹奇格（G. D. Dantzig）於 1947 年導出單形法，用以分析美國空軍戰備資源的分配問題。
2. 線性規劃：乃是在一組不等式的限制條件下，求取目標函數極值的方法。即線性規劃是單一目標的規劃，如何在有限資源的條件下，追求最大利潤或最小成本，兩者選其一。
3. 線性規劃模式建立步驟：
   (1) 找出決策變數，並以符號表示（常以 x_j 表示）。
   (2) 找出目標準則，冠上極大或極小字眼表示（即 Max 或 Min）。
   (3) 找出所有限制條件，並利用決策變數作線性組合。
   (4) 表明決策變數的非負性（即 $x_j \geq 0$ ）。
4. 線性規劃模式建立的架構：
   (1) 模式：
   (A) 目標函數：$\text{Max } Z = \sum_{j=1}^{n} c_j x_j$ （或 $\text{Min } Z = \sum_{j=1}^{n} c_j x_j$ ）
   (B) 結構限制式：$\text{subject to} \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_j \leq b_i$ （不等式≤或≥組成）
   (C) 非負限制式：$x_j \geq 0$ ， $j = 1,\ 2,\ 3,\ \cdots\cdots,\ n$
   註：結構限制式與非負限制式，統稱為「條件不等式」。
   (2) 符號說明：
   (A) x_j ：為決策變數（decision variable），表示第 j 項產品的生產數量。

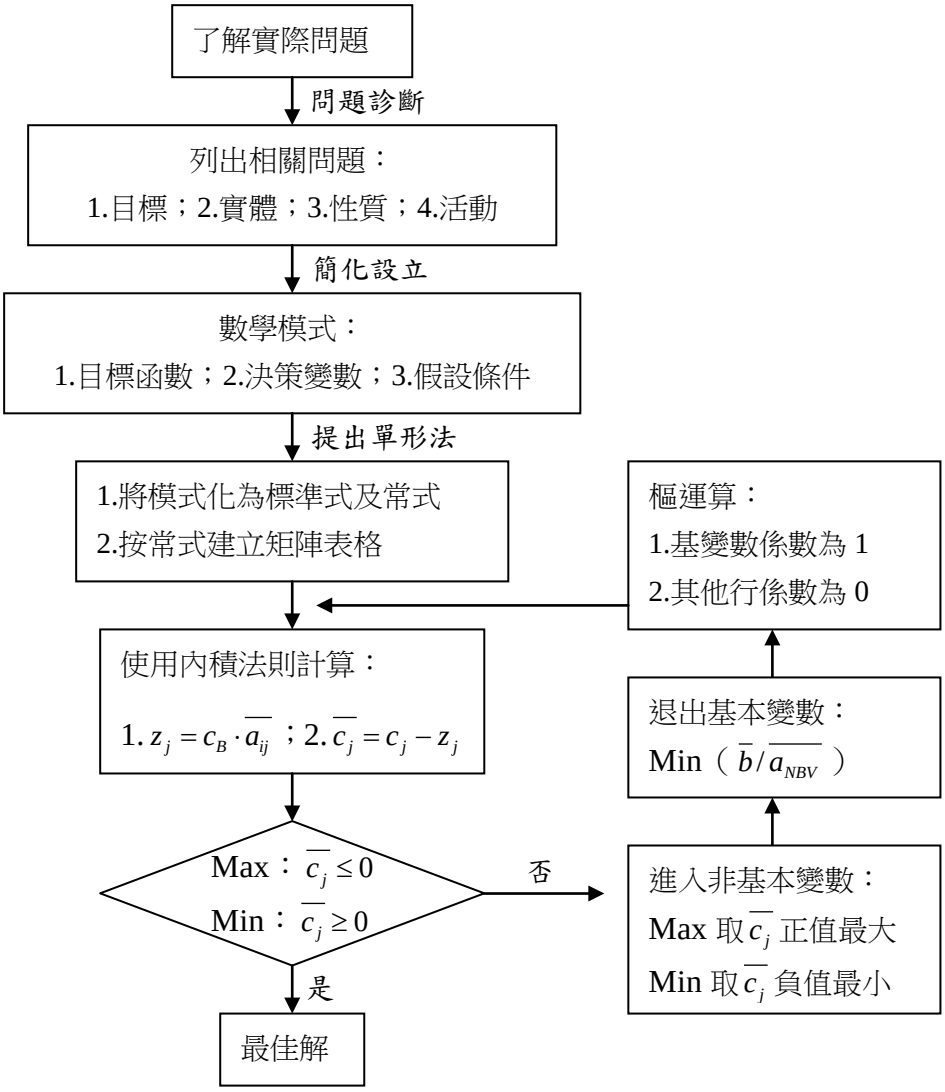
(B) c_j ：為目標函數中決策變數之係數，代表第 j 種產品之邊際利潤或單位利潤（Max 時），或單位成本（Min 時）。

(C) a_{ij} ：為限制式係數（或投入產出係數 input-output coefficient），代表第 j 種產品，所需要之第 i 種資源的投入數量。

(D) b_i ：為限制條件式的右手係數（right-hand coefficient），代表第 i 種可用資源的數量。

(E) Z ：為目標函數（objective function），表示效用或成本的衡量水準。

5. 單形法：單形（simplex）並不是簡單（simple）的意思，係指由數個端點所形成的凸多面體。單形法是依據兩個基本觀念：第一是，若可行解區不是空集合，則是一個凸集合的多面體；第二是，若有最佳解，則一定有一個最佳解在可行解區的端點上。單形法就是根據以上兩個觀念推導出來的線性規劃求解演算法。解線性規劃問題包含端點之決定，並由一端點移至相鄰端點以尋求最佳解。如何使用單形法求線性規劃的問題，特別製作一流程圖，使學生更容易理解線性規劃思考的架構。



三、線性規劃的模式要先轉化為標準式及常式 》

1. 將線性規劃模式轉化為標準式（standard form）：

(1) 將所有不等式化為等式，使成為線性形式，所加變數之目標函數係數為 0。

Max $z = cx$ → Max $z = cx + 0s_1$

$ax \le b$ → $ax + s_1 = b$

Min $z = cx$ → Min $z = cx + 0s_2$

$ax \ge b$ → $ax - s_2 = b$

說明：

(A) s_1 為閒置變數（slack variable）：指在不等式 $ax \le b$ 中，加上閒置變數，使成等式之變數，表示多餘未利用完的資源。

(B) s_2 為剩餘變數（surplus variable）：指在不等式 $ax \ge b$ 中，減去剩餘變數，使成等式之變數，表示資源最低需求的超餘，即較規定的資源 b 為多的數量。

(2) b 為負數時，乘上負號，化 b 為正數。

(3) 決策變數為不限正負或無符號限制（unrestraint）時，以二個新非負性變數替代。若 x_3 不限正負，則令 $x_3 = x_3^+ - x_3^-$ 代入，且 x_3^+ ， $x_3^- \ge 0$ 。例如： x_3 表示一年度產量與目前生產數量之差額，則下一年度產量如果增加，則 x_3 為正值；反之，若減產，則 x_3 為負值。

(4) 決策變數有負值下限，即 $x_j \ge b_i$ 且 $b_i < 0$ 時，則令 $x_j = b_i + x_j'$ 且 $x_j' \ge 0$ 。

(5) 決策變數有負值上限，即 $x_j \le b_i$ 且 $b_i > 0$ 時，則令 $x_j = b_i - x_j'$ 且 $x_j' \ge 0$ 。

2. 將標準式轉化為常式（或正規型式 canonical form）：

(1) 常式定義：每一條方程式中，至少要有一個基本變數（basic variables），此基本變數在本身方程式中的行係數為 1，而在其他方程式中的行係數為 0，所加人工變數之目標函數係數為 $-m$（Max 時）或 m（Min 時）， m 是無窮大的數。

Max $z = cx$ → Max $z = cx - ms_3$

$ax = b$ → $ax + s_3 = b$

Min $z = cx$ → Min $z = cx + ms_3$

$ax = b$ → $ax + s_3 = b$

(2) 說明：

(A) 基本變數（basic variable 簡稱 B.V）：其變數簡寫為 x_B ，指一變數在本身方程式中的行係數為 1，而在其他方程式中的行係數為 0，否則，稱為非基本變數（nonbasic

variables 簡稱 N. B. V），其變數簡寫為 x_N 。

(B) s_3 為人工變數（artificial variable）：指在等式 $ax=b$ 中，所加的虛擬變數，使等式產生基本變數之變數，稱為人工變數。事實上，人工變數是不存在的，主要目的是在證明「無解」用。

