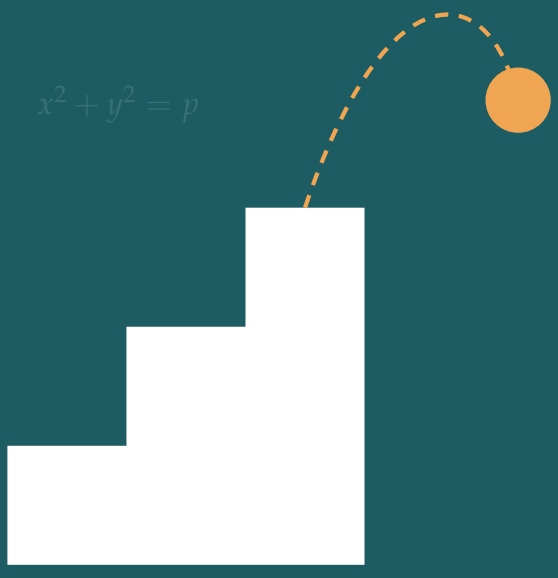
STEP 備試 · 大學數學

Beyond STEP

第 1 章

數論與證明



KEITH McNULTY

Beyond STEP

以歷屆 STEP 試題為門
走進大學數學

第 1 章

數論與證明

Keith McNulty

Beyond STEP：以歷屆 STEP 試題為門，走進大學數學

第 1 章：數論與證明

本冊是 *Beyond STEP* 全書 13 章中的第 1 章。全書、各章的單行本、每一節的可列印工作紙，以及每一道 STEP 試題的詳細解答，均可在 `beyondstep.keithmcnulty.org` 免費閱讀及下載。

2026 年 11 月首次於網上發表。

本 PDF 內凡屬作者本人創作的內容，包括正文、解答、插圖、練習及答案，均按照 Creative Commons CC0 1.0 Universal 授權條款貢獻予公有領域：你可以為任何目的複製、改編及分享，毋須徵求許可。詳見 `creativecommons.org/publicdomain/zero/1.0`。

本書討論的 STEP 試題，版權屬 Cambridge University Press & Assessment 所有。本書並無轉載這些試題：每一題均附連結，通往官方來源的題目，即 STEP Support Programme 的試題資料庫或 OCR 的歷屆試卷。

如有錯漏，歡迎到 `github.com/keithmcnulty/step_book_mcnulty` 提交 issue 指正。

章

1

數論與證明

整數是數學中最古老的對象，卻至今仍藏着數學中一些最深奧的祕密。

本章內容

1.1	質數工廠	STEP II 2002
1.2	質數分佈得有多稀疏？	STEP III 2016
1.3	最小反例	STEP III 2015
1.4	e 是無理數，e^2 也是	STEP III 2024
1.5	無窮遞降法	STEP III 2022
1.6	兩個平方數之和	STEP II 2023
1.7	因數分解失效之時	STEP I 2016
1.8	點算有理數	STEP III 2020
1.9	三次曲線的切線	STEP I 2009
A	練習答案	第 67 頁

為甚麼是整數？

> 數學是科學的皇后，而數論（*number theory*）是數學的皇后。
>
> — 高斯（Carl Friedrich Gauss）

整數是每個人最先接觸到的數學對象。你還未識字，就已經學會數數。然而，關於整數的最簡單的問題，卻可以難得出奇。每一個大於 2 的偶數，是否都是兩個質數（prime）之和？沒有人知道：哥德巴赫（Christian Goldbach）在 1742 年提出這個問題，電腦已經驗證到 4×10^{18} 以外，但至今仍然沒有人能夠證明。像 11 和 13，或 101 和 103 這樣相差 2 的質數對，是否有無窮多對？這同樣沒有人知道。不過在 2013 年，一位幾乎寂寂無名的數學家張益唐（Yitang Zhang）震驚了全世界：他證明了有無窮多對質數，彼此相差不超過 70 百萬，而這個數字後來已被降低至 246。費馬（Pierre de Fermat）在 1637 年於書頁邊的空白處隨手寫下：當 $n \geq 3$ 時，$x^n + y^n = z^n$ 沒有正整數解。人們花了超過 350 年，並動用了有史以來最精深的一些數學，才終於由懷爾斯（Andrew Wiles）在 1994 年證明他是對的。

問題連小孩子都聽得懂，答案卻可能要花上幾個世紀——正是這種組合令數論叫人欲罷不能。這也是為甚麼數論一直是證明（proof）的訓練場。整數有無窮多個，你不可能逐一檢查每個情況，於是就必須找出一個能一舉涵蓋所有情況的論證。你在往後的數學生涯中會用到的證明技巧，大部分最初都是在有關整數的問題上磨練出來的。

純粹、無用，卻支撐着互聯網

1940 年，劍橋數學家哈代（G. H. Hardy）頗為自豪地寫道：數論是所有數學中最純粹的，與日常生活相距太遠，不可能有任何實際用途，因而也不可能有任何有害的用途。他錯得不能再錯了。每當你在網上購物、發送加密訊息或為手機解鎖，你都在依靠數論。RSA 系統（1977 年）所依賴的事實是：把兩個大質數相乘很容易，但要從它們的乘積還原出這兩個質數，卻似乎難得無從入手。現代的系統所用的，正是你會在本章末遇到的那些曲線上的算術。十八、十九世紀的「無用」數學，成了二十一世紀的安全保障。

