P＝4n－1與P＝4n＋1

李恭晴

一、引言

歐幾里德在兩仟多年以前就已經證明了質數有無限多個這個事實（見本文第3節）。這無限多個質數中，除了2是偶數以外，其餘的質數都是奇數。因此它們必定分佈在下列兩個等差數列之中：

$3, 7, 11, 15, \cdots, 4n-1, \cdots\cdots$

$1, 5, 9, 13, \cdots, 4n+1, \cdots\cdots$

歐幾里德的證明即使以現在的眼光來看，仍然是非常精巧完美的。本文主要的目的就是要仿照他的證明方法，來證明上列兩個等差數列中，也各有無限多個質數存在。也就是要證明具有$4n-1$形式及具有$4n+1$形式之質數各有無限多個。

二、預備知識

假設a和b是兩個整數，且$a \neq 0$。如果有一個整數q存在，使得$aq=b$，那麼我們就稱a爲b的因數，b爲a的倍數，並且以$a \mid b$表示。如果a不是b的因數，那麼就以$a \nmid b$表示。

若a爲b的因數，並且a也是c的因數，我們稱a爲b與c的公因數。由於1是任何整數的因數，所以任意兩個整數必有一個公因數1。若兩個整數除了1這個公因數之外沒有其他正的公因數，我們就稱這兩個數互質。

若$a \mid b$且$a \mid c$，則我們可以找到兩個整數q與q'，使得$aq=b$且$aq'=c$。因此$a(q-q')=b-c$，由此可知

$$a \mid (b-c)$$

其次，若$b-c$是a的倍數，k爲任意一個正整數，則由恒等式

$$b^k-c^k=(b-c)(b^{k-1}+b^{k-2}c+\cdots\cdots+bc^{k-2}+c^{k-1})$$

可知b^k-c^k也是a的倍數。換句話說，由$a \mid (b-c)$可以推得$a \mid (b^k-c^k)$對於所有的正整數k都成立。

顯然地，除了1以外，每一個正整數n最少都有兩個正的因數，就是1與n本身。例如2恰有兩個正的因數，即1與2；4有三個正的因數，即1，2與4；21有四個因數，即1，3，7與21。一個正整數如果剛好只有兩個正的因數時，我們就稱這個數爲質數，下列是從小算起的一些質數：

2，3，5，7，11，13，17，19，23，29，31，37，……

如果正整數n有三個以上的正的因數時，我們就稱n這個數爲合成數。例如

4，6，8，9，10，12，14，15，16，18，20，21，……

都是合成數。顯然每一個合成數都可以分解爲質數的乘積。因此，除了1以外，每一個正整數最少都有一個質數因數，這種質數因數我們簡稱爲質因數。

三、歐幾里德定理

歐幾里德是採用歸謬證法以證明質數有無限多個。他首先假設質數只有有限多個，令其爲$p_1, p_2, \cdots, p_r$等r個，他將“全部”的這些質數相乘以後再加1，而得到一個數，令這個數爲N，即

$$N=p_1p_2\cdots p_r+1$$

則N最少有一個質因數（因爲$N>1$），令其中

一個質因數爲 p，由於 p_1，p_2，……，p_r 都不是N的因數，所以 p 不等於 p_1，p_2，…，p_r 中的任何一個。換句話說，除了 p_1，p_2，……，p_r 外，我們還可以再找出一個質數 p。此與假設質數只有 p_1，p_2，…，p_r 等 r 個矛盾。所以質數有無限多個。

四、P＝4n－1

現在利用歐幾里德的證明方法來證明等差數列 3，7，11，15，…，$4n-1$，…
中有無限多個質數，也就是證明具有 $4n-1$ 形式的質數有無限多個。由於 $(4n+1)(4m+1)=4(4nm+n+m)+1=4k+1$，其中 $k=4nm+n+m$ 爲一整數，所以我們知道任意兩個 $4n+1$ 形式的數相乘，它的乘積也必定仍然具有 $4n+1$ 這種形式。

如果N是一個具有 $4n-1$ 之形式的正整數，則它的質因數中不可能全部都具有 $4n+1$ 之形式，否則其乘積N就必定是 $4n+1$ 之形式而不是 $4n-1$ 之形式。又因爲N是奇數，所以N的所有的質因數必定都是奇數，因此可知N有一個奇數的質因數 p 不是 $4n+1$ 之形式，它是 $4n-1$ 之形式。由上列之討論可得：若正整數N具有 $4n-1$ 之形式，則N最少有一個質因數也具有 $4n-1$ 之形式。

現在假設具有 $4n-1$ 形式之質數只有有限多個，令其爲 p_1，p_2，…，p_r，即假設具有 $4n-1$ 形式之質數只有 p_1，p_2，…，p_r 等 r 個。選取

$$N=4p_1p_2\cdots p_r-1$$

則N具有 $4n-1$ 之形式，因此N最少有一質因數 p 具有 $4n-1$ 之形式。由於 p_1，p_2，…，p_r 都不是N的因數，所以 p 不等於 p_1，p_2，…，p_r 中的任何一個。因此，除了 p_1，p_2，…，p_r 外，我們又找到另一個具有 $4n-1$ 形式的質數 p，此與假設矛盾，所以具有 $4n-1$ 形式之質數有無限多個。

