數不盡的質數

許介彥
大葉大學　電信工程學系

質數與合數

12 可以寫成兩個小於 12 的正整數相乘，如 $3\cdot4$ 或 $2\cdot6$ 等，而 7 卻無法寫成兩個小於 7 的正整數相乘。當一個正整數不能寫成比本身還小的兩個正整數相乘，我們稱此數為「質數」(prime number)；反之，如果某個正整數可以寫成兩個比本身還小的正整數相乘，也就是說，如果它除了 1 及本身之外還有其他的正因數，我們稱它為「合成數」或「合數」(composite number)；因此 7 是質數，而 12 是合數。

由於 1 的情況較特殊，數學上通常不將 1 歸類為質數，但是 1 當然也不是合數，因此最小的質數是 2，它是所有的質數中唯一的偶數，也是所有偶數中唯一的質數；由 2 開始的質數由小而大依序為 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …。

任何一個大於 1 的整數若本身不是質數的話一定可以經由持續的因數分解而寫成一些質數的乘積，例如 $6 = 2\cdot3$ 而 2 與 3 都是質數，$30 = 5\cdot6 = 5\cdot2\cdot3$ 而 5、2、3 都是質數等；同樣地，$24 = 3\cdot8 = 3\cdot2\cdot4 = 3\cdot2\cdot2\cdot2$，因此 24 可以拆成四個質數相乘，其中有一個 3 及三個 2。

對加法而言，構成正整數最基本的單位只有一個，就是數字 1，因為任何正整數都可以由一些 1 相加而得，而 1 不能寫成另外兩個正整數相加。對乘法而言，構成正整數最基本的單位為質數，因為任何大於 1 的正整數都可以由一些質數相乘而得，而每個質數都不能寫成另外兩個正整數相乘。相較於加法時的基本單位只有一個，乘法時的基本單位（也就是質數）有幾個呢？

質數的個數

正整數的個數有無窮多個，其中除了 1 以外，每個正整數若非質數即是合數，我們由此可以推斷在質數與合數這兩大類中至少會有一類包含了無窮多個數。合數的個數很顯然有無窮多個（例如所有 4 的倍數都是合數），於是我們很自然地要問：質數的個數也有無窮多個嗎？或者是有限的？也就是說，是否存在著一個「最大的質數」，所有比此數大的整數都是合數？早在西元前三世紀，希臘大數學家歐幾里得（Euclid）在他的名著《幾何原本》（*Elements*）中對這個問題就提出了解答，他証明了質數的個數是無限的；他的証明方式堪稱數學論證的經典之作，雖已歷經兩千多年仍不減其光芒。

歐幾里得的証明

基於對數字的了解，我們知道如果將 3 的任何一個倍數加 1，結果一定不會是 3 的倍數，例如 $7 = 3\cdot2+1$ 與 $16 = 3\cdot5+1$ 都不是 3

的倍數。同樣地，我們也可以肯定如果將 5 的任何一個倍數加 1，結果一定不會是 5 的倍數；由此又可推知如果將 15（$=3\cdot5$）的任何一個倍數加 1，結果一定既不是 3 的倍數也不是 5 的倍數。有了以上概念後，我們接著看下面幾個式子：

$$2\cdot3+1=7$$

$$2\cdot3\cdot5+1=31$$

$$2\cdot3\cdot5\cdot7+1=211$$

$$2\cdot3\cdot5\cdot7\cdot11+1=2311$$

$$2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031$$

這些式子都是計算由 2 開始由小而大連續幾個質數相乘的結果再加 1 的值，因此每個式子等號右邊算出來的數一定不會是該式等號左邊所用到的任何一個質數的倍數；例如 31 一定不是 2 或 3 或 5 的倍數，而 2311 一定不是 2 或 3 或 5 或 7 或 11 的倍數等。

上面這些式子算出來的 7、31、211、2311 其實都是質數，不過 30031 並不是質數。即使我們一下子看不出來 30031 除了 1 及本身之外還有哪些因數，我們卻可以肯定 30031 除了 1 以外的所有因數（包含「質因數」）一定全都大於 13，因為所有小於或等於 13 的質數都不是 30031 的因數。事實上，$30031=59\cdot509$，而 59 和 509 都是質數而且確實都大於 13。

要証明質數的個數有無窮多個，其實只要將上述概念一般化就可以了。假設 p 是任意一個質數，我們令

$$N=2\cdot3\cdot5\cdot7\cdot11\cdots p+1$$

N 顯然會比 p 大，而且所有小於或等於 p 的質數都不會是 N 的因數。

N 有兩種可能，其一是 N 本身就是一個質數（比 p 大的質數），另一種可能是 N 不是質數，不過它的所有的質因數都比 p 大；不管是哪一種情形，我們都証明了不管 p 有多大，一定有比 p 更大的質數存在，因此質數的個數是無限的。