你在大學會遇到甚麼

如果你在大學修讀數學，數論會是你最先到達的地方之一，也會是你最後到達的地方之一。

- **在第一個學期**，你幾乎一定會修讀一門名為數與集合（Numbers and Sets）或數學基礎（Foundations）之類的課程。它會教你怎樣正式地書寫證明，而其中大部分素材都來自數論：歸納法（induction）、歐幾里得算法（Euclidean algorithm）、模算術（modular arithmetic）、費馬小定理（Fermat's Little Theorem）、中國餘數定理（Chinese Remainder Theorem），以及一個令人驚訝的事實——有些無窮集合比另一些無窮集合更大。
- **在羣論（group theory）中**（通常在第一年修讀），你會發現許多數論事實，原來都是同一條關於對稱的定理——拉格朗日定理（Lagrange's Theorem）——投下的影子。
- **在第二年**，一門數論課程通常會涵蓋二次互反律（quadratic reciprocity，即高斯的「黃金定理」）、連分數（continued fractions）和佩爾方程（Pell's equation）。
- **再往後**，你還可以走得更遠：代數數論（algebraic number theory），其中高斯整數（Gaussian integers）等新的數系挽救了唯一分解（unique factorisation）；解析數論（analytic number theory），它運用微積分和複分析（complex analysis）來數算質數；以及橢圓曲線（elliptic curves）的理論，它既是費馬最後定理（Fermat's Last Theorem）證明背後的支柱，也是七道懸賞一百萬美元的千禧年大獎難題（Millennium Prize Problems）之一的根源。

貫穿本章的問題

本章的九道 STEP 題目，圍繞着三個大問題打轉。做題時請把它們記在心上；我們會在本章結尾回到這些問題。

1. **質數有多少個？它們是怎樣分佈的？**人人都知道質數有無窮多個。但它們越往後變得有多稀疏？甚麼樣的論證才能告訴我們答案？
2. **怎樣證明一個數不是分數？**要說明一個數是有理數（rational），只需舉出一個例子。要說明它是無理數（irrational），卻要排除無窮多種可能。這到底是怎樣做到的？
3. **哪些方程有整數解？當我們改變數系時，又會發生甚麼事？**有時我們能證明某個方程完全沒有解。有時要了解整數，最好的方法卻是走出整數的範圍，進入複數（complex numbers），或走到一條曲線上。

關於證明的一章

在這三個問題底下，還貫穿着第四個主題：怎樣證明。每一節之所以入選，部分原因是它展示了一種不同的證明方法的實際運用；合起來，它們就是一套相當適合大學一年級

生的工具。

§	課題	思考方式
1.1	費馬數（Fermat numbers）	一個需要無窮多個質數的無窮族
1.2	質數的乘積	強歸納法（strong induction）；隱藏在二項式係數（binomial coefficients）中的信息
1.3	再談 $\sqrt{2}$	「取最小的那一個」：良序原理（well-ordering principle）
1.4	e 與 e^2	把一個整數嚴格地困在 0 與 1 之間
1.5	不可能的方程	無窮遞降法（infinite descent）；模 n 運算
1.6	兩個平方數之和	轉換場景：複數
1.7	一個奇怪的數系	質疑你視為理所當然的事
1.8	把分數逐一列出	構造雙射（bijection）；反向的遞降
1.9	立方數與曲線	用幾何解決算術問題

怎樣閱讀本章

每一節都以一道 STEP 題目的連結開始，題目與當年考試所出的完全一樣。請先自己嘗試，至少做半小時，然後才往下讀。一道你曾經苦苦思索過的題目，會比一道你只是讀過的題目令你學到多得多。當你往下讀時，問問自己方框是邀請你在答案出現之前先停下來想一想，而停一停，試一試方框則標示着關鍵思路已在你觸手可及之處的時刻。之後，每一節的背後的數學部分會把目光越過考試，望向你在大學將會遇到的數學。

各節的深度大致上逐步遞增，但它們基本上互相獨立。如果某一節未能吸引你，就先跳過，稍後再回來。

1.1 質數工廠

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`

引子

你幾乎肯定早已知道質數（prime）有無窮多個。歐幾里得（Euclid）約在公元前 300 年證明了這件事，這也是每個人最早接觸到的證明之一。那麼，STEP 的題目為甚麼要你再證明一次？

因為這個證明的運作方式完全不同。歐幾里得的論證是說：給我任何一張有限的質數清單，我都能指出它並不完整。而這個證明則說：這裏有一個預先寫好、明確給出的數列（*sequence*），當中每一個數都含有一個其他各數都沒有的質數。它是一部製造新質數的機器，而它之所以行得通，全靠一條簡潔優美的恆等式（identity），題目會一步一步引領你走向它。

途中你還會遇上一些連費馬（Fermat）本人也被騙倒的數。

動筆之前

先把題目從頭到尾讀一遍，留意它的結構。它分為四個階段：

1. 計算一些例子；
2. 找出（其實是題目告訴你）一個規律，並用這些例子驗證；
3. 證明這個規律在一般情況下成立；
4. 兩次運用這個規律：先推導出關於公因數（common factor）的結論，再推導出關於質數的結論。