四、單形法的求解步驟（參考流程圖）》

第 1 步：將模式化為標準式及常式，其目的是為了建立矩陣運算。

第 2 步：按常式建立矩陣表格，如下表。

基本變數係數 c_B	基本變數 x_B	目標函數係數 c_j		可用資源 b
		非基本變數 x_N	基本變數 x_B	
c_B	x_B	限制式係數 A（即 $\overline{a_{ij}}$）	單位矩陣 I	$\overline{b}$
	z_j			
	$c_j - z_j$			

第 3 步：使用內積法則，先計算

1. $z_j = c_B \cdot \overline{a_{ij}}$ 。

2. $\overline{c_j} = c_j - z_j = c_j - c_B \cdot \overline{a_{ij}}$ 。

第 4 步：判別 $\overline{c_j}$ 。

在 Max 時，所有 $\overline{c_j} \le 0$ 有最佳解；在 Min 時，所有 $\overline{c_j} \ge 0$ 有最佳解。

若不符合上述條件，則到第 5 步驟；若符合上述條件，則到第 6 步驟。

第 5 步：重新進入一個非基本變數，並退出一個基本變數。

1. 進入非基本變數：在 Max 時，取 $\overline{c_j}$ 正值最大；在 Min 時，取 $\overline{c_j}$ 負值最小；若有樞列相等，任選其一。
2. 退出基本變數：均採用 Min（ $\frac{\overline{b}}{\overline{a}_{n.b.v}}$ ）且 $\overline{b} > 0$ 、 $\overline{a}_{n.b.v} > 0$ 。
3. 重新樞運算：本身（基本變數）行係數為 1，其他行係數為 0。
4. 重新回到第 3 步驟。

第 6 步：最佳解（optimal solution）的判定。

1. 恰有一組解（optimal solution）：當 $\bar{b} \geq 0$ 且 $\overline{c_j}$ 中 0 的個數等於 c_B 中基本變數的個數時，表示恰有一組可行解，使得目標函數值最佳者。
2. 無限多組解（alternative optimal solution）：當 $\bar{b} \geq 0$ 且 $\overline{c_j}$ 中 0 的個數大於 c_B 中基本變數的個數時，表示有二組以上可行解，使得目標函數值最佳者。其原因是目標函數的斜率等於某一條限制式的斜率（重合）。
3. 無解（infeasible solution）：當 $\bar{b} < 0$ 或無法消除人工變數為 m（即人工變數有 m 的解）時，表示可行解區是空集合，即限制條件交集為空集合。其原因是限制條件不一致，以致無交集。
4. 退化解（degeneracy solution）：當 $\bar{b} = 0$ 時，表示在求解過程中，某一限制條件的存在，並不影響其他限制條件值的變動，仍是恰有一組解。其原因是有重複限制因素或多餘限制條件。
5. 無限值解（unbounded solution）：當 Min 法則失敗，即計算 Min（$= \frac{\bar{b}}{a_{n.b.v}}$）時，所有 $\bar{a}_{n.b.v} \leq 0$，表示可行解會使目標函數值趨向於無限大（或無限小），即不能使目標函數值具有定量的最佳解。其原因是漏列了某些限制條件。

五、利用單形法求解 》

將民國 95 年社會組指考題，修改成三個變數的問題：為預防禽流感，營養師吩咐雞場主人每天必須從飼料中提供至少 4 單位的營養素 A、至少 3 單位的營養素 B 給他的雞群。這兩種營養素可由三種飼料中獲得，且知第一種飼料每公斤成本 36 元，並含有 3 單位的營養素 A 與 2 單位的營養素 B；第二種飼料每公斤成本 36 元，並含有 2 單位的營養素 A 與 3 單位的營養素 B；第三種飼料每公斤成本 14 元，並含有 1 單位的營養素 A 與 1 單位的營養素 B。若雞場主人想以最少的飼料成本來達到雞群的營養要求，則最少的飼料成本為多少元？

首先我們要先建立線性規劃模式如下：

假設雞場主人每天使用 x_1 公斤的第一種飼料，x_2 公斤的第二種飼料，x_3 公斤的第三種飼料，就能符合營養師要求。

Min $\quad z = 36x_1 + 36x_2 + 14x_3$（單位：元）

s. t $\quad \begin{cases} 3x_1 + 2x_2 + x_3 \geq 4 \\ 2x_1 + 3x_2 + x_3 \geq 3 \end{cases}$

非負性 $\quad x_1 \geq 0$ ， $x_2 \geq 0$ ， $x_3 \geq 0$

因為限制式為三元一次不等式，無法利用直角坐標系的圖解法求解；而且單形法是較有系統、有效率解決線性規劃問題的方法，所以我們採用單形法求解。

第 1 步：將線性規劃模式轉化為標準式及常式

1. 將所有不等式化為等式，使成為線性形式，所加變數之目標函數係數為 0。

Min $z = 36x_1 + 36x_2 + 14x_3 + 0x_4 + 0x_5$

s. t $3x_1 + 2x_2 + x_3 - x_4 = 4$

$2x_1 + 3x_2 + x_3 - x_5 = 3$

非負性 $x_j \geq 0$ ， $j = 1,\ 2,\ 3,\ 4,\ 5$

2. 將標準式轉化為常式：

Min $z = 36x_1 + 36x_2 + 14x_3 + 0x_4 + 0x_5 + mx_6 + mx_7$

s.t $3x_1 + 2x_2 + x_3 - x_4 + x_6 = 4$

$2x_1 + 3x_2 + x_3 - x_5 + x_7 = 3$

非負性 $x_j \geq 0$ ， $j = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$

第 2 步：按常式建立表格，如下表。

		c_j	36	36	14	0	0	m	m	
	c_B	x_B	x_1	x_2	x_3	x_4	x_5	x_6	x_7	$\overline{b_i}$
R_1	m	x_6	3	2	1	–1	0	1	0	4
R_2	m	x_7	2	3	1	0	–1	0	1	3
R_3		z_j	$5m$	$5m$	$2m$	$-m$	$-m$	m	m	$7m$
R_4		$c_j - z_j$	$36-5m$	$36-5m$	$14-2m$	m	m	0	0	
R_5	36	x_1	1	$\frac{2}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{4}{3}$
R_6	m	x_7	0	$\frac{2}{3}$	$\frac{1}{3}$	$\frac{2}{3}$	–1	$-\frac{2}{3}$	1	$\frac{1}{3}$
R_7		z_j	36	$24+\frac{2m}{3}$	$12+\frac{m}{3}$	$\frac{2m}{3}-12$	$-m$	$12-\frac{2m}{3}$	m	$48+\frac{m}{3}$
R_8		$c_j - z_j$	0	$12-\frac{2m}{3}$	$2-\frac{m}{3}$	$12-\frac{2m}{3}$	m	$\frac{m}{3}-12$	0	
R_9	36	x_1	1	0	0	–1	1	1	–1	1
R_{10}	36	x_2	0	1	$\frac{1}{2}$	1	$-\frac{3}{2}$	–1	$\frac{3}{2}$	$\frac{1}{2}$
R_{11}		z_j	36	36	18	0	–18	0	18	54
R_{12}		$c_j - z_j$	0	0	–4	0	18	m	$m-18$	
R_{13}	36	x_1	1	0	0	–1	1	1	–1	1
R_{14}	14	x_3	0	2	1	2	–3	–2	3	1
R_{15}		z_j	36	28	14	–8	–6	6	6	50
R_{16}		$c_j - z_j$	0	8	0	8	6	$m-6$	$m-6$	

【第一輪的演算過程】

第 3 步：使用內積法則，先計算

1. $z_j = c_B \cdot \overline{a_{ij}}$（看第 R_3 列）。

2. $\overline{c_j} = c_j - z_j$（看第 R_4 列）。

第 4 步：因第 R_4 列有 $\overline{c_j} = c_j - z_j \le 0$，尚未達到最佳解。

1. 進入非基本變數：$\text{Min}\left(36-5m, 36-5m, 14-2m\right) = 36-5m$（看第 R_4 列係數），選 x_1。

2. 退出基本變數：採用 $\text{Min}\left(\frac{4}{3}, \frac{3}{2}\right) = \frac{4}{3}$（看第 1 行 c_1 係數），選 x_6。

3. 重新樞運算：本身（基本變數）行係數為 1，其他行係數為 0。

   (1) x_1 列係數（看第 R_5 列係數）：$R_1 \div 3 = R_5$。

   (2) x_7 列係數（看第 R_6 列係數）：$R_5 \times (-2) + R_2 = R_6$。

   (3) 重新回到第 3 步驟。

【第二輪的演算過程】

第 3 步：使用內積法則，先計算

1. $z_j = c_B \cdot \overline{a_{ij}}$（看第 R_7 列）。

2. $\overline{c_j} = c_j - z_j$（看第 R_8 列）。

第 4 步：因第 R_8 列有 $\overline{c_j} = c_j - z_j \le 0$，尚未達到最佳解。

1. 進入非基本變數：$\text{Min}\left(12-\frac{2m}{3}, 2-\frac{m}{3}, 12-\frac{2m}{3}\right) = 12-\frac{2m}{3}$（看第 R_8 列係數），選 x_2。