請讀者留意上面的論述重點是要証明有比 p 大的質數「存在」，只要能夠証明其存在就足以說明質數個數的無限，我們並沒有（事實上也不需要）透過實際找出比 p 大的下一個質數或是任何一個比 p 大的質數來說明有比 p 大的質數存在（因此上述証明屬於 nonconstructive proof）。

目前世界上已知的質數中最大的數發現於 2001 年 11 月，大小為

$$2^{13466917}-1$$

它總共有 4053946 個位數（十進制）；當然，它絕不是「最大的質數」。

質數間的間隙

上述証明過程巧妙地避開了求出比 p 大的下一個質數或是任何一個比 p 大的質數的問題，因為這是一個相當困難的問題；由於質數在數線上的分布極不規則，因此並沒有一個簡單的「公式」可以讓我們有系統地將不同的值代入來得出一個一個的質數。

質數分布的凌亂由質數間的間隙可見一斑；連續兩個質數之間的距離有時大有時小，最小為 1（2 與 3 差 1），有可能為 2（如 71 與 73），或是 4（如 37 與 41），或是 6（如 23 與 29）等；很明顯，相鄰的兩個質數的距離除了一開始的 1 之外全都是偶數，不過最

大是多少呢？以下我們將証明，連續兩個質數的距離可以任意大；說得更明確一點，對任意正整數 n，不管 n 有多大，在數線上一定可以找到連續 n 個整數而且它們每一個都是合數，由此可知一定存在著距離大於 n 的連續兩個質數。

以下的証明與歐幾里得的前述作法有密切的關連。首先，假設 p 是所有整數中大於 n 的第一個質數，接著考慮以下連續 n 個整數：

$$2\cdot3\cdot5\cdot7\cdot11\cdots p+2$$
$$2\cdot3\cdot5\cdot7\cdot11\cdots p+3$$
$$2\cdot3\cdot5\cdot7\cdot11\cdots p+4$$
$$\vdots$$
$$2\cdot3\cdot5\cdot7\cdot11\cdots p+(n+1)$$

這 n 個數都具有如 $2\cdot3\cdot5\cdot7\cdot11\cdots p+k$ 的形式，其中 $2\le k\le(n+1)\le p$，因此 k 的所有質因數必定都小於或等於 p，所以 $2\cdot3\cdot5\cdot7\cdot11\cdots p+k$ 必為合數，也就是上面的 n 個連續整數全部都是合數，我們因此証明了有距離大於 n 的連續兩個質數「存在」。

這個問題的另一個可能的証明方式是利用

$$(n+1)!+2$$
$$(n+1)!+3$$
$$(n+1)!+4$$
$$\vdots$$
$$(n+1)!+(n+1)$$

等 n 個數都是合數（很明顯可看出）來說明有距離大於 n 的連續兩個質數存在。

與歐幾里得的証明一樣，我們在上述証明過程中並沒有（也不需要）真的找出符合要求的兩個質數。

等差數列中的質數

等差數列 a，$a+d$，$a+2d$，…中總共包含了多少個質數？這個問題的答案很顯然和 a 與 d 的值有關，例如等差數列 3, 6, 9, 12, 15, 18, …中，3 是唯一的質數，而等差數列 2, 5, 8, 11, 14, 17, …中的質數個數很明顯較多；有多少個呢？這個問題在西元 1837 年由德國數學家狄利克雷（G. Lejeune Dirichlet，1805-1859）提出了解答，他証明了只要 a 與 d 互質（即 a 與 d 的最大公因數為 1），等差數列 a，$a+d$，$a+2d$，…中必定含有無窮多個質數（此定理通常稱為狄利克雷定理）。他的証明方式相當複雜，本文不予討論，不過對某些特殊的 a 與 d 的值所形成的數列，我們卻不難証明其中含有無窮多個質數；以下我們來看兩個例子。

例題一：

證明等差數列 2, 5, 8, 11, …中包含了無窮多個質數。

解：

整數可以分成三種，一種是能被 3 整除的數，一種是除以 3 餘 1 的數，一種是除以 3 餘 2 的數；題目中的數列即是由所有除以 3 餘 2 的正整數組成的。

一個除以 3 餘 2 的數一定不會是 3 的倍數；它可能是一個質數，也可能不是質數；如果不是質數，那麼它的質因數一定不會全部都是除以 3 餘 1 的質數（也就是說，它必有至少一個除以 3 餘 2 的質因數），因為兩個除以 3 餘 1 的數相乘的結果除以 3 一定餘 1：