這種「例子 → 猜想 → 證明 → 推論」的結構，正是許多數學研究的實際做法，STEP 的

題目也經常依循這個模式。遇到這種結構時，開頭的部分通常不只是熱身：你日後需要的直覺，正是在那裏建立的。

> **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？

請記住這個問題，我們稍後會回來討論。

逐步解題

階段 1　熟習這些數

要小心記號：2^{2^n} 是指 $2^{(2^n)}$，而不是 $(2^2)^n$。指數（exponent）本身就是 2 的冪，所以這些數增長得非常快。

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

> **想一想**　這四個數有甚麼值得留意的地方？

它們全是質數。（驗證 257：它不能被 $2, 3, 5, 7, 11$ 或 13 整除，而 $17^2 = 289 > 257$，所以可以就此停下。）下一個數 $F_4 = 2^{16} + 1 = 65537$ 也是質數。皮埃爾 · 德 · 費馬在 1640 年正正注意到這一點，並猜想（conjecture）所有這種形式的數都是質數。請把這件事記在心裏，稍後我們會看看他是否猜對了。

階段 2　驗證恆等式

現在就較小的 k 驗證 $(*)$：

- $k = 1$：左邊只有 $F_0 = 3$，而 $F_1 - 2 = 3$。✓
- $k = 2$：$F_0 F_1 = 3 \times 5 = 15$，而 $F_2 - 2 = 15$。✓
- $k = 3$：$F_0 F_1 F_2 = 15 \times 17 = 255$，而 $F_3 - 2 = 255$。✓

> **想一想**　看看由 $k = 2$ 到 $k = 3$ 的那一步。我們把 15 乘以 17，得到 255。用費馬數來表達，就是計算了 $(F_2 - 2) \times F_2$，結果得到 $F_3 - 2$。這是巧合嗎？

這個觀察就是整個證明的縮影。讓我們看看它為甚麼應該成立。

階段 3　證明恆等式

停一停，試一試 繼續讀下去之前，試試直接證明

$$(F_k - 2)\, F_k = F_{k+1} - 2.$$

提示：把所有東西都用 2 的冪來表示。$F_k - 2$ 是甚麼樣子的？

我們有 $F_k - 2 = 2^{2^k} - 1$ 和 $F_k = 2^{2^k} + 1$，所以

$$(F_k - 2)\, F_k = \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right).$$

想一想 這是一個形如 $(a-1)(a+1)$ 的乘積。它等於甚麼？

它是平方差（difference of two squares）$a^2 - 1$。取 $a = 2^{2^k}$，則

$$a^2 = \left(2^{2^k}\right)^2 = 2^{2\cdot 2^k} = 2^{2^{k+1}},$$

所以

$$(F_k - 2)\, F_k = 2^{2^{k+1}} - 1 = F_{k+1} - 2. \tag{†}$$

這就是整部機器的引擎。留意平方的作用：它把指數加倍，而 2^k 加倍後就是 2^{k+1}。費馬數的定義與平方差的因式分解（factorisation）配合得天衣無縫。

這樣一來，歸納法（induction）幾乎是水到渠成。

想一想 在歸納步驟中，我們究竟要證明甚麼？

假設 $(*)$ 對某個 $k \geq 1$ 成立，即

$$F_0 F_1 \cdots F_{k-1} = F_k - 2,$$

而我們想證明它對 $k+1$ 也成立：

$$F_0 F_1 \cdots F_{k-1} F_k = F_{k+1} - 2.$$

把假設的等式兩邊同乘以 F_k，再運用 (†)：

$$F_0 F_1 \cdots F_{k-1} F_k = (F_k - 2)\, F_k = F_{k+1} - 2.$$

我們已經驗證了 $k = 1$ 的情況，所以根據歸納法，$(*)$ 對所有 $k \geq 1$ 都成立。 ■

想一想 我們能否完全不用歸納法？

可以，而且值得看看怎樣做。由 $F_0 - 2 = 1$ 出發，反覆運用 (†)：

$$F_k - 2 = (F_{k-1} - 2)F_{k-1} = (F_{k-2} - 2)F_{k-2}F_{k-1} = \cdots = (F_0 - 2)\, F_0 F_1 \cdots F_{k-1}.$$

由於 $F_0 - 2 = 1$，證明便完成了。這種「逐層展開」的做法，其實就是把同一個歸納法完整地寫出來，不過有些人會覺得這樣更容易看明白。

階段 4　沒有公因數

我們想證明：若 $m \neq n$，則 F_m 與 F_n 沒有大於 1 的公因數。

> **想一想**　假設某個數 d 同時整除 F_m 和 F_n，其中 $m < n$。F_m 在 $(*)$ 的哪個位置出現？

在 $(*)$ 中取 $k = n$：

$$F_0 F_1 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

由於 $m < n$，F_m 是左邊其中一個因數。所以若 d 整除 F_m，則 d 整除整個左邊；也就是說，d 整除 $F_n - 2$。

> **想一想**　現在 d 既整除 F_n，又整除 $F_n - 2$。它還必定整除甚麼？

它們的差：d 整除 $F_n - (F_n - 2) = 2$。所以 $d = 1$ 或 $d = 2$。

> **想一想**　d 可以是 2 嗎？

不可以：每個費馬數都是 2 的冪加 1，所以是奇數。因此 $d = 1$，即任何兩個不同的費馬數都沒有大於 1 的公因數。 ■

數學家會說費馬數*兩兩互質*（pairwise coprime）。

階段 5　無窮多個質數

現在回到我們一開始提出的問題。

> **想一想**　每個大於 1 的整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。對於你選出的這些質數，你能說些甚麼？

