1.1 質數工廠

工作紙

題目

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

提示

請先自行嘗試解題。如果遇到困難，請逐一閱讀提示，每讀完一個便回到題目再試。標有停一停，試一試的提示是關鍵步驟。每個提示之後均留有空位供你演算。

> **想一想**　最後一行問的是無窮多個質數，中間問的是公因數。「任何兩個費馬數（Fermat number）都沒有公因數」和「質數有無窮多個」之間，究竟有甚麼關係？

階段 1　感受一下這些數

涵蓋：首四個費馬數（Fermat numbers）

> **想一想**　留意這個指數塔（power tower）：2^{2^n} 的意思是 $2^{(2^n)}$。先就 $n = 0, 1, 2, 3$ 算出 2^n，然後才把 2 自乘至該次冪（power）。

階段 2 驗證恆等式（identity）

涵蓋：$(*)$ 在 $k = 1, 2, 3$ 時的情況

想一想 當 $k = 1, 2, 3$ 時，$(*)$ 的左方分別是一個、兩個和三個費馬數的乘積。逐一計算這些乘積，再與 $F_k - 2$ 比較。

階段 3　證明恆等式

涵蓋：$(*)$ 對所有 $k \geq 1$ 成立

想一想　歸納法（induction）是最自然的工具。若 $(*)$ 對 k 成立，你要把兩邊同時乘以甚麼，才能得到 $k+1$ 時的左方？

想一想　完成這一步之後，你需要證明 $(F_k - 2)\,F_k = F_{k+1} - 2$。把 $F_k - 2$ 和 F_k 分別寫成 2 的冪減去或加上 1 的形式。

停一停，試一試　$(a-1)(a+1) = a^2 - 1$。取 $a = 2^{2^k}$：把 a^2 寫成 2 的冪，會是甚麼？

階段 4 沒有公因數（common factor）

想一想 假設 d 同時整除 F_m 和 F_n，其中 $m < n$。在 $(*)$ 中取 $k = n$。F_m 是否左方的其中一個因數？

停一停，試一試 因此 d 既整除 F_n，也整除 $F_n - 2$。那麼 d 必定整除甚麼？在各個可能之中，哪些可以排除？為甚麼？

階段 5　無窮多個質數（prime）

想一想　每個費馬數都至少有一個質因數（prime factor）。從每個費馬數中各選一個質因數。

停一停，試一試　你為 F_m 選的質數，會否與你為 F_n 選的質數相同？運用上一部分的結果。

背後的數學

費馬猜對了嗎？

沒有。1732 年，萊昂哈德．歐拉證明了

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

歐拉並不是靠運氣找到 641 的。他證明了 F_n 的任何質因數都必定具有一種非常特殊的形式（當 $n = 5$ 時，它必定是 64 的倍數加一），從而大幅減少了需要考慮的可能。你可以在練習 4 中親自證明這一點。

自此以後，凡是有人成功檢驗過的費馬數，由 F_5 到 F_{32}，結果全都是合成數（compos-

ite）。就目前所知，F_0 至 F_4 可能是僅有的費馬質數，但沒有人能夠證明這一點。這是一個貨真價實的未解難題。

妙就妙在我們的證明完全不受影響。不論是質數還是合成數，費馬數依然能產生無窮多個質數。

費馬質數與正多邊形作圖

費馬質數會在一個相當意想不到的地方出現。古希臘人懂得用直尺和圓規作出等邊三角形和正五邊形，而請留意 $3 = F_0$ 和 $5 = F_1$。其後兩千年間，沒有人能作出其他邊數為質數的正多邊形（regular polygon）。到了 1796 年，年僅 19 歲的卡爾．弗里德里希．高斯（Gauss）示範了怎樣作出正十七邊形，而 $17 = F_2$。

高斯更進一步：正 N 邊形可以用直尺和圓規作出，當且僅當 N 是 2 的冪乘以若干個互不相同的費馬質數。（Pierre Wantzel 在 1837 年補全了這個證明。）所以哪些正多邊形可以作圖，取決於費馬質數有多少個。你會在 Section 6.2（STEP II 1991，第 4 題）遇到高斯正十七邊形背後的關鍵計算，而完整的來龍去脈則屬於伽羅瓦理論（Galois theory），那是大學本科數學課程的精華之一。