2. 退出基本變數：採用 $\text{Min}\left(\frac{\frac{4}{3}}{\frac{2}{3}}, \frac{\frac{1}{3}}{\frac{2}{3}}\right) = \frac{1}{2}$（看第 2 行 c_2 係數），選 x_7。

3. 重新樞運算：本身（基本變數）行係數為 1，其他行係數為 0。

   (1) x_2 列係數（看第 R_{10} 列係數）：$R_6 \times \left(\frac{3}{2}\right) = R_{10}$。

   (2) x_1 列係數（看第 R_9 列係數）：$R_{10} \times \left(-\frac{2}{3}\right) + R_5 = R_9$。

   (3) 重新回到第 3 步驟。

【第三輪的演算過程】

第 3 步：使用內積法則，先計算

1. $z_j = c_B \cdot \overline{a_{ij}}$（看第 R_{11} 列）。

2. $\overline{c_j} = c_j - z_j$（看第 R_{12} 列）。

第 4 步：因第 R_{12} 列有 $\overline{c_j} = c_j - z_j \le 0$，尚未達到最佳解。

1. 進入非基本變數：$\text{Min}(-4) = -4$（看第 R_{12} 列係數），選 x_3。

2. 退出基本變數：採用 $\text{Min}\left(\frac{\frac{1}{2}}{\frac{1}{2}}\right) = 1$（看第 3 行 c_3 係數），選 x_2。

3. 重新樞運算：本身（基本變數）行係數為 1，其他行係數為 0。
   (1) x_3 列係數（看第 R_{14} 列係數）：$R_{10} \times 2 = R_{14}$。
   (2) x_1 列係數（看第 R_{13} 列係數）：R_9 不運算 $= R_{13}$。
   (3) 重新回到第 3 步驟。

【第四輪的演算過程】

第 3 步：使用內積法則，先計算

1. $z_j = c_B \cdot \overline{a_{ij}}$（看第 R_{15} 列）。

2. $\overline{c_j} = c_j - z_j$（看第 R_{16} 列）。

第 4 步：因第 R_{16} 列所有 $\overline{c_j} = c_j - z_j \ge 0$，有最佳解為 $x_1 = 1$，$x_2 = 0$，$x_3 = 1$，$\text{Min}\, z = 50$。

最佳解：雞場主人每天使用 1 公斤的第一種飼料，0 公斤的第二種飼料，1 公斤的第三種飼料，最小成本為 50 元。

六、結論 》

因為三個變數以上之線性規劃的問題，無法利用「圖解法」求解，必須改用「單形法」才能求解，而且變數愈多，人工的計算愈繁瑣。這時，若配合電腦程式 SAS/OR 或 Microsoft office Excel/規劃求解功能來計算，則計算問題就輕鬆解決了。從例題中，我們可發現單形法不僅在求最佳解外，亦可從閒置變數（slack variable）或剩餘變數（surplus variable）中了解資源是否有

浪費的情形？再配合敏感性分析（sensitivity analysis），即最佳解後的分析，讓管理者更能有效率的掌控資源，達成任務目標。

參考資料：

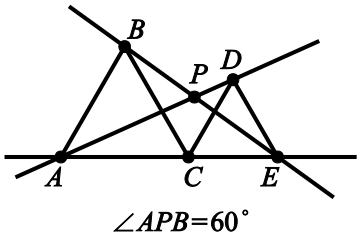
1. 高孔廉、張緯良，作業研究，五南圖書出版公司（1993）。
2. 陳文賢，管理科學—作業研究與數量方法，三民書局（1991）。

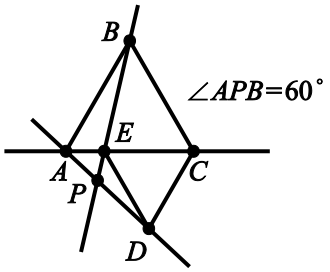
尋找動點軌跡的幾何圖形

江慶昱／衛道中學退休教師

數學的發展是問題取向的，從發現問題到分析演算之間，GSP 提供實驗探索的工具，可印證想法，也可再引發問題。

楔子 》





上面兩個圖中，△ABC 、△CDE 都是正三角形，$\overleftrightarrow{AD}$ 、$\overleftrightarrow{BE}$ 交於 P 點，則△ACD ≅△BCE 可以得到 $\angle APB = 60°$ 是一個不變量。這是國中的一個基本題。這種狀況用 GSP 統一這兩個圖形，並且看看在動態中能引發什麼問題是 GSP 最擅長的事。

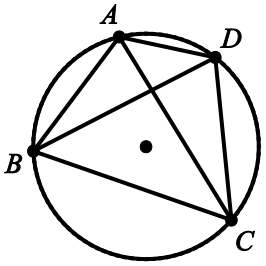
我追蹤 P 點的軌跡，發現 P 點的軌跡是一個圓形。於是，我繼續我的探尋之路……。

§1　四點共圓的條件 》

(1) A 、B 、C 、D 四點共圓 ⇔ 對角互補…… (1)

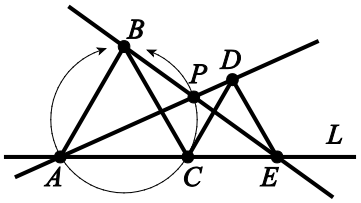
(2) A 、B 、C 、D 四點共圓 ⇔ $\angle ABD = \angle ACD$ ……(2)

四邊形對角互補是它有外接圓的充要條件，這是國中的基本定理，在這裡引入窮舉法來證明是一件很美妙的事，可惜被基測的考法拋棄了。另一個四點共圓的條件(2)比較沒被注意，可以當作一個習作。



§2-1 由正三角形中的不變量引出軌跡 》

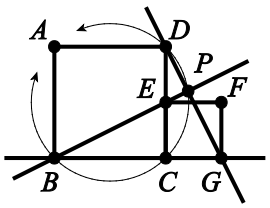
$\triangle ABC$、$\triangle CDE$ 都是正三角形，$\overleftrightarrow{AD}$、$\overleftrightarrow{BE}$ 交於 P 點，則 $\triangle ACD \cong \triangle BCE$，可以得到 $\angle APB = 60°$ 是一個不變量，讓 E 點在 $\overleftrightarrow{AC}$ 上移動，因為 $\angle APB = \angle ACB$ ，由(2)得知 P 點的軌跡為一圓。



$\angle APB$=60˚

§2-2 由正方形中的不變量引出軌跡 》

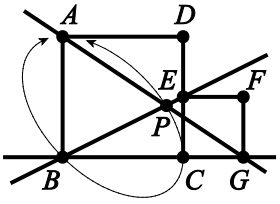
相同的狀況，若 $ABCD$ 、$CEFG$ 都是正方形，$\overleftrightarrow{BE}$ 、$\overleftrightarrow{DG}$ 交於 P ，則 $\triangle GCD \cong \triangle ECB$ ，可以得到 $\angle DPE = 90°$ 是一個不變量，讓 G 點在 $\overleftrightarrow{BC}$ 上移動，因為 $\angle BCD = \angle BPD = 90°$ ，由(2)得知 P 點的軌跡為一圓。



$\angle BPD$=90˚

§3-1 變量中引出的軌跡 》

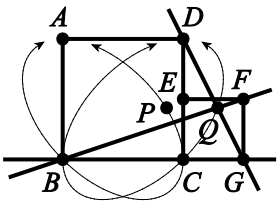
接下來，我取 P 點為 $\overleftrightarrow{AG}$ 、$\overleftrightarrow{BE}$ 的交點，G 點在 $\overleftrightarrow{BC}$ 上移動，則 P 點的軌跡如圖(1) $\angle APB$ 在變動，而 P 點的軌跡看起來像一個橢圓，問題：它是一個橢圓嗎？



圖(1)

§3-2　對稱性 》

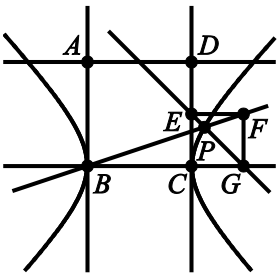
我取 Q 點為 $\overleftrightarrow{DG}$、$\overleftrightarrow{BF}$ 的交點，G 點在 $\overleftrightarrow{BC}$ 上動，則 Q 點的軌跡如圖(2)，看起來動點 Q 的軌跡與動點 P 的軌跡對稱於線段 $\overline{BC}$ 的中垂線。合理的想法是它們一定與某種對稱性有關。



圖(2)