設 p_n 為任意一個整除 F_n 的質數。假如其中兩個相等，例如 $p_m = p_n$ 而 $m \neq n$，那麼這個質數就是 F_m 與 F_n 的一個大於 1 的公因數，但我們剛剛證明了這是不可能的。所以質數

$$p_0,\ p_1,\ p_2,\ p_3,\ \ldots$$

全都*互不相同*。費馬數有無窮多個，所以不同的質數也有無窮多個。 ■

留意我們從來不需要知道每個費馬數是被*哪一個*質數整除，甚至不需要知道費馬數本身是不是質數。我們只需要知道它們永遠沒有公因數。每個費馬數都必須「用掉」至少一個其他費馬數不能用的質數。

n	$F_n = 2^{2^n} + 1$	質因數分解
0	3	質數
1	5	質數
2	17	質數
3	257	質數
4	65 537	質數
5	4 294 967 297	$641 \times 6\,700\,417$
6	18 446 744 073 709 551 617	$274\,177 \times 67\,280\,421\,310\,721$

圖 1.1.1 最初幾個費馬數。費馬猜想它們全是質數，但歐拉（Euler）在 1732 年找到了 F_5 的因數 641，而 F_4 之後至今仍未發現任何費馬數是質數。即使如此，恆等式 $(*)$ 表明不同費馬數的因數永不重疊：每一行都帶來新的質數。

回顧

值得停下來看看這道題成功的關鍵何在，因為同樣的想法會在本書中多次重現。

- **例子並不是裝飾。**看出 $15 \times 17 = 255$ 其實是「$(F_2 - 2) \times F_2 = F_3 - 2$」，正是關鍵思路。當題目給你一些簡單情況時，要問每一步在做甚麼，而不只是看數字是否吻合。
- **一條恆等式完成了所有工作。**一切都源自 $(a-1)(a+1) = a^2 - 1$。看似艱深的 STEP 題目，往往只是由一小段簡單的代數推動。
- **最後的論證着眼於結構，而非大小。**我們證明了質數有無窮多個，卻沒有找出任何一個新的質數。我們證明的是：要構成這個無窮的數族，必須用上無窮多個質數。

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（composite）。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。

思維技巧

從結構性質出發建立論證

要證明 A 類對象有無窮多個，可以找出無窮多個 B 類對象，而每個 B 類對象都需要一個專屬於自己的 A 類對象。

這裏 A = 質數，B = 費馬數，而「需要一個專屬於自己的」是指「有一個不與

其他任何一個共用的質因數」。同樣的模式也出現在計數論證、線性代數（linear algebra）（無窮多個線性獨立的向量必然導致無窮維）和分析（analysis）之中。

你也練習了歸納法，尤其是養成追問「由 k 到 $k+1$ 的那一步實際上做了甚麼？」的習慣。這個問題往往比形式上的範本更有用。

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。

1.2 質數分佈得有多稀疏？

題目

STEP III 2016，第 5 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/16-s3-q5`

引子

在 Section 1.1 中，我們已看到質數（prime）有無窮多個。但「無窮多個」是個很粗略的說法。質數確實愈來愈稀疏：100 以下有 25 個質數，但 900 與 1000 之間只有 14 個。它們究竟會稀疏到甚麼程度？

這道題要證明的結論聽來相當平凡：把不超過 n 的所有質數相乘，所得的積小於 4^n。然而，這個看似平平無奇的不等式（inequality），正是回答「有多稀疏？」的第一步實質進展，也是數學史上最著名的簡短證明之一的關鍵引理（lemma）；該證明出自年輕的保羅·艾狄胥（Paul Erdős）之手，時為 1932 年。

動筆之前

記號 $P_{r,s}$ 看來有點繁瑣，但背後的意思很簡單：把某個範圍內的質數相乘。務必先弄懂題中的例子。$P_{3,7}$ 用的是大於 3 而不超過 7 的質數，即 5 和 7，所以它等於 35。

> **想一想** 第 (iv) 部分要求你對所有 $n \geq 2$ 證明一個命題。第 (iii) 部分則假設該命題對不超過 $2m$ 的每一個 k 都成立。這是哪一種歸納法（induction）？

這是強歸納法（strong induction）：要證明 n 的情況，你可以假設前面所有情況都成立，而不僅是緊接在前的那一個。請把這一點記在心裏；題目之所以這樣編排，原因正在於此。

逐步解題

階段 1　二項式係數不會太大

想一想　在 $(1+x)^{2m+1}$ 的二項展開式（binomial expansion）中代入 $x=1$，會得到甚麼？

你會得到

$$2^{2m+1} = \binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{2m+1}.$$

各項都是正數，所以每一項都小於 2^{2m+1}。這還不夠好；我們想要的是 2^{2m}，即它的一半。

想一想　帕斯卡三角形（Pascal's triangle）是對稱的。和式中還有哪一項等於 $\binom{2m+1}{m}$？

由對稱性，$\binom{2m+1}{m} = \binom{2m+1}{m+1}$，而這是和式中兩個不同的項（因為 $m \neq m+1$）。所以

$$2\binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} < 2^{2m+1},$$

這裏是嚴格不等式，因為和式中還有其他正項，例如 $\binom{2m+1}{0} = 1$。兩邊除以 2，即得 $\binom{2m+1}{m} < 2^{2m}$。 ■

階段 2　哪些質數整除這個二項式係數？

把這個二項式係數（binomial coefficient）寫出來：

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!} = \frac{(m+2)(m+3)\cdots(2m+1)}{m!}.$$

