

Farey 數列與 $P=4n+1$

李恭晴

一、引言

在本刊第二十三期中，我們曾經利用排列數證明了具有 $4n+1$ 之形式的質數有無限多個，現在我們要利用 Farey 數列來證明它，這兩種證明方法雖然並不相同，但是所得出的結果則一致。從比較它們的證明過程中，也可以看出數學結構之優美。

二、預備知識

若 a 與 b 都是整數，且 $b > 0$ ，我們稱 $\frac{a}{b}$ 為一個分數， a 是它的分子， b 是它的分母。如果一個分數的分子 a 與分母 b 的最大公因數為 1，即 $(a, b) = 1$ ，我們就稱 $\frac{a}{b}$ 為既約分數。若 $0 \leq \frac{a}{b} \leq 1$ 時，我們稱 $\frac{a}{b}$ 為真分數（一般真分數是指大於 0 且小於 1 的分數，在這裡為了敘述方便起見，我們將 $\frac{0}{1}$ 與 $\frac{1}{1}$ 也稱為真分數）。

三、Farey 數列

對於任意自然數 N ，我們將所有分母不大於 N 的既約真分數集合在一起，構成一個集合

$$\left\{ \frac{a}{b} : 0 \leq a \leq N, 1 \leq b \leq N, (a, b) = 1 \right\}$$

將這個集合的元素按其大小順序由小而大加以排列，則我們可以得到一個數列，稱為 N 階 Farey 數列，以 F_N 表示。例如：

當 $N = 3$ 時，我們得到三階 Farey 數列

$$F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$$

當 $N = 4$ 時，四階 Farey 數列為

$$F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$$

當 $N = 5$ 時，五階 Farey 數列為

$$F_5 : \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5},$$

$$\frac{1}{1}$$

……等等。

我們發現每一個 $N+1$ 階 Farey 數列 F_{N+1} 可由 N 階 Farey 數列 F_N 加上一些分數而得，它的加法是這樣的：若 F_N 中兩個連續項分母的和等於 $N+1$ ，則在這兩項之間加入一個分數，這個分數的分子為這兩項分子的和，而分母為這兩項分母的和（即 $N+1$ ）。如果連續兩項分母的大於 $N+1$ ，則這兩項之間就不必加進任何分數。例如在 F_4 中，第一、二兩項，第三、四兩項，第四、五兩項，第六、七兩項分母的和都是 5，所以這些項的中間分別要插進 $\frac{1}{5}, \frac{2}{5}, \frac{3}{5}$

$\frac{4}{5}$ ，而在第二、三項，第五、六項之間就不必插入分數，如此即可得到 F_5 。這些性質我們將在下面定理 1 中加以詳細的證明。

現在我們看一看每一個 Farey 數列的各項之間的關係，我們發現在每一個 Farey 數列中，連續兩項的分母必定都互質，並且後一個分數減去前一個分數，它的差的分子都等於 1。這是 Farey 數列的一個重要的性質。我們將以數學歸納法來證明它，並且利用它來證明一些有趣的結果。

定理 1：

設 $\frac{a}{b} < \frac{c}{d}$ 為 Farey 數列 F_N 中連續的兩項，

則 $bc - ad = 1$

並且由此得知

$$(b, d) = 1$$

證明：

當 $N = 1, 2, 3, 4, 5$ 時，我們很容易驗算得知定理成立。現在假設 Farey 數列 F_N 具有上列性質，我們將證明在 Farey 數列 F_{N+1} 中也具有上列性質。

假設 $\frac{a}{b} < \frac{c}{d}$ 為 F_N 中連續兩項，我們將證明在這兩個分數中間最多只有一個分數在 F_{N+1} 中，這個分數就是 $\frac{a+c}{b+d}$ （如果 $\frac{a+c}{b+d} \notin F_{N+1}$ ，則在 $\frac{a}{b}$ 與 $\frac{c}{d}$ 之間就沒有分數 $\in F_{N+1}$ ，此時 $\frac{a}{b}, \frac{c}{d}$ 也是 F_{N+1} 中連續的兩項）。

因為 $\frac{a}{b} < \frac{c}{d}$ 為 F_N 中連續兩項，所以由數學歸納法知

$$bc - ad = 1 \quad \text{且} \quad (b, d) = 1$$

現在，若 $\frac{\ell}{m} \in F_{b+a}$ ， $(\ell, m) = 1$ 且 $\frac{a}{b} < \frac{\ell}{m} < \frac{c}{d}$ ，我們令

$$\lambda = cm - d\ell$$

$$\mu = b\ell - am$$

則由簡單的計算即可得知

$$\lambda a + \mu c = \ell$$

$$\lambda b + \mu d = m$$

因此

$$\frac{\ell}{m} = \frac{\lambda a + \mu c}{\lambda b + \mu d}$$

又因為 $(\ell, m) = 1$ ，所以 $(\lambda, \mu) = 1$ 。我們由 λ 與 μ 的定義中可以看出 $\lambda > 0, \mu > 0$ 。

若 $\frac{\ell}{m} \in F_{b+a}$ ，則

$$\lambda b + \mu d \leq b + d,$$

又因 $\lambda > 0, \mu > 0$ 且 $(\lambda, \mu) = 1$ 故得

$$\lambda = 1 \quad \text{且} \quad \mu = 1$$

所以

$$\frac{\ell}{m} = \frac{a+c}{b+d}$$

至於 $\frac{a+c}{b+d}$ 是否屬於 F_{N+1} ，就必須視 $b+d = N+1$ 與否而定。

由此可知，在 F_N 中連續兩項 $\frac{a}{b} < \frac{c}{d}$ 之間最多只有一項 $\frac{a+c}{b+d} \in F_{N+1}$ （當 $b+d = N+1$ 時），若 $b+d > N+1$ ，則 $\frac{a}{b} < \frac{c}{d}$ 中間沒有 F_{N+1} 的項存在。