§3-3　改變選取的變量 》

取 P 為 $\overleftrightarrow{BF}$ 、$\overleftrightarrow{GE}$ 的交點，G 點在 $\overleftrightarrow{BC}$ 上移動，則 P 點的軌跡如圖(3)，是一雙曲線嗎？

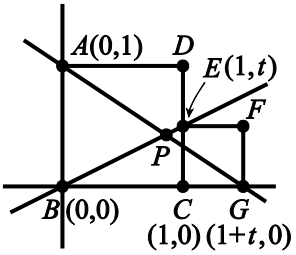


圖(3)

§3-4　驗證一下 》

建立一坐標系，使得 $B(0,0)$ 、$A(0,1)$ 、$C(1,0)$ 、$E(1,t)$ 、$G(1+t,0)$，則

$\overleftrightarrow{BE}: y=tx$ ； $\overline{AG}: -x=(1+t)(y-1)$

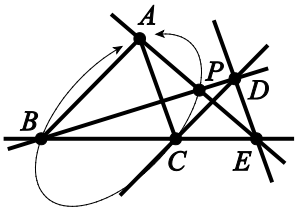


消去 t ，得 $x^2+xy+y^2-x-y=0$

$\delta=1^2-4=-3<0$ ，是橢圓類，因為圖形沒有退化，因此肯定圖(1)中的圖形就是橢圓。同理可以確定圖(3)是一雙曲線。

§4-1　把兩正三角形改成兩相似三角形看看 》

作任意 $\triangle ABC$ ，過 C 作直線 $L // \overleftrightarrow{AB}$ ，在 $\overleftrightarrow{BC}$ 上取一動點 E ，過 E 作一直線 $// \overleftrightarrow{AC}$ ，交直線 L 於 D ，則 $\triangle DCE \sim \triangle ABC$ ，連接 $\overleftrightarrow{BD}$ 、$\overleftrightarrow{AE}$ ，設兩線交於 P 點，讓 E 點在 $\overleftrightarrow{BC}$ 上動，則 P 點的軌跡看起來似乎是一個橢圓。

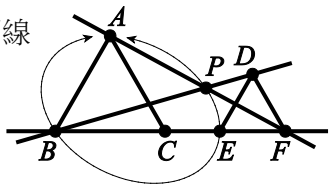


§4-2 合理的猜測 》

合理的猜測是§4-1 的圖是§2-1 的圓的線性變換。

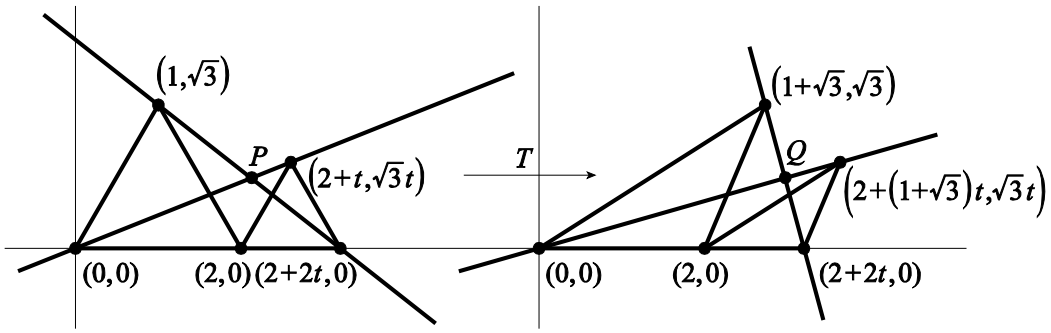
§4-3 讓兩正三角形離開看看 》

在直線 L 上作兩正 $\triangle ABC$ 、 $\triangle DEF$ ，如圖，連接 $\overleftrightarrow{BD}$ 、 $\overleftrightarrow{AF}$ ，假設兩線交於 P 點，讓 F 在 L 上移動，則 P 點的軌跡看起來似乎是一個橢圓。



§4-4 驗證你的猜測 》

作線性變換，令 $T=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ ，則 $T\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$ ， $T\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\1\end{bmatrix}$



$$\begin{cases}\dfrac{y}{x}=\dfrac{\sqrt{3}t}{2+t}\\ \dfrac{y-\sqrt{3}}{x-1}=\dfrac{-\sqrt{3}}{1+2t}\end{cases}$$

消去參數 t ，得 P 點的軌跡方程式： $x^2+y^2-2x-\dfrac{2\sqrt{3}}{3}y=0$ ……(1)

$$\begin{cases}\dfrac{y}{x}=\dfrac{\sqrt{3}t}{2+\left(1+\sqrt{3}\right)t}\\ \dfrac{y-\sqrt{3}}{x-\left(1+\sqrt{3}\right)}=\dfrac{-\sqrt{3}}{\left(1-\sqrt{3}\right)+2t}\end{cases}$$

消去參數 t 得 Q 點的軌跡方程式： $x^2-2xy+2y^2-2x+\left(2-\dfrac{2\sqrt{3}}{3}\right)y=0$ ……(2)

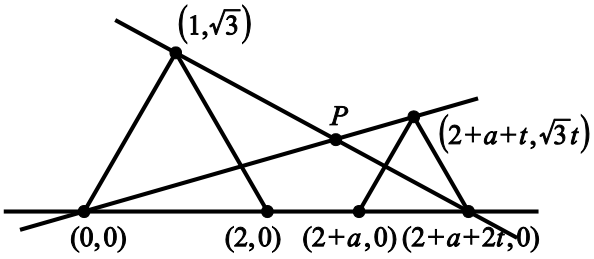
這個結果與直接用矩陣變換一樣，是意料中的事。

亦即 $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}=\begin{bmatrix}x+y\\ y\end{bmatrix}$，令 $X=x+y$，$Y=y$，則 $x=X-Y$，$y=Y$ 代入(1)中，化簡得(2)

因此，我們可以確定§4-1 的圖形是一個橢圓。

回到§4-3

P 是 $\begin{cases}\dfrac{y}{x}=\dfrac{\sqrt{3}t}{2+a+t}\\ \dfrac{y-\sqrt{3}}{x-1}=\dfrac{-\sqrt{3}}{1+a+2t}\end{cases}$ 的解

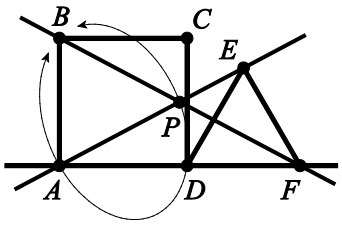


消去參數 t，得 $3x^2+\sqrt{3}axy+(3+a)y^2-(6+3a)x-\left(2\sqrt{3}+\sqrt{3}a\right)y=0$

$\delta=\left(\sqrt{3}a\right)^2-12(3+a)=3a^2-12a-36=3(a-6)(a+2)$，所以§4-3 的圖形可以是橢圓，雙曲線或拋物線（$a=-2$ 時，圖形顯然是一直線）。

§5-1 把正方形與三角形擺在一起》

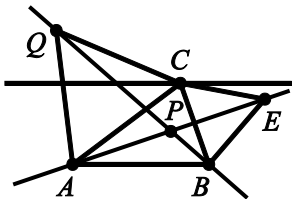
接著我作一個正方形 $ABCD$，一個正△DEF，作 $\overleftrightarrow{AE}$、$\overleftrightarrow{BF}$ 的交點 P，讓 F 在 $\overleftrightarrow{AD}$ 上移動，則 P 點的軌跡看起來是一個橢圓，諸位看官何不驗證一下！



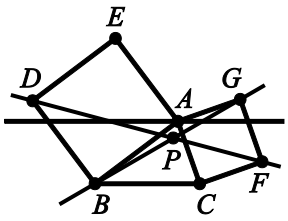
§5-2 接下來是你的探尋之路……。

習作 》

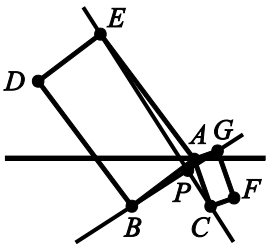
1. 在△ABC的兩邊$\overline{AC}$，$\overline{BC}$往外各作一個正△ACQ、△BCE，假設$\overleftrightarrow{AE}$、$\overleftrightarrow{BQ}$交於P點，讓C點在某一直線上移動，則P點的軌跡為何？



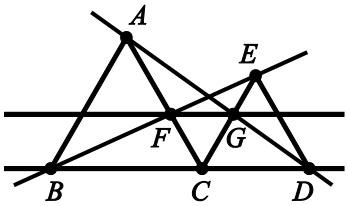
2. 在△ABC的兩邊$\overline{AC}$、$\overline{AB}$往外各作一個正方形$ACFG$、$ABDE$，假設$\overleftrightarrow{BG}$、$\overleftrightarrow{DF}$交於P，讓A點在某一直線上移動，則P點的軌跡為何？