想一想　設 p 為質數，且 $m+1 < p \leq 2m+1$。p 整除分子嗎？它有可能整除分母嗎？

分子 $(m+2)(m+3)\cdots(2m+1)$ 的因子當中就有 p 本身，所以 p 整除分子。分母 $m!$ 是若干個數的積，而這些數全都小於 p；由於 p 是質數，如果它不能整除其中任何一個數，就不能整除它們的積。因此 p 整除分子而不整除分母，於是 p 整除整個二項式係數（別忘記，它是一個整數）。

停一停，試一試　我們現在知道，這個範圍內的每一個質數都整除 $\binom{2m+1}{m}$。為甚麼由此可知它們的積 $P_{m+1,2m+1}$ 也整除它？（小心：即使 4 和 6 都整除某個

數，24 也不一定整除它。）

分別在於，我們的質數是**相異質數**。如果相異質數 $p_1, p_2, \ldots$ 各自整除 N，那麼它們的積也整除 N：寫 $N = p_1 N_1$；這時 p_2 整除 $p_1 N_1$ 但不整除 p_1，所以它整除 N_1；如此類推。（這裏用到一個事實：如果一個質數整除某個積，它必整除其中一個因子。這個事實值得我們稍加敬重；Section 1.7 會展示一個世界，在那裏與它相應的命題並不成立。）

所以 $P_{m+1,2m+1}$ 整除 $\binom{2m+1}{m}$，而正數的因數不會大於該數本身，故

$$P_{m+1,\,2m+1} \le \binom{2m+1}{m} < 2^{2m}. \qquad \blacksquare$$

階段 3 把積拆開

想一想 $P_{1,2m+1}$ 是不超過 $2m+1$ 的所有質數的積，怎樣用我們已經掌握的積把它拼出來？

把不超過 $2m+1$ 的質數分成兩批：不超過 $m+1$ 的，以及大於 $m+1$ 的：

$$P_{1,2m+1} = P_{1,m+1} \times P_{m+1,2m+1}.$$

由第 2 階段，第二個因子小於 $2^{2m} = 4^m$。至於第一個因子，我們可以假設 $P_{1,k} < 4^k$ 對由 2 至 $2m$ 的每一個 k 都成立，而 $k = m+1$ 正在這個範圍之內（因為由 $m \ge 1$ 可得 $2 \le m+1 \le 2m$）。所以

$$P_{1,2m+1} < 4^{m+1} \times 4^m = 4^{2m+1}. \qquad \blacksquare$$

強歸納法正是在這裏大派用場：要處理 $2m+1$，我們需要的是 $m+1$ 的情況，它的大小約為一半，而不是緊接在前的那個情況。

階段 4 所有 n

想一想 第 (iii) 部分處理了奇數。對於偶數 $n = 2m+2$，情況又如何？它是質數嗎？

先驗證起始情況：$P_{1,2} = 2 < 16$ 及 $P_{1,3} = 6 < 64$。現在假設 $P_{1,k} < 4^k$ 對由 2 至 $n-1$ 的所有 k 都成立，其中 $n \ge 4$。

- 若 n 是偶數，則 n 不是質數（因為它大於 2），所以不超過 n 的質數與不超過 $n-1$ 的質數完全相同。因此 $P_{1,n} = P_{1,n-1} < 4^{n-1} < 4^n$。
- 若 n 是奇數，寫 $n = 2m+1$，其中 $m \ge 2$。這時由第 (iii) 部分直接得出 $P_{1,n} < 4^n$。

由強歸納法，$P_{1,n} < 4^n$ 對每一個 $n \ge 2$ 都成立。 $\blacksquare$

回顧

- **二項式係數蘊藏算術資訊。**$\binom{2m+1}{m}$ 是單獨一個數，它不大（小於 4^m），卻必須被許多質數整除。把許多質數擠進一個不大的數裏，就說明這些質數不可能太多。
- **當問題會把自己減半時，強歸納法是最自然的工具。**$2m+1$ 的情況取決於 $m+1$ 的情況。
- **小的情況須另行驗證。**歸納要到 $n \geq 4$ 才能開始運作，所以 $n = 2$ 和 3 必須親手計算。

背後的數學

從 4^n 到質數定理

對結果取對數：$\ln P_{1,n} < n \ln 4$，即

$$\sum_{p \leq n} \ln p < (\ln 4)\, n \approx 1.39\, n.$$

在 1850 年代，切比雪夫（Pafnuty Chebyshev）證明了正是這一類的界（bound），而且上界和下界俱備，從而說明 $\sum_{p \leq n} \ln p$ 的增長與 n 成正比。高斯（Gauss）在大約 15 歲時，已從數表中猜到不超過 n 的質數個數大約是 $n / \ln n$。這後來成為質數定理（Prime Number Theorem），最終在 1896 年由阿達馬（Jacques Hadamard）和德拉瓦萊普桑（Charles de la Vallée Poussin）運用複分析（complex analysis）證明。它的對數形式是