一個定理，多種證明

數學家為甚麼要不厭其煩地把同一個定理證明多於一次？因為不同的證明會揭示不同的東西。這個證明一般歸功於克里斯蒂安．哥德巴赫（Goldbach）在 1730 年寫給歐拉的一封信，它表明：任何一個由大於 1 的整數組成、各項兩兩互質的無窮數列，都必然帶來無窮多個質數。費馬數只是其中一個方便的例子。（練習 3 給出另一個例子。）

它給出的結論也比歐幾里得的證明更多。質數 $p_0, p_1, \ldots, p_{n-1}$ 是 n 個不同的質數，每個都不超過 F_{n-1}。所以不大於 $2^{2^{n-1}} + 1$ 的質數至少有 n 個。這是一個關於質數如何分佈的定量陳述。它非常弱（實際情況要好得多），但它是邁向十九世紀數學其中一項偉大成果的第一步，那就是質數定理（Prime Number Theorem），它精確地描述了質數怎樣變得越來越稀疏。Section 1.2 會踏出下一步。

延伸練習

1 **歐幾里得的版本。**寫出歐幾里得對「質數有無窮多個」的證明。它在甚麼意義上是「反證法」（by contradiction），而費馬數的證明又在甚麼意義上是「構造性」（constructive）的？

2 **末位數字。**證明當 $n \geq 2$ 時，費馬數 F_n 的末位數字是 7。

3 **西爾維斯特（Sylvester）數列。**定義 $a_1 = 2$ 及 $a_{n+1} = a_n^2 - a_n + 1$，於是數列的開頭幾項是 $2, 3, 7, 43, 1807, \ldots$

(a) 證明 $a_{n+1} - 1 = a_1 a_2 \cdots a_n$。

(b) 由此推導出各項兩兩互質，從而給出「質數有無窮多個」的另一個證明。

(c) 較難 證明 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$。

4 **歐拉的妙着。**本題需要用到費馬小定理（*Fermat's Little Theorem*）：若 p 是質數且 $p \nmid a$，則 $a^{p-1} \equiv 1 \pmod{p}$。假設質數 p 整除 F_n。

(a) 證明 $2^{2^n} \equiv -1 \pmod{p}$，從而證明 $2^{2^{n+1}} \equiv 1 \pmod{p}$。

(b) 設 d 為滿足 $2^d \equiv 1 \pmod{p}$ 的最小正整數。證明 d 整除 2^{n+1} 但不整除 2^n，並由此得出 $d = 2^{n+1}$。

(c) 利用費馬小定理，證明 d 整除 $p - 1$。由此推導出 $p \equiv 1 \pmod{2^{n+1}}$。

(d) 當 $n = 5$ 時，這表示 F_5 的任何質因數都具有 $64k + 1$ 的形式。驗證 641 確實如此。小於 641 而又具有這種形式的質數有多少個？

5 **質數的一個上界。**利用一個定理，多種證明中的論證，證明第 n 個質數不超過 $2^{2^{n-1}} + 1$。當 $n = 5$ 時，這個上界有多準確？

延伸閱讀

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK***（Springer），第 1 章「Six proofs of the infinity of primes」（質數無窮性的六個證明）。書中除了這個證明外，還收錄了歐幾里得的證明和另外四個證明，其中一個用上了拓撲學（topology）。這是入讀大學前最值得一讀的書之一。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press），第 1–2 章。一本文筆優美的入門書，介紹質數與因數分解，最適合在入讀大學前的暑假閱讀。
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers***（Springer，2001）。關於費馬數的一切，由歐拉的分解到高斯的正多邊形，應有盡有。不妨翻翻開首幾章。
- **Ian Stewart, *Why Beauty Is Truth***（Basic Books），關於高斯的一章。以一般讀者為對象，講述正十七邊形的故事。

完整的引導式解答見第 1.1 節：

https://beyondstep.keithmcnulty.org/zh-hant/ch01/fermat-numbers.html

每星期一道 STEP 題目，完整講解：The STEP Up，以電郵免費發送，訂閱網址：keithmcnulty.substack.com