3. 在△ABC的兩邊$\overline{AC}$、$\overline{AB}$往外各作一個矩形$ACFG$、$ABDE$，使得$\overline{AG}:\overline{AC}=\overline{AB}:\overline{AE}=1:2$，$\overleftrightarrow{BG}$、$\overleftrightarrow{CE}$交於$P$點，讓$A$點在某一直線上移動，則$P$點的軌跡為何？



4. 楔子中（如右圖），試證：



(1) △CFG為正三角形

(2) $\overleftrightarrow{FG}\,//\,\overleftrightarrow{BD}$

(3) 假設△ABC、△CDE、△CFG的邊長分別為a、b、c，試證$\frac{1}{a}+\frac{1}{b}=\frac{1}{c}$

參考資料：

1. 全任重教授，動態幾何 http://poncelet.math.nthu.edu.tw/disk3/moe-proj/index1.html。
2. 陳創義教授，http://math.ntnu.edu.tw/~cyc/。
3. 江慶昱老師，江老師數學，http://home.educities.edu.tw/kuen/。
4. 成功高中官老師，http://140.111.115.8/longlife/。

高中數學專題研究教案（Part I）

陳敏晧／蘭陽女中

壹、前言 》

教過高中數理班的老師通常都會實施數學專題研究，以筆者任教的學校為例，方式為在高一階段先進行前置作業：尋找研究題目（Title）、研究動機（Motivation）、如何蒐集相關資料（Materials）、相關研究法（Methods）、如何進行研究討論（含寫摘要）（Conclusions & Abstract）、如何強調研究發現（Findings）、如何製作研究結論（Conclusions）、參考文獻的格式（References）。高一下時，進行分組，原則上是每組三人，共十組，高二上學期約第三週，進行初期報告，由老師與同學提問，高二上學期末必須要有一些具體的研究發現，筆者利用寒假期間將學生作品審閱，挑選出有研究潛力組別，報名北區數學科展比賽及全國高中職小論文競賽，讓學生有舞臺表現。以下所呈現是林佩柔、李依庭、鄭羽呈三位學生的作品「數學『撕』想」。

貳、數學專題研究教案分享 》

摘　要

在某些機緣下，我們看到了一篇有關撕郵票的《數學傳播》資料，裡面討論的內容是希望找到一大張尚未撕開的郵票的最佳撕法，也就是最有效率、撕開次數最少的撕法，於是展開了一連串的探討。我們將此問題推廣至各種平面圖形和立體圖形來看，平面圖形包含矩形、正三角形以及正六邊形等，每種形狀再細分為規則排列、不規則排列以及內部有洞三種情況；另外立體圖形我們目前討論了柏拉圖多面體（Platonic Solids），希望未來還能朝向阿基米德多面體（Archimedean Solids）等各種立體圖形繼續研究下去。

研究動機

我們的研究動機是思考該如何撕郵票？不同形狀的郵票，究竟有沒有差別？我們想出除了矩形以外的郵票形狀，還有正三角形及正多邊形，也可從平面延伸至立體，並討論正多面體的切割次數，該如何切？需要切幾次才能使正多面體逐一切開成為單獨的面，希望能得到類似多面體尤拉公式$V+F-E=2$般地優美，其中V是多面體的頂點數、F是總面數、E是稜長數。

研究討論

一、平面幾何圖形「撕一次」與「洞」的定義

二、討論正方形郵票的撕裂次數

(一) $p\times q$ 張正方形郵票排列而成的矩形圖案

(二) 不規則排列

(三) 內部有洞

三、討論正三角形排列的撕裂次數

(一) 邊為 r 個三角形排列而成的正三角形圖案

(二) 不規則排列

(三) 內部有洞

四、討論正多邊形排列的撕裂次數

(一) 完整排列

(二) 內部有洞

五、立體幾何圖形「切割」的定義

六、討論柏拉圖多面體切割的次數

(一) 正四面體

(二) 正六面體

(三) 正八面體

(四) 正十二面體

(五) 正二十面體

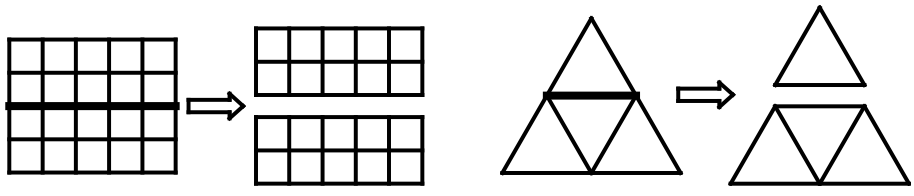
七、朝向阿基米德立體圖形研究

研究過程與發現

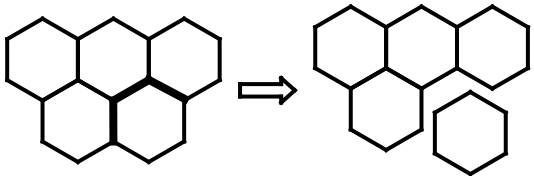
一、平面幾何圖形「撕一次」與「洞」的定義

(一)「撕一次」的定義：

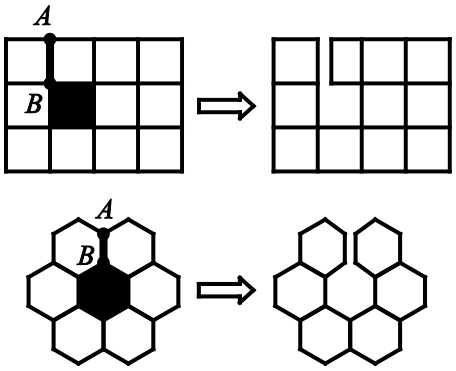
1. 矩形及三角形的完整排列、不規則排列：將整頁郵票沿某直線撕成兩小頁的動作，稱為「撕一次」。例如：



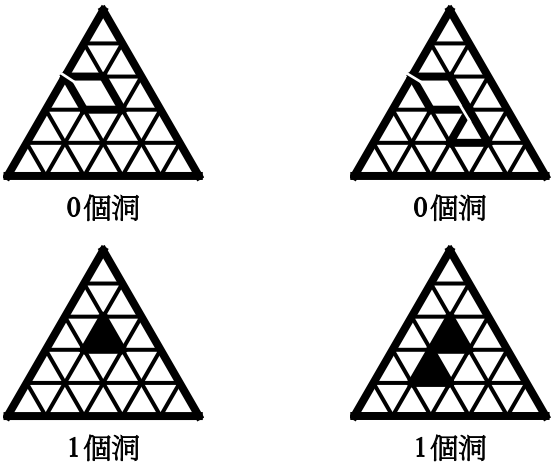
2. 正多邊形的完整排列、不規則排列：沿著相連的邊撕開，撕成兩小頁的動作，稱為「撕一次」。例如：



3. 內部有洞：必須先將內部有洞的圖形撕開成不規則圖形。設 A 和 B 為封閉折線上的兩點，此兩點可能在同一折線上，也可能分別在不同的折線上。 A 到 B 的直線段都是平面之間的連結線，而且不再經過任何折線，則從 A 撕到 B 的動作，稱為「撕一次」。例如：



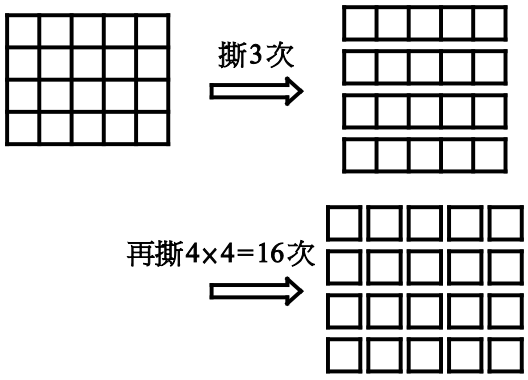
(二) 「n 個洞」的定義：將一頁未撕開，邊緣描繪所形成的圖形為 $n+1$ 個彼此不相連的封閉折線，則此頁有「n 個洞」。例如：