$$\sum_{p \leq n} \ln p \sim n,$$

所以不超過 n 的質數之積大約是 e^n。我們的界 4^n 其實相差不遠：圖 1.2.1 把三者一併畫出。

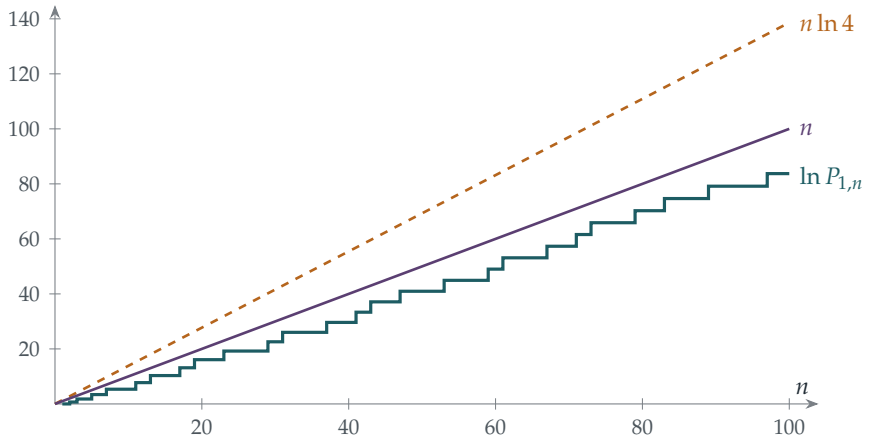


圖 1.2.1　不超過 n 的所有質數之積的對數（藍綠色），在每個質數 p 處跳升 $\ln p$。本節證明它始終低於 $n \ln 4$（琥珀色虛線）；質數定理則指出它的增長與 n 相若（紫紅色）。

伯特蘭公設

1845 年，伯特蘭（Joseph Bertrand）猜想：對每一個 $n \geq 1$，在 n 與 $2n$ 之間總有一個質數。這就是伯特蘭公設（Bertrand's postulate）。切比雪夫在 1852 年證明了它。八十年後，年僅 19 歲的艾狄胥找到了一個優美的初等證明。它的關鍵材料，就是本題的引理，再加上仔細考察哪些質數整除中間的二項式係數 $\binom{2n}{n}$。Martin Aigner 和 Günter Ziegler 把它選為 *Proofs from THE BOOK* 的第 2 章，該書匯集了數學中最優雅的證明。

接下來的方向

質數的精確分佈，由黎曼 ζ 函數（Riemann zeta function）

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

的零點（zero）所支配。你會在 Section 2.4 中遇見這個函數樸素得多的一面，那裏有 $\zeta(2) = \pi^2/6$。黎曼猜想（Riemann Hypothesis）預測了這些零點的確切位置；它若成立，便能把質數定理中的誤差限定得緊無可緊。它也許是數學中最著名的未解難題，也是千禧年大獎難題（Millennium Prize Problems）之一。

思維技巧

強歸納法，以及從巧妙的對象中提取資訊

如果 n 的情況取決於遠小於 $n-1$ 的情況，就一次過假設前面所有情況都成立。

這裏的另一個想法較為微妙，也極具數論（number theory）的特色：要證明某個範圍內所有質數的某種性質，就找出一個對象（這裏是一個二項式係數），使得這些質數每一個都必須整除它，而你又能證明它不會太大。

延伸練習

1 **感受一下數字。**對 $n = 10, 20, 30$ 計算 $P_{1,n}$，並把它與 4^n 及 e^n 比較。（這裏可以使用計算機。）

2 **中間的二項式係數。**證明 $\binom{2m}{m}$ 是 $(1+1)^{2m}$ 展開式的 $2m+1$ 項中最大的一項，並由此推出 $\binom{2m}{m} \geq \dfrac{4^m}{2m+1}$。

3 **質數不會太多。**設 $\pi(n)$ 為不超過 n 的質數個數。介乎 $\sqrt{n}$ 與 n 之間的每個質數都大於 $\sqrt{n}$，而它們的積至多為 $P_{1,n} < 4^n$。由此推出

$$\pi(n) - \pi(\sqrt{n}) < \frac{2\ln 4}{\ln n}\, n,$$

從而得出 $\pi(n) < 2.8\, n/\ln n + \sqrt{n}$。把這個結果與質數定理的 $\pi(n) \approx n/\ln n$ 比較。

4 **驗證伯特蘭公設。**對 $n = 1, 2, \ldots, 50$ 驗證伯特蘭公設，即在每個情況下找出一個介乎 n 與 $2n$ 之間的質數。你能否利用一張簡短的質數表有效率地完成，使表中每個質數都小於前一個的兩倍？

延伸閱讀

- **Aigner & Ziegler, *Proofs from THE BOOK***，第 2 章「Bertrand's postulate」（伯特蘭公設）。
- **Marcus du Sautoy, *The Music of the Primes***（Fourth Estate）。一部講述質數定理與黎曼猜想歷史的普及讀物。
- **G. J. O. Jameson, *The Prime Number Theorem***（Cambridge University Press）。嚴謹而平易近人，為大學本科生而寫；開首幾章只需要高級程度（A-level）的微積分。

1.3 最小反例

題目

STEP III 2015，第 5 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/15-s3-q5`

引子

你大概見過 $\sqrt{2}$ 是無理數(irrational)的證明：假設 $\sqrt{2} = a/b$ 為最簡分數(lowest terms)，兩邊平方，推出 a 是偶數，繼而推出 b 也是偶數，於是得出矛盾（contradiction）。這是個漂亮的證明，但它依賴一個關於偶數的技巧，而這個技巧看不出可以怎樣推廣。換成 $\sqrt[3]{2}$ 又如何？$\sqrt{7}$ 呢？