因為 $bc - ad = 1$ ，所以 $b(a+c) - a(b+d) = bc - ad = 1$ ，且 $(b+d)c - (a+c)d = bc - ad = 1$ 。由此得知定理在 F_{N+1} 時也成立。

四、利用 F_N 中分數的逼近

利用定理 1 我們可以將任意分數用 F_N 中的元素來加以逼近，使得它的誤差不會太大。

定理 2：

若 $\xi = \frac{\ell}{m}$ 為任一分數，則存在一個分數 $\frac{a}{b} \in F_N$ ，使得

$$\left| \xi - \frac{a}{b} \right| \leq \frac{1}{b(N+1)}$$

證明：

若 $\frac{\ell}{m} \in F_N$ ，則我們可以選取 $\frac{a}{b} = \frac{\ell}{m}$ ，而得

$$\left| \frac{\ell}{m} - \frac{a}{b} \right| = 0, \text{ 故定理成立。若 } \frac{\ell}{m} \notin F_N, \text{ 則}$$

$\frac{\ell}{m}$ 必在 F_N 中兩個連續項之間，設這兩項為 $\frac{a}{b}$ 與 $\frac{c}{d}$ 且 $\frac{a}{b} < \frac{c}{d}$ 。

若 $\frac{a}{b} < \frac{\ell}{m} \leq \frac{a+c}{b+d}$ ，則

$$\left| \frac{\ell}{m} - \frac{a}{b} \right| \leq \left| \frac{a+c}{b+d} - \frac{a}{b} \right| = \frac{bc-ad}{b(b+d)}$$

$$= \frac{1}{b(b+d)} \leq \frac{1}{b(N+1)}$$

若 $\frac{a+c}{b+d} < \frac{\ell}{m} < \frac{c}{d}$ ，則

$$\left| \frac{\ell}{m} - \frac{c}{d} \right| \leq \left| \frac{a+c}{b+d} - \frac{c}{d} \right| = \left| \frac{ad-bc}{d(b+d)} \right|$$

$$= \frac{1}{d(b+d)} \leq \frac{1}{d(N+1)}$$

所以定理得證。

五、表示成兩數的平方和

定理 3：

若 A 為任一整數且 $n \mid (A^2 + 1)$ ，則 n 必可寫成兩個整數的平方和。即存在兩個整數 b 與 c ，使得

$$n = b^2 + c^2$$

證明：

若 $n = 1$ ，則 n 顯然可以寫成 $n = 0^2 + 1^2$ 。因此可假設 $n \geq 2$ 。令 $N = [\sqrt{n}]$ 表示 $\leq \sqrt{n}$ 的最大整數。

對於 $\frac{A}{n}$ 這個分數，必存在一個分數 $\frac{a}{b} \in F_N$ ，

使得 $\left| \frac{A}{n} - \frac{a}{b} \right| \leq \frac{1}{b(N+1)}$

所以

$$|Ab - an| \leq \frac{n}{N+1} < \frac{n}{\sqrt{n}} = \sqrt{n}$$

因此

$$0 < b^2 + (Ab - an)^2 < N^2 + (\sqrt{n})^2 \leq 2n$$

即

$$0 < b^2 + (Ab - an)^2 < 2n$$

另一方面，

$$b^2 + (Ab - an)^2 = (1 + A^2)b^2 - 2Aabn + a^2n^2$$

為 n 的倍數（因為 $1 + A^2$ 是 n 的倍數）。所以

$$b^2 + (Ab - an)^2 = n$$

故 n 可寫成

$$n = b^2 + c^2$$

其中

$$c = |Ab - an|$$

六、 $P = 4n + 1$

現在我們可以證明

定理 4：

具有 $4n + 1$ 形式的質數有無限多個。

證明：

假設具有 $4n + 1$ 形式之質數只有有限多個

，設其為 $p_1, p_2, \dots, p_k$

令 $A = 2p_1 p_2 \dots p_k$ ，則 $A^2 + 1$ 必有一質因數，令其為 p 。首先我們注意到 $p \neq p_1, p \neq p_2, \dots, p \neq p_k$ ，這是因為 p 是 $A^2 + 1$ 的因數；而 $p_1, p_2, \dots, p_k$ 都不是 $A^2 + 1$ 的因數的緣故。其次我們證明 p 也具有 $4n + 1$ 之形式，如此即得到一個矛盾的結果。

因為 $p \mid A^2 + 1$ ，所以由定理 3 可知存在兩個整數 b 與 c ，使得 $p = b^2 + c^2$ 。又因為 p 為奇數（ A 是偶數，所以 $A^2 + 1$ 是奇數，其因數也必是奇數）。所以 b 與 c 之中必有一為偶數，另一為奇數。我們可設

$$b = 2h$$

$$c = 2\ell + 1$$

則

$$p = (2h)^2 + (2\ell + 1)^2 = 4(h^2 + \ell^2 + \ell) + 1$$

因此得證 p 也具有 $4n + 1$ 之形式（ $n = h^2 + \ell^2 + \ell + 1$ ）。

七、結語

在定理 4 的證明中，我們也可以令 $A = m$ ，其中 m 為任意自然數，並令 p 為 $A^2 + 1$ 之質因數，則不難證明 $p > m$ 且 p 具有 $4n + 1$ 之形式。因此，對於任意自然數 m ，必存在一個具有 $4n + 1$ 形式的質數 $p > m$ 。所以得知具有 $4n + 1$ 形式之質數有無限多個。

〔作者現職：國立臺灣師範大學數學研究所所長〕