$$(3x+1)(3y+1)=9xy+3x+3y+1$$
$$=3(3xy+x+y)+1$$

假設 p 是等差數列 2, 5, 8, 11, …中任意一個大於 2 的質數；我們再次採用與歐幾里得類似的作法，令

$$M=2\cdot3\cdot5\cdot7\cdot11\cdots p-1$$

由於 M 是 3 的倍數減 1，因此 M 除以 3 一定餘 2。我們還可以肯定所有小於或等於 p 的質數都不是 M 的因數。

M 有兩種可能，其一是 M 本身就是一個質數（比 p 大而且是一個除以 3 餘 2 的質數），另一種可能是 M 不是質數，不過它的所有質因數都大於 p；由於 M 一定有除以 3 餘 2 的質因數，因此 M 一定有大於 p 且除以 3 餘 2 的質因數。不管是哪一種情形，我們都証明了不管 p 有多大，在數列 2, 5, 8, 11, …中一定有比 p 更大的質數存在，因此該數列中的質數個數是無限的。

例題二：

證明等差數列 3, 7, 11, 15, …中包含了無窮多個質數。

解：

題目中的數列是由所有除以 4 餘 3 的正整數組成的。一個除以 4 餘 3 的數可能是一個質數，也可能不是質數；如果不是質數，那麼它的質因數一定不會全部都是除以 4 餘 1 的質數（也就是說，它必有至少一個除以 4 餘 3 的質因數），因為兩個除以 4 餘 1 的數相乘的結果除以 4 一定餘 1，不可能餘 3。

假設 p 是等差數列 3, 7, 11, 15, …中的任意一個質數；我們再次採用與歐幾里得類似的作法，令

$$K=4(2\cdot3\cdot5\cdot7\cdot11\cdots p)-1$$

由於 K 是 4 的倍數減 1，因此 K 除以 4 一定餘 3。我們還可以肯定所有小於或等於 p 的質數都不是 K 的因數。

K 有兩種可能，其一是 K 本身就是一個質數（比 p 大而且是一個除以 4 餘 3 的質數），另一種可能是 K 不是質數，不過它的所有質因數都大於 p，因此 K 有大於 p 而且除以 4 餘 3 的質因數；不管是哪一種情形，我們都証明了不管 p 有多大，在數列 3, 7, 11, 15, …中一定有比 p 更大的質數存在，因此該數列中的質數個數是無限的。

細心的讀者也許已經發覺，除了將 K 設為 $4(2\cdot3\cdot5\cdot7\cdot11\cdots p)-1$ 之外，其實還有許多可能，如

$$K=2(2\cdot3\cdot5\cdot7\cdot11\cdots p)-1$$
$$K=4(3\cdot5\cdot7\cdot9\cdot11\cdots p)-1$$
$$K=4(3\cdot7\cdot11\cdot15\cdot19\cdots p)-1$$
$$K=2(p!)-1$$

等，也都是可行的。簡單來說，如果某數 A 是 4 的倍數，而且所有不大於 p 且除以 4 餘 3 的質數都是 A 的因數，那麼

$$K=A-1$$

就可以用於上述証明。

讀者不難看出，正整數中有無窮多個質數的性質其實是狄利克雷定理在 $a=d=1$ 時的特例。

兩個有趣的應用

前面幾個証明都利用了相似的觀念來証明某個或某些質數存在的必然性，以下我們再看這個觀念的兩個應用。

應用一：

求証：對任意大於 2 的整數 n 而言，在 n 與 $n!$ 之間必有質數存在。

這個問題只要能抓到關鍵的話其實很容易。對任意大於 2 的整數 n，很顯然所有小於或等於 n 的質數都不會是 $n!-1$的因數，因此 $n!-1$必定有大於 n 的質因數，所以 n 與 $n!$ 之間必有質數存在。

應用二：

以下方法可以用來「製造」出新的質數。假設我們將最小的 n 個質數 2, 3, 5, …, p_n 任意分成兩組，然後將各組中的質數相乘以得出兩個數 A 與 B（如果某一組不含任何質數的話就將其所含質數的乘積當作是 1)。求証：若 $A+B<p_{n+1}^2$，則 $A+B$ 必為質數；若 $|A-B|<p_{n+1}^2$，則 $|A-B|$ 必為質數。

舉例來說，如果我們將 2, 3, 5, 7, 11 等最小的五個質數分成 (3,11) 與 (2,5,7) 兩組，算出 $A=3\cdot 11=33$ 與 $B=2\cdot 5\cdot 7=70$，那麼 $A+B=103$ 與 $|A-B|=37$ 的值都小於 $13^2=169$，而 103 與 37 確實都是質數。如果分成的兩組是 (2,7) 與 (3,5,11)，那麼 $A+B=179$，$|A-B|=151$，此時只有 151 小於 13^2，而 151 也確實是質數。繼續往下看之前，讀者不妨先想一想原因何在。