本題給出另一個證明，它的核心想法簡單得近乎荒謬：*看看最小的那一個*。在本章裏，同一個想法還會改頭換面地出現好幾次。

動筆之前

這是一道不尋常的 STEP 題目：它給你一個證明的骨架，要你補上當中欠缺的理據。大學生正是這樣學習閱讀數學的。課本裏的證明常常說「顯然」或「由此可得」，而你的部分工作，就是查證事實是否真的如此。

想一想 第 4 步說「定義 k 為 S 中最小的正整數」。我們憑甚麼可以這樣做？假如 S 是一個由正實數組成的集合，這樣做還可以嗎？

任何由正整數組成的非空集合都有最小元素。這稱為*良序原理*（well-ordering principle），它與數學歸納法（mathematical induction）原理等價。對於由正實數組成的集合，這個原理*並不成立*：集合 $\{x : x > 0\}$ 就沒有最小元素。所以第 4 步既依賴第 3 步（集合必須非空），也依賴 S 由整數組成這一點。

逐步解題

階段 1　第 3 步：S 非空

想一想　若 $\sqrt{2} = a/b$，其中 a 和 b 是正整數，你能寫出 S 的一個元素嗎？

若 $\sqrt{2} = a/b$，則 $b\sqrt{2} = a$，是一個整數。所以 b 屬於 S，S 非空。

階段 2　第 5 步：一個更小的元素

現在 k 是 S 的最小元素，所以 $k\sqrt{2}$ 是整數，記為 j。

停一停，試一試　要證明 $(\sqrt{2}-1)k$ 屬於 S，你必須檢查三件事。是哪三件？

我們需要 $(\sqrt{2}-1)k$ 滿足：(a) 是整數；(b) 是正數；(c) 乘以 $\sqrt{2}$ 後得到整數。

- (a) $(\sqrt{2}-1)k = k\sqrt{2} - k = j - k$，是兩個整數之差。
- (b) $\sqrt{2} > 1$，所以 $\sqrt{2} - 1 > 0$，因此 $(\sqrt{2}-1)k > 0$。
- (c) $(\sqrt{2}-1)k \cdot \sqrt{2} = 2k - k\sqrt{2} = 2k - j$，是整數。

所以 $(\sqrt{2}-1)k \in S$。

階段 3　第 6 步：矛盾

想一想　$\sqrt{2} - 1$ 有多大？

由於 $1 < \sqrt{2} < 2$，我們有 $0 < \sqrt{2} - 1 < 1$，所以 $(\sqrt{2}-1)k < k$。我們找到了 S 的一個元素，它比 S 的最小元素 k 還要小。這是不可能的，所以第 1 步的假設不成立：$\sqrt{2}$ 是無理數。 ■

留意我們從頭到尾都不需要「最簡分數」，也不需要任何關於奇偶數的事實。整個證明只建基於三個事實：$\sqrt{2} \cdot \sqrt{2}$ 是整數；$\sqrt{2}$ 嚴格地介乎兩個連續整數之間；整數具有良序性。

階段 4　立方根：把兩個數聯繫起來

設 $c = 2^{1/3}$，則 $c^2 = 2^{2/3}$ 且 $c^3 = 2$。

想一想　若 c 是有理數（rational），c^2 是否也是？反過來，若 c^2 是有理數，你能否只用乘法和除法回到 c？

若 c 是有理數，則 $c^2 = c \times c$ 也是有理數。反之，若 c^2 是有理數，則 $2/c^2 = c^3/c^2 = c$ 也是有理數。所以 $2^{1/3}$ 是有理數，當且僅當 $2^{2/3}$ 是有理數。 ■

階段 5 改造論證

? **想一想** 在第 (i) 部分，關鍵在於 $(\sqrt{2})^2 = 2$ 是整數，所以把 S 的元素乘以 $\sqrt{2}$ 兩次，就會回到整數。對於 $c = 2^{1/3}$，你需要乘三次。集合 S 應該怎樣修改？

假設 c 是有理數，則 c^2 也是。定義

$$S = \{n \text{ 為正整數} : nc \text{ 和} nc^2 \text{ 都是整數}\}.$$

- S **非空。**若 $c = a/b$ 且 $c^2 = a'/b'$，則 bb' 屬於 S。
- **設** k **為它的最小元素**，並考慮 $(c-1)k$。我們有 $1 < c < 2$（因為 $1^3 < 2 < 2^3$），所以 $0 < (c-1)k < k$。
- **它是整數：**$(c-1)k = kc - k$。
- **乘以** c**：**$(c-1)k \cdot c = kc^2 - kc$，是整數。
- **乘以** c^2**：**$(c-1)k \cdot c^2 = kc^3 - kc^2 = 2k - kc^2$，是整數。

所以 $(c-1)k \in S$，而且比 k 小：矛盾。因此 $2^{1/3}$ 是無理數，而根據第 4 階段，$2^{2/3}$ 也是無理數。 ■

回顧

- **「取最小的那一個」是一種證明技巧。**假設反例存在，取其中最小的一個，再由它造出一個更小的。這稱為*極端原理*（extremal principle），或稱*最小反例*（minimal counterexample）論證。
- **集合** S **替我們記帳。**我們不必周旋於分子和分母之間，而是把所有「好」的乘數收進同一個集合。
- **推廣，就是追問證明真正行得通的原因。**對於 $\sqrt{2}$，需要乘以 $\sqrt{2}$ 一次；對於 $\sqrt[3]{2}$，則需要乘兩次。看出這一點，我們就清楚知道該怎樣重新定義 S。