二、正方形郵票

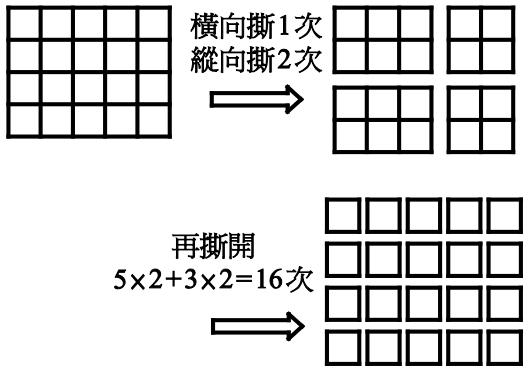
(一) 完整排列：以 $p\times q$ 張正方形郵票排列而成的矩形圖案

1. 一頁 4×5 的郵票



【方法 1】

先橫向撕開 3 次後，再縱向逐一撕開成小張正方形，共需撕 $3+4\times4=19$ 次。



【方法 2】

將一頁分成 4 份，再逐一撕開成小張正方形，共需撕 $3+5\times2+3\times2=19$ 次。

由上得知：當矩形邊長為 $p\times q$ 時，撕的次數為張數 $(p\times q-1)$ 次。

利用數學歸納法證明：已知有 m 張郵票，求證需撕 $m-1$ 次，$\forall m\in$ □ 。

證明：當 $m=1$ 時，1 張郵票需撕 $1-1=0$ 次，成立

設 $m=k\in$ □ ，k 張郵票需撕 $k-1$ 次

則 $m=k+1$ 時，$(k+1)$ 張郵票需撕 k 次

設撕開第 1 次後，郵票分為兩部分，各為 x 張和 y 張，其中 $x+y=k+1$

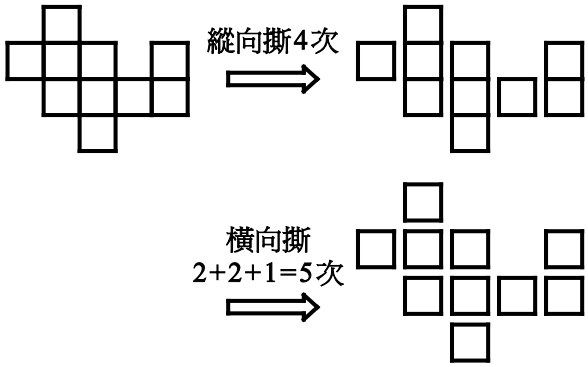
$1\le x\le k$ ，完全撕開需 $(x-1)$ 次

$1\le y\le k$ ，完全撕開需 $(y-1)$ 次

$\therefore 1+(x-1)+(y-1)=x+y-1=(k+1)-1=k$ ，成立。

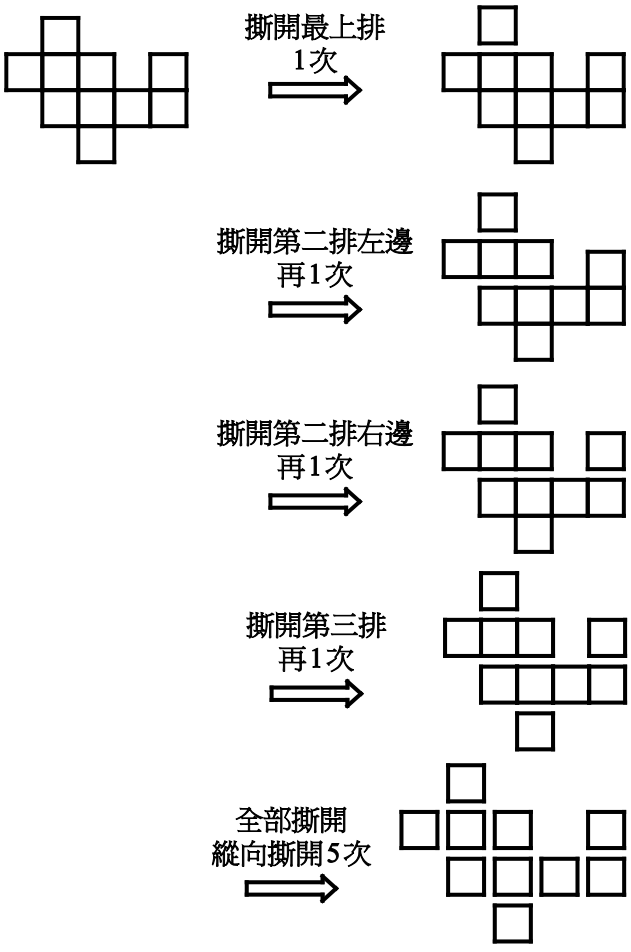
(二) 不規則排列：以 m 張正方形的郵票，排列出不規則形狀

1. 一頁 10 張正方形郵票不規則排列



【方法 1】

先縱向撕 4 次後，再橫向逐一撕開成小正方形，共需 $4+(2+2+1)=9$ 次。



【方法 2】

先以水平方向撕開 4 次後，再縱向逐一撕開成小正方形，共需撕 $4+2+3=9$ 次。

由上得知：當總張數為 m 張時，撕的次數為張數 $(m-1)$ 次。

利用數學歸納法證明：同正方形郵票完整排列。已知有 m 張郵票，求證需撕 $m-1$ 次，$\forall m\in\square$ 。

證明：當 $m=1$ 時，1 張郵票需撕 $1-1=0$ 次，成立

設 $m=k\in\square$ ，k 張郵票需撕 $k-1$ 次

則 $m=k+1$ 時，$(k+1)$ 張郵票需撕 k 次

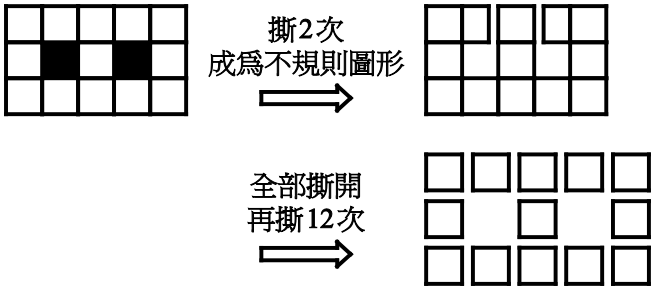
設撕開第 1 次後，郵票分為兩部分，各為 x 張和 y 張，其中 $x+y=k+1$

$1\le x\le k$ ，完全撕開需 $(x-1)$ 次，$1\le y\le k$ ，完全撕開需 $(y-1)$ 次

$\therefore 1+(x-1)+(y-1)=x+y-1=(k+1)-1=k$ ，成立。

(三) 內部有洞：張數 m 張、n 個洞的不規則排列。

1. 一頁 13 張且 2 洞的矩形郵票



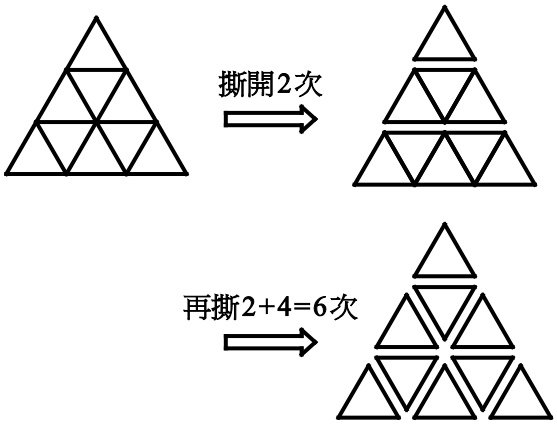
撕開 2 次，使其成為不規則排列，再逐一撕成小正方形，共需 $2+12=14$ 次。