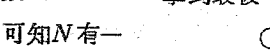
利用相似的討論也可以證明具有 $6n-1$ 形式的質數也有無限多個，我們將它留給讀者作練習。

五、Fermat定理

要證明具有 $4n+1$ 形式之質數有無限多個，其原理也是相同的，只是它必須要用到所謂的 Fermat 定理：若 p 爲質數，n 爲任意正整數，則 $p\mid(n^p-n)$。

由於 n^p 與 n 同爲奇數或同爲偶數，所以，當 p 等於 2 時 Fermat 定理顯然成立。對於大於 2 的質數 p，我們以排列加以說明如下：

假設我們有 n 種不同顏色的球，每一種顏色的球都有相當多個（例如多於 p 個）。若從這些色球中每次取出 p 個排成一列，則因同顏色的球可以重複選取，因此全部共有 n^p 種不同的排列方法。在這 n^p 種不同的排法中，有 n 種排法是整排 p 個球都是同顏色的，除此之外，剩下的 n^p-n 種排法中，對於每種排法，每次我們將第一個球拿到最後一個，則可構成另一種排法。例如



經拿動一次以後變成

再拿動一次以後變成

等等。這些新的排法和原來的排法是否會相同呢？爲了回答這個問題，我們假設拿動 k 次以後會與原來的排法相同，而且最少要拿動 k 次以後才會和原來的排法相同。顯然 $1<k\leq p$。以 k 除 p，令其商爲 q，餘數爲 r，則有

$$p=qk+r \text{ 且 } 0\leq r<k$$

由於拿動 k 次以後的排法和原來的排法一樣，所以拿動 k 次以後再拿動 k 次就相當於只有拿動 k 次一樣。因此拿動 $2k$ 次以後的排列也和原來的排列法相同。同樣的道理，拿動 $3k$ 次，$4k$ 次，…等等都與原來的排列法相同。特別地，拿動 $(q+1)k$ 次以後的排列也是與原來的排列相同。

但是

$$(q+1)k=qk+k=qk+r+(k-r)$$
$$=p+(k-r)$$

所以拿動 $(q+1)k$ 次就相當於只有拿動 $k-r$ 次。它們的排列都與原來的排列相同。即拿動 $k-r$ 次以後的排列與原來的排列相同。又因爲 $0<k-r\leqslant k$，且由 k 之選取知最少要拿動 k 次才會和原來的排法相同，所以 $k-r=k$，即 $r=0$。由此可得 $p=qk$，故 $k\mid p$。又因 p 爲質數，且 $1<k\leq p$，所以 $k=p$。

換句話說，最少要拿動 p 次以後才會和原來的排法一樣。因此對於每一種排法，我們都可以依照上列的方法依次拿動 1 次，2 次，…，$(p-1)$ 次，而得到總共 p 種不同的直線排列法（包括原來的一種）。這 p 種不同的直線排列法如果依照順時鐘方向的順序排成環狀排列時，都是同一種環狀排列。由此可知，每 p 種上列這種直線排列可以化爲一種環狀排列。全部有 n^p-n 種直線排列，即可化爲 $\frac{n^p-n}{p}$ 種環狀排列，它是一個整數。因此得知 $p\mid(n^p-n)$，而 Fermat 定理即得到證明。

如果 n 與 p 互質，則可將關係式 $p\mid(n^p-n)$ 右邊的因數 n 消去而得 $p\mid(n^{p-1}-1)$，此爲 Fermat 定理的另一種形式。

六、P＝4n＋1

要證明具有 $4n+1$ 形式之質數有無限多個，我們只要證明對於任意整數 $m>1$，必可找到一個比 m 大的質數具有 $4n+1$ 之形式即可。因爲具有 $4n+1$ 形式之質數如果只有有限多個。假設爲 p_1，p_2，…，p_r 等 r 個，令 m 爲 p_1，p_2，…，p_r 中最大的一個，則我們又可以找到一個比 m 大的質數 p 具有 $4n+1$ 之形式，這就得到一個矛盾的結果。所以只要能證明對於每一個 $m>1$ 都可找到一個比 m 大的質數 p 具有 $4n+1$ 之形式，即可得知具有 $4n+1$ 形式之質數有無限多個。