道理並不難。每一個小於或等於 p_n 的質數一定能而且只能整除 A 與 B 其中之一，因此一定不能整除 $A+B$ 或 $|A-B|$；對 $A+B$ 與 $|A-B|$ 的任一數而言有兩種可能，其一是它本身就是一個質數，另一種可能是它不是質數，不過它的所有質因數（每個合數有至少兩個質因數）都大於 p_n，此時它的值必定不會小於 p_{n+1}^2，而這種情況已經被題目所述的條件排除了，因此滿足題目限制的 $A+B$ 與 $|A-B|$ 一定是質數；這裡所運用的其實是我們在中學學過的「如果所有小於或等於 $\sqrt{n}$ 的質數都不是 n 的因數，則 n 必為質數」的觀念。

結語

「數論」（Number Theory）是數學的一個分支，專門研究數（尤其是正整數）的性質，在所有數學領域中有最悠久的歷史，可以說是最「純」的數學，常被暱稱為「數學中的皇后」（the Queen of Mathematics）。

與數學的其他領域比較起來，數論的特點之一是它有許多問題看似簡單，其實卻很難；有些問題的題目簡單得連小學生都看得懂，但是卻能讓數學家窮畢生之力都無法解決；最有名的例子當屬費瑪最後定理（Fermat's Last Theorem）的証明，這個定理是說方程式 $x^n+y^n=z^n$ 在 n 為大於 2 的整數時沒有正整數解；費瑪（Pierre de Fermat, 1601-1665）只簡短地描述了這個性質而沒有提供証明，後世數學家雖然大多相信這個未經証明的「定理」是對的，長久以來卻苦於找不到証明的方法；一直到 1995 年，這個三百多年來困擾了一代又一代頂尖數學家的超級難題才由任教於普林斯頓大學的 Andrew Wiles 予以解決。

除了等差數列外，是否還有其他「簡單」的數列也包含著無窮多個質數？舉例來說，由形如 n^2+1 的數，或形如 2^n-1 或 $n!+1$ 的數形成的數列中是否包含著無窮多個質數？這

種看似簡單的問題常很難回答，有些問題到目前為止在學術界還沒有確切的答案。

在 n 與 $n!$ 之間存有質數似乎不足為奇，因為隨著 n 的遞增，$n!$ 增大的速度相當快；當 $n=3$ 時，$n!$ 為 6，而當 $n=10$ 時，$n!$ 已經大到 3628800；因此以上對質數落點的預測是相當粗糙的；在 n 與 $n!$ 之間不僅有質數，而且常有數量龐大的質數。

俄國數學家柴比雪夫（P. L. Chebyshev, 1821-1894）於西元 1850 年証明了對任意大於 1 的整數 n，在 n 與 $2n$ 之間必有質數存在。對較大的 n 而言，$2n$ 當然比 $n!$ 小得多，因此這是對質數分布較準確的估計，不過其証明方式不同於本文所述的方式。

由於數論所探討的對象是正整數，是最「自然」的數，因此對一般人而言特別容易親近，也特別容易感受其中的美妙。儘管經過了數千年的研究，數論中仍有許多問題長久以來懸而未決，答案僅止於人們的「猜想」（conjectures）；沒有人可以肯定這些謎團最終能不能被解開，但是我們可以肯定數論一定會持續為現代及未來的數學家及業餘的數學愛好者提供源源不絕的研究題材。

練習題

以下是幾個與本文內容相關的問題，提供讀者參考。

1. 證明等差數列 5, 11, 17, 23, 29, …中包含了無窮多個質數。
2. 証明對任意一個大於 1 的正整數 n 而言，n^4+4 必為合數。
3. 証明 $2^{2002}+1$ 與 $2^{2002}-1$ 都不是質數。
4. 証明末四位數為 0003 的質數有無窮多個。
5. 例題二中如果令

   $K=4(2\cdot 3\cdot 5\cdot 7\cdot 11\cdots p)+3$

   可不可行？
6. 某數列 $a_1, a_2, a_3, \cdots$ 以遞迴的方式定義如下：

$$a_{n+1}=\begin{cases}2 & n=0\\ a_n^2-a_n+1 & n>0\end{cases}$$

證明此數列中任意兩項皆互質。（提示：$a_n^2-a_n=a_n(a_n-1)$）

參考資料

1. C. V. Eynden, *Elementary Number Theory*, 2nd edition, McGraw-Hill, 2001.
2. K. H. Rosen, *Elementary Number Theory And Its Applications*, 4th edition, Addison-Wesley, 1999.

作者信箱：chsu@mail.dyu.edu.tw