由上得知：當有 n 個洞且 m 張時，撕的次數為 $n+(m-1)$ 次。

三、正三角形

(一) 完整排列：設每個三角形皆為邊長為 1 的小正三角形，而以邊長 r 排列而成的三角形圖形。

1. 一頁邊長為 3 的排列

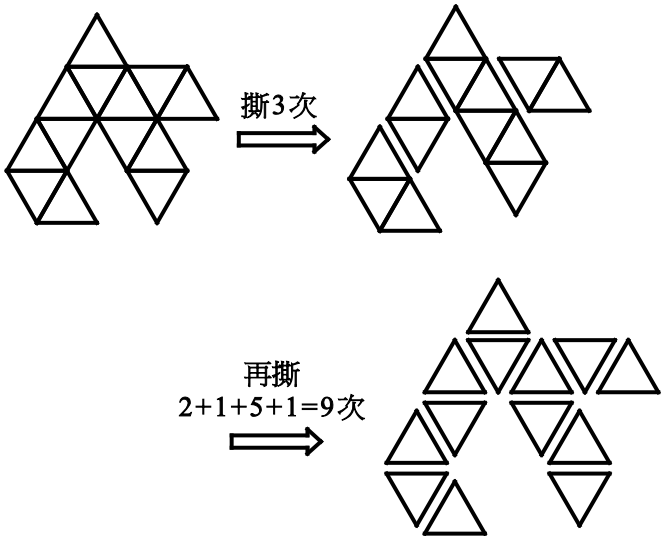


先橫向撕開 2 次後，再逐一撕開成小正三角，共需撕 $2+2+4=8$ 次。

由上得知：當以邊長皆為 1 的小正三角形排列成邊長為 r 的規則圖形時，撕的次數為 (r^2-1) 次。

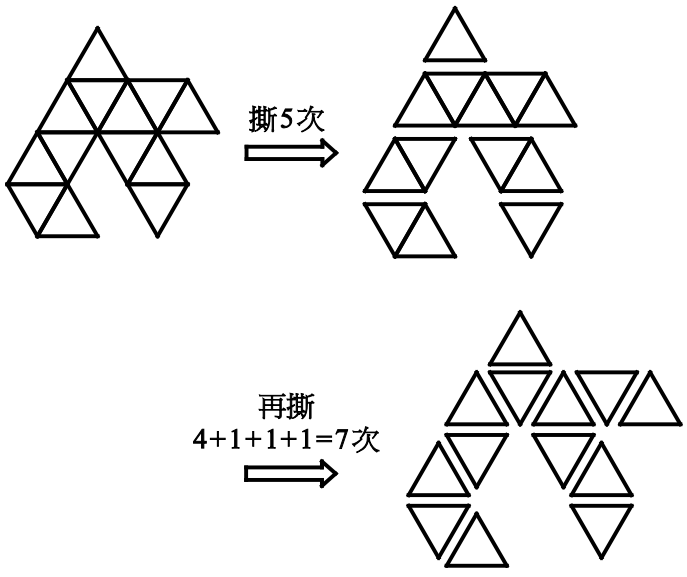
(二) 不規則排列：以 m 張小三角形，排列出不規則形狀。

1. 一頁 13 個正三角形排列



【方法 1】

先斜向撕 3 次後，再逐一撕開成小正三角，共需撕 $3+(2+1+5+1)=12$ 次。



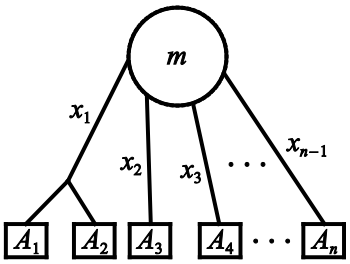
【方法 2】

先橫向撕 5 次後，再逐一撕開成小正三角，共需撕 12 次。

由上得知：當總張數為 m 張時，撕的次數為 $(m-1)$ 次。證明如下：

已知：撕裂第 K 次為 X_K ，而 A_K 為撕裂成規則圖形後的張數， m 為總張數， $f(K)$ 為總張數撕開次數的函數。求證：不規則排列郵票最少撕裂次數為 $(m-1)$ 次。

證明：因為 $A_1+A_2+A_3+\cdots+A_n=m$ ，所以



$$f(n)=(A_1-1)+(A_2-1)+(A_3-1)+\cdots+(A_n-1)+n-1$$

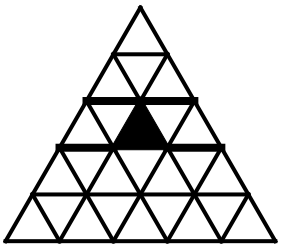
$$=(A_1+A_2+A_3+\cdots+A_n)-n+n-1=m-1\ 。$$

∴不規則排列郵票最少撕裂次數為 $(m-1)$ 次

(三) 內部有洞： m 張內部有 n 個洞的三角形

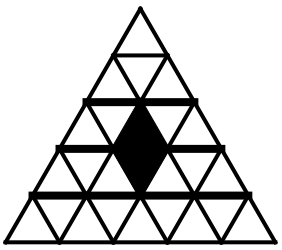
1. 一頁 23 張內部有 1 個洞的三角形

(1) 一張為 1 洞



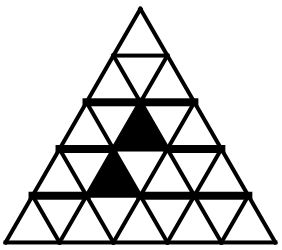
先橫向撕開 6 次後，再逐一撕開成小三角形，共需撕 $6+2+2+6+8=24$ 次。

(2) 兩張為 1 洞



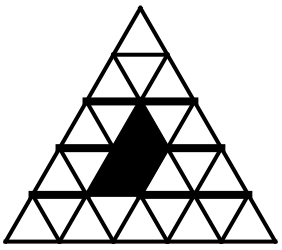
先橫向撕開 7 次後，再逐一撕開成小三角形，共需撕 $7+2+2+4+8=23$ 次。

(3) 兩張為 1 洞



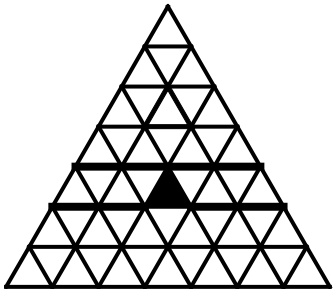
先橫向撕開 7 次後，再逐一撕開成小三角形，共需撕 $7+2+2+4+8=23$ 次。

(4) 三張為 1 洞



先橫向撕開 7 次後，再逐一撕開成小三角形，共需撕 $7+2+2+3+8=22$ 次。

2. 一頁 48 張內部有 1 個洞的三角形

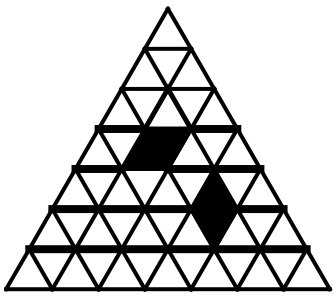


先橫向撕開 8 次後，再逐一撕開成小三角形，共需撕

$8+2+4+6+6+10+12=48$次。

3. 一頁 45 張內部有 2 個洞的三角形

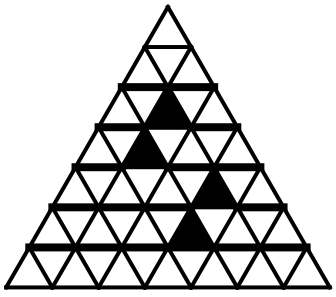
(1) 兩張為 1 洞，共 2 洞



先橫向撕開 11 次後，再逐一撕開成小三角形，共需撕

$11+2+4+3+6+8+12=46$次。

(2) 兩張為 1 洞，共 2 洞



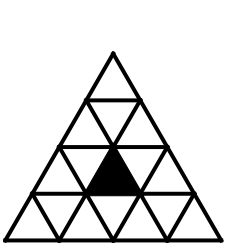
先橫向撕開 12 次後，再逐一撕開成小三角形，共需撕

$12+2+2+4+6+8+12=46$次。

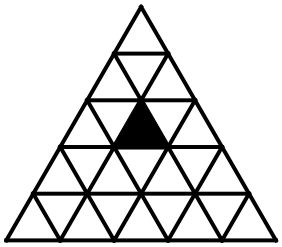
由上述例子得知：當有 n 個洞且總張數為 m 張，撕的次數為 $n+(m-1)$ 次。

利用數學歸納法證明： m 張內部有 n 個洞的三角形。

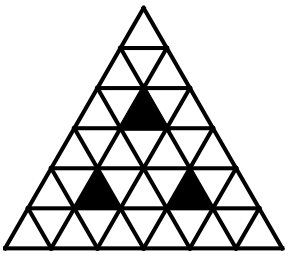
1. 在內部有洞的正三角形郵票中，因為洞數 n 會隨著每邊正三角個數而定，故不適合使用一般數學歸納法證明。
2. 最大洞數隨著每邊正三角形個數而改變，1 洞的正三角形郵票，最少每邊為 4 個正三角形。假設每邊為 r 張正三角形、內部 n 個洞：



若r=4，最多n=1

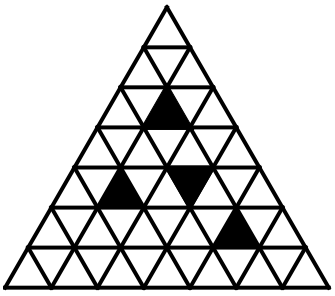


若r=5，最多n=1



若r=6，最多n=3

$1 \le n \le 3$



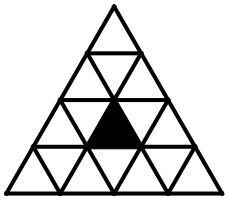
若r=7，最多n=4

$1 \le n \le 4$

以上皆為每邊 r 個正三角形內，洞數最多的情形。

3. 為了套用數學歸納法來證明總張數 m 與洞數 n 之間的關係，我們想到了以固定洞的數目來解決問題。
4. 固定洞數 n ，每邊 r 張正三角形，則總張數 m 為 r^2-n 張，共需撕 $n+(m-1)$ 次

(1) 設洞數 $n=1$ ，則 $r \ge 4$ ，總張數 $m=r^2-1$



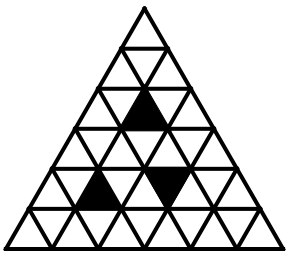
當 $r=4$ 時，總張數 $m=15$ ，則撕裂次數為 $1+(15-1)=15$ 次，成立