現在我們來證明：對於每一個整數 $m>1$，必可找到一個比 m 大的質數 p 具有 $4n+1$ 之形式。我們令

$$N=(m!)^2+1$$

其中 $m!$ 表示 $1\cdot2\cdot3\cdot\cdots\cdot m$，並且令 p 爲 N 之最小的質因數。由於 $\leq m$ 的正整數都可以整除 $(m!)^2$，所以不會是 $N=(m!)^2+1$ 的因數，既然 p 是 N 的因數，p 必不是 $\leq m$ 的正整數，因此得到 $p>m$。另外，由 $p\mid N$ 可得

$$p\mid(m!)^2-(-1)$$

利用第 2 節中的性質，我們將 $(m!)^2$ 及 (-1) 自乘 $\frac{p-1}{2}$ 次而得

$$p\mid((m!)^2)^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{2}}$$

或

$$p\mid(m!)^{p-1}-(-1)^{\frac{p-1}{2}}$$

又由 Fermat 定理的第二種形式知

$$p\mid(m!)^{p-1}-1$$

上列兩個關係式的右邊相減，得

$$p\mid 1-(-1)^{\frac{p-1}{2}}$$

但是 $1-(-1)^{\frac{p-1}{2}}=0$ 或 2，而 p 爲奇質數（因爲 N 爲奇數，所以它的質因數都是奇數），故得

$$1-(-1)^{\frac{p-1}{2}}=0$$

或

$$(-1)^{\frac{p-1}{2}}=1$$

由此可知 $\frac{p-1}{2}$ 爲偶數，令其等於 $2n$，則得 $p=4n+1$。因此我們證得：對於每一個整數 $m>1$，恒可找到一個 $4n+1$ 形式之質數 $p>m$。所以，具有 $4n+1$ 形式之質數有無限多個。

（下接44頁）

3. 研討有關教材與教法之疑難問題。

㈡時間分配：

分區	日期	主辦學校	參加研討人員
北區	67年10月下旬	台北市立和平國民中學	分區內各實驗學校數學科實驗教師，每校兩名。
	67年12月下旬	台北市立大同國民中學	
	68年 3 月下旬	台北市立華江國民中學	
	68年 5 月下旬	台北縣立重慶國民中學	
中區	67年10月中旬	新竹縣立建華國民中學	同上。
	67年12月中旬	台中縣立豐原國民中學	
	68年 3 月中旬	雲林縣立土庫國民中學	
	68年 5 月中旬	新竹縣立建華國民中學	
南區	67年10月上旬	台南市立大成國民中學	同上。
	67年12月上旬	高雄市立苓雅國民中學	
	68年 3 月上旬	台南市立大成國民中學	
	68年 5 月上旬	高雄市立苓雅國民中學	
東區	67年11月中旬	花蓮縣立花崗國民中學	同上。
	68年 4 月中旬	花蓮縣立花崗國民中學	

㈢主辦學校之職責：

1. 在舉辦教學研討會前十天發出書面通知邀請有關人員參加研討，其對象包括：(1)師大科教中心，(2)各實驗學校，(3)教育部國教司及該主辦學校所在地之縣市教育局。

2. 安排研討會一切場地及用具，研討會活動內容原則如下：

時間	活動內容	主持人
9:00～ 9:50	教學觀摩	實驗教師
10:00～11:30	教學研討會	實驗學校校長

3. 將研討會記錄整理妥當，在會後兩週內寄達師大科教中心，其餘各實驗學校、教育部國教司及各該縣市教育局。

（上接32頁，$P=4n-1$ 與 $P=4n+1$）

七、結語

利用歐幾里德的方法，我們還可以證明其他一些等差數列中有無限多個質數，例如等差數列

$$4, 9, 14, \cdots, 5n-1, \cdots$$
$$7, 15, 23, \cdots, 8n-1, \cdots$$
$$5, 13, 21, \cdots, 8n-3, \cdots$$
$$3, 11, 19, \cdots, 8n+3, \cdots$$

等等。但是到現在還沒有人能夠仿照他的方法證明一般的等差數列中也都有無限多個質數。我們只能夠利用解析的方法才能證明它，這就是所謂的Dirichlet定理：在首項與公差互質的無窮等差數列中（各項皆爲正整數），必有無限多個質數。對於Dirichlet定理的解析證法有興趣的讀者，可以參看「數論導引」一書或其他有關的解析數論方面的書籍。

〔作者現職：國立臺灣師範大學數學研究所所長〕

（上接34頁，合成函數的一種幾何表現）

(1)當 $f(x_0)$ 爲極大值〔極小值〕且 $g'(y)$ 恒正時，則 $g\circ f(x_0)$ 爲極大值〔極小值〕。

(2)當 $f'(x)$ 恒正且 g 在 $f(x_0)$ 爲極大值〔極小值〕時，則 $g\circ f(x_0)$ 爲極大值〔極小值〕。

參考資料

〔1〕 陳昭地、顏啓麟合著，數學分析，汝旭圖書有限公司發行，第二版，1978。

〔2〕 Smith, W.K., Inverse Functions, The Macmillan Company, New York, 第三版, 1967。

〔3〕 Swokowski, Calculus with Analytic Geometry, 協進圖書有限公司發行，1977。

〔作者現職：國立臺灣師範大學數學系副教授〕