詳細解答

STEP II 2002，第 3 題

純數學 • 費馬數與質數

> **STEP II 2002，第 3 題**
>
> 繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：
>
> step.maths.org/questions/02-s2-q3

本題在 *Beyond STEP* 第 1.1 節質數工廠中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch01/fermat-numbers.html

關鍵思路

寫出 $F_k - 2 = 2^{2^k} - 1$。把它乘以 $F_k = 2^{2^k} + 1$，便得到一個平方差（difference of two squares），而這正是歸納法（induction）所需要的那一步。乘積公式一旦成立，任何兩個費馬數（Fermat number）的公因數（common factor）都必須整除 2。由於每個費馬數都是奇數，這個因數只可能是 1。

解答

首四個費馬數

由於 $2^0 = 1$、$2^1 = 2$、$2^2 = 4$ 及 $2^3 = 8$，

$$F_0 = 2^1 + 1 = 3, \qquad F_1 = 2^2 + 1 = 5, \qquad F_2 = 2^4 + 1 = 17, \qquad F_3 = 2^8 + 1 = 257.$$

現在就 k 的首三個值驗證 $(*)$：

$$\begin{aligned} k = 1: &\quad F_0 = 3 = 5 - 2 = F_1 - 2, \\ k = 2: &\quad F_0 F_1 = 15 = 17 - 2 = F_2 - 2, \\ k = 3: &\quad F_0 F_1 F_2 = 15 \times 17 = 255 = 257 - 2 = F_3 - 2. \end{aligned}$$

證明 $(*)$ 對所有 $k \geq 1$ 成立

我們對 k 使用歸納法。$k = 1$ 的情況已在上面完成。

假設 $(*)$ 對某個 $k \geq 1$ 成立，即 $F_0 F_1 \cdots F_{k-1} = F_k - 2$。那麼

$$\begin{aligned} F_0 F_1 \cdots F_{k-1} F_k &= (F_k - 2)\, F_k \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) \\ &= \left(2^{2^k}\right)^2 - 1 \\ &= 2^{2 \cdot 2^k} - 1 = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2. \end{aligned}$$

所以 $(*)$ 對 $k+1$ 同樣成立，根據歸納法，它對每個 $k \geq 1$ 都成立。

想一想 為甚麼 $\left(2^{2^k}\right)^2$ 等於 $2^{2^{k+1}}$，而不是 $2^{2^{2k}}$ 或其他式子？

把一個冪平方，指數 (exponent) 便會加倍：$\left(2^a\right)^2 = 2^{2a}$。這裏 $a = 2^k$，而 $2a = 2 \cdot 2^k = 2^{k+1}$。歸納步驟的大部分工夫，就在於小心處理這類層層疊起的指數。

任何兩個費馬數都沒有公因數

取兩個不同的費馬數 F_m 和 F_n，其中 $m < n$。那麼 $n \geq 1$，而在 $k = n$ 時的 $(*)$ 中，F_m 是因數 $F_0, \ldots, F_{n-1}$ 的其中一個。所以

$$F_n - 2 = F_m \times (\text{某個整數}),$$

這表示 F_m 整除 $F_n - 2$。

現在假設正整數 d 同時整除 F_m 和 F_n。由於 $d \mid F_m$ 及 $F_m \mid F_n - 2$，我們有 $d \mid F_n - 2$。又由於 d 也整除 F_n，它便整除兩者之差：

$$d \mid F_n - (F_n - 2) = 2,$$

所以 $d = 1$ 或 $d = 2$。但 $F_m = 2^{2^m} + 1$ 是一個偶數加 1，所以是奇數（注意 $2^m \geq 1$）。因此 $d \neq 2$，從而 $d = 1$。由此可見，任何兩個費馬數都沒有大於 1 的公因數。

質數有無限多個

每個 F_n 都至少是 3，所以它至少有一個質因數（prime factor）。選取其中一個，稱它為 p_n。這樣，每個 $n = 0, 1, 2, \ldots$ 都對應一個質數。

想一想 兩個不同的費馬數會不會給出同一個質數？

不會。假如 $p_m = p_n$ 而 $m \neq n$，這個質數便會同時整除 F_m 和 F_n。它就成了一個大於 1 的公因數，而上一部分已排除了這個可能。所以質數 $p_0, p_1, p_2, \ldots$ 全部互不相同。由於費馬數有無限多個，互不相同的質數也有無限多個。

留意我們從來不需要 F_n 本身是質數，只需要每個費馬數都有某個質因數，是其他費馬數所沒有的。

驗算

- $k = 4$ 時的 $(*)$：$255 \times 257 = 65535 = 65537 - 2 = F_4 - 2$。我們亦用電腦以精確運算驗證了 $(*)$ 對直至 12 的所有 k 都成立。
- $F_0, \ldots, F_5$ 的最小質因數分別是 $3, 5, 17, 257, 65537, 641$，全部不同，正如論證所預測。$F_5 = 4294967297 = 641 \times 6700417$ 是第一個不是質數的費馬數。
- 我們以數值計算確認了對所有 $0 \leq m < n \leq 10$，都有 $\gcd(F_m, F_n) = 1$。

常見錯誤

- 把 2^{2^n} 讀成 $(2^2)^n = 4^n$。指數是 2^n，所以 $F_3 = 2^8 + 1$，而不是 $4^3 + 1$。
- 得出 $d \mid 2$ 之後，忘記排除 $d = 2$。正是「費馬數是奇數」這個事實，才令論證得以完成。
- 假設每個費馬數都是質數。最後一部分不需要這個假設，而且它根本是錯的（$641 \mid F_5$）。

STEP 之外

這個證明出自波利亞（Pólya）。它屬於「質數有無限多個」的一系列證明之一。這類證明都是構造一個兩兩互質（pairwise coprime）的無窮整數數列，於是每一項都貢獻一個屬於自己的新質數。歐幾里得（Euclid）的證明也可以這樣理解。費馬數在數論課程中還會再次出現：高斯（Gauss）證明了正 n 邊形可以用尺規作圖（ruler and compass construction），當且僅當 n 是 2 的冪乘以若干個互不相同的費馬質數（Fermat prime）之積，而至今仍未發現 F_4 之後的費馬質數。想了解更多，可閱讀 Davenport 的 *The Higher Arithmetic*（一本經典的數論入門書）。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。