設 $r=k \in$ □ ， $m=k^2-1$ ，撕裂次數為 $1+\left[\left(k^2-1\right)-1\right]=k^2-1$ 次

則 $r=k+1$ 時， $m=(k+1)^2-1$

撕裂次數為 $1+\left\{\left[(k+1)^2-1\right]-1\right\}=(k+1)^2-1$ 次，成立。

(2) 設洞數 $n=3$，則 $r\geq 6$，總張數 $m=r^2-3$



設 $r=k\in$□，$m=k^2-3$，撕裂次數為 $3+\left[\left(k^2-3\right)-1\right]=k^2-1$ 次

則 $r=k+1$ 時，$m=\left(k+1\right)^2-3$

撕裂次數為 $3+\left\{\left[\left(k+1\right)^2-3\right]-1\right\}=\left(k+1\right)^2-1$ 次，成立。

《待續，請見數亦優第 22 期》

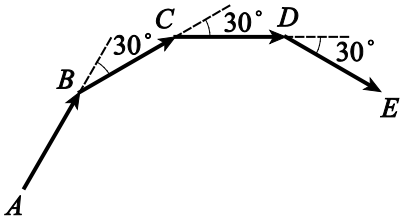
專欄 動手玩數學

許志農／臺灣師大數學系

遊戲 81

☆☆☆☆☆

如圖所示，一螞蟻從 A 點出發，往前直走 $8\sin 15°$ 公分至 B 點；接著右轉 $30°$，再往前直走 $8\sin 15°$ 公分至 C 點。螞蟻再重複右轉 $30°$ 及往前走 $8\sin 15°$ 公分兩次，分別到達 D 點及 E 點：



求下列的長度：

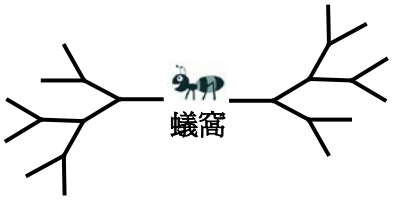
(1) A 點至 C 點的直線距離。

(2) A 點至 E 點的直線距離。

〔玩鎖・玩索〕

螞蟻只能看到平面（二維空間）的事物，只能在二維空間內做 $360°$ 方向上的任意運動。雖然螞蟻只生活在平面上，但是科學家卻發現螞蟻天生具有某種幾何的洞察力，能利用幾何原則尋找回窩的路。螞蟻的路線系統就像羅馬人的道路一樣……條條道路通羅馬；對螞蟻來說……條條路線通蟻窩。

要了解螞蟻尋找方向的訣竅，可以假想有一個「Y」字母的交叉點，而一隻離開蟻窩的螞蟻從「Y」字母底下往上爬，碰到這樣一個叉路，發現有兩條以狹窄角度交叉的路線。相反地，回窩的螞蟻會碰到兩條叉路：一條的交叉角度較小，而另一條的角度大得多，角度較大的那一條路才是回家的路。也就是說，螞蟻的網路是由「Y」字來構成，而且較小的交叉角是 $60°$ 左右，科學家稱它為「六十度法則」。如圖所示，一隻螞蟻從蟻窩出來，朝東邊方向以六十度法則向外覓食，而這蟻窩裡的螞蟻構造了向東及向西兩個方向的覓食網。



遊戲 82

☆☆

對於多項式的求值問題，秦九韶提出過一種演算法，舉例來說：多項式

$$f(x)=2x^3-5x^2+4x+8$$

的函數值 $f(a)$ 可以利用以下的小、中、大三層括弧依序來完成

$$f(a)=\{[(2a-5)a+4]a+8\}$$

想想看，秦九韶演算法跟高中課程的哪一個方法有雷同之處？並說明之。

〔玩鎖・玩索〕

秦九韶演算法，是中國南宋時期的數學家秦九韶最先提出的一種多項式求值的方法，後來在西方被 19 世紀初英國數學家威廉・喬治・霍納重新發現，又被稱作霍納演算法，而日本數學史家三上義夫在《中日數學史》一書中寫道「誰能否認，霍納的輝煌方法，至少在早於歐洲 600 年之前，已經在中國運用了」。

在現代數值分析學上有一種巢狀乘法（nested multiplication）的求值方法，事實上，它也是秦九韶演算法。

遊戲 83

☆☆☆☆☆

(1) 證明

$$\cot\frac{\pi}{24}=\frac{1+\cos\left(\frac{\pi}{3}-\frac{\pi}{4}\right)}{\sin\left(\frac{\pi}{3}-\frac{\pi}{4}\right)}。$$

(2) 求 $\cot\frac{\pi}{24}$ 的精確值。

〔玩鎖・玩索〕

這是一道有趣的求值問題。

遊戲 84

☆☆☆☆

試證：對任意實數 a、b、c，等式

$$\left[(2a-b-c)+(b-c)\sqrt{3}i\right]^3$$

$$=\left[(2c-a-b)+(a-b)\sqrt{3}i\right]^3$$

$$=\left[(2b-a-c)+(c-a)\sqrt{3}i\right]^3$$

恆成立。

〔玩鎖・玩索〕

此題是大學推甄申請入學考題，從以下的恆等式找答題線索：

$$(-a)^2=a^2\text{，}(a+bi)^4=(-b+ai)^4。$$

動手玩數學~破解秘笈 第20期

遊戲 77

當 $a-b=a+b$ 時，解得 $b=0$，此時 $\frac{a}{b}$ 無意義，不合。因此，三個相同數值的數只有

$$a+b=ab=\frac{a}{b}\cdots\cdots①$$

或

$$a-b=ab=\frac{a}{b}\cdots\cdots②$$

兩種情形。由 $ab=\frac{a}{b}$ 得到 $a\left(b^2-1\right)=0$，即 $a=0$ 或 $b=\pm1$，而當 $a=0$ 時，無論哪一種都推得 $b=0$（不合）。

(1) 當 $b=1$ 時，由第一式得 $a+1=a$（不合）；由第二式得 $a-1=a$（不合）。

(2) 當 $b=-1$ 時，由第一式得 $a-1=-a$，即 $(a,b)=\left(\frac{1}{2},-1\right)$；由第二式得 $a+1=-a$，即 $(a,b)=\left(-\frac{1}{2},-1\right)$。

綜合得到兩組解

$$(a,b)=\left(\frac{1}{2},-1\right)\text{或}\left(-\frac{1}{2},-1\right)。$$

遊戲 78

由餘弦定理知：以 a 、 b 、 c 為邊長，且 $\angle C=45°$ 的三角形，邊長 c 會滿足

$c^2=a^2+b^2-2ab\cos45°=a^2-\sqrt{2}ab+b^2$，

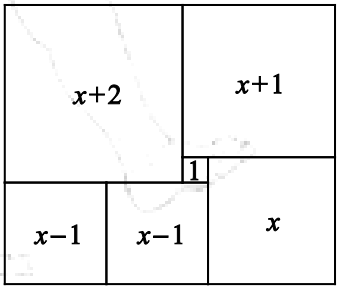
即

$$c=\sqrt{a^2-\sqrt{2}ab+b^2}\ 。$$

因此，根據餘弦定理，作一個 45° 夾角的射線，在射線兩邊各取長度為 a 與 b 的線段，再將兩線段端點連接，此連接的線段長度為所求。

遊戲 79

設右下角的正方形之邊長為 x，依逆時針與順時針方向考慮其餘正方形的邊長，可以得到下圖中央的數字（此中央的數字代表該正方形的邊長）：



由下邊的寬 $(x-1)+(x-1)+x$ 與上邊的寬 $(x+2)+(x+1)$ 必須相等，得

$(x-1)+(x-1)+x=(x+2)+(x+1)$，

解得 $x=5$。故長方形的寬 13，高 11，面積 143。

遊戲 80

設多項式 x^2-7x+4 的兩個根為 α 與 β。根據題意，甲、乙兩個正方形的邊長分別為 $\sqrt{\alpha}$ 與 $\sqrt{\beta}$（或者相反）。因此，剛好包住甲、乙兩個正方形的正方形之邊長為

$$\sqrt{\alpha}+\sqrt{\beta}\ ,$$

而面積為

$$\left(\sqrt{\alpha}+\sqrt{\beta}\right)^2=(\alpha+\beta)+2\sqrt{\alpha\beta}\ 。$$

利用根與係數的關係，我們知道

$$\alpha+\beta=7\ ,\ \alpha\beta=4\ 。$$

故剛好包住甲、乙兩個正方形的正方形之面積為

$$7+2\sqrt{4}=11\ 。$$