背後的數學

一個畫得出來的證明

第 (i) 部分背後有一幅優美的圖，出自 Stanley Tennenbaum。若 $\sqrt{2} = a/b$，則 $a^2 = 2b^2$：一個邊長為 a 的正方形，面積等於兩個邊長為 b 的正方形面積之和。如圖 1.3.1 所示，把兩個邊長為 b 的正方形放在邊長為 a 的正方形的兩個對角。它們重疊之處是一個小正方形，另外還有兩個小正方形沒有被蓋住。由於面積相等，重疊部分必定等於兩個未被蓋住的正方形之和，於是得到一對更小而具有同樣性質的整數。整數對不可能無止境地愈變愈小，所以這樣的正方形並不存在。這對較小的整數正是 $(2b - a,\ a - b)$，也就是我們那一步 $(\sqrt{2} - 1)k$ 的化身。

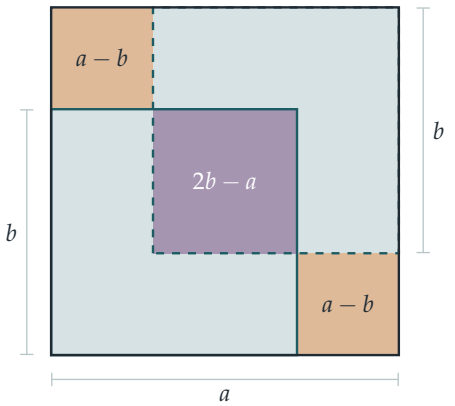


圖 1.3.1　Tennenbaum 的證明。兩個邊長為 b 的正方形（藍綠色）放在邊長為 a 的正方形的兩個對角。若 $a^2 = 2b^2$，則被計算了兩次的面積（紫紅色的重疊部分）必定等於沒有計算到的面積（兩個琥珀色的角落），所以 $(2b - a)^2 = 2(a - b)^2$：一個更小的解。

良序、歸納與遞降

良序原理與歸納法原理在邏輯上等價：兩者可以互相推導。到了大學，你會看到兩者都被用作自然數的基礎。在 Section 1.5 中，我們會以另一種形式運用同一個原理，那就是費馬（Fermat）的*無窮遞降法*（method of infinite descent）：不存在由正整數組成的無窮嚴格遞減數列。

它能走多遠？

這個論證可以證明，只要 N 不是完全平方數（perfect square），$\sqrt{N}$ 就是無理數（見練習）；更一般地，一個整數的 n 次方根要麼是整數，要麼是無理數。到了大學，這會變成一個關於代數整數（algebraic integers）的命題：若一個有理數滿足某個整數係數的首一多項式（monic polynomial）方程，例如 $x^3 - 2 = 0$，它就必定是整數。你會在 Section 6.3 再次遇到這個想法。

相傳畢達哥拉斯學派（Pythagoreans）因為希帕索斯（Hippasus）洩露了 $\sqrt{2}$ 是無理數而把他淹死，這個傳說多半並不屬實。屬實的是，這個發現迫使希臘數學家把對數的研究與對長度的研究分開；這道裂痕要等到十九世紀，待戴德金（Dedekind）構造出實數，才得以彌合。

思維技巧

極端原理

如果你想證明某件事永遠不會發生，就假設它會發生，選出最小（或最大、或最簡單）的例子，再用它造出一個更小的例子。

決定「最小」是甚麼意思，正是需要創意的一步。在這裏，它是使 $n\sqrt{2}$ 成為整數的最小的 n。

延伸練習

1. **其他平方根。**改造這個論證，證明 $\sqrt{3}$ 是無理數。哪一個數擔當了 $\sqrt{2}-1$ 的角色？
2. **所有非平方數。**設 N 為一個不是完全平方數的正整數，並設 m 為滿足 $m < \sqrt{N} < m+1$ 的整數。考慮 $(\sqrt{N} - m)k$，從而證明 $\sqrt{N}$ 是無理數。
3. **找出漏洞。**試把這個論證套用於 $\sqrt{4}$。究竟是哪一步行不通？
4. **Tennenbaum 的圖。**利用圖 1.3.1 證明：若 $a^2 = 2b^2$，則 $(2b-a)^2 = 2(a-b)^2$。再用代數方法驗證這個恆等式。

延伸閱讀

- **Daniel Velleman, *How to Prove It***（Cambridge University Press）。一本全面的證明入門書，內容包括歸納法和良序原理。

- **R. P. Burn, *A Pathway into Number Theory***（Cambridge University Press）。全書由精心編排次序的問題組成，是修讀大學一年級課程前的理想準備。
- **John Conway & Joseph Shipman, "Extreme proofs I: the irrationality of $\sqrt{2}$"**（*Mathematical Intelligencer*，2013）。同一個事實的多個證明，比較得妙趣橫生。

1.4 e 是無理數，e^2 也是

本節會用到兩道題目。第一道出自 1997 年，證明 e 是無理數（irrational number）。第二道出自 2024 年，把同一個想法用得更巧妙，證明 e^2 是無理數，而這原來確實困難得多。

熱身題

STEP III 1997，第 7 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/97-s3-q7`

主題目

STEP III 2024，第 7 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2024 年 STEP 試卷（zip 檔案）內的 STEP III 試卷：

`www.ocr.org.uk/Images/725753-2024-past-papers.zip`

引子

在 Section 1.3 中，我們證明了 $\sqrt{2}$ 是無理數，用的是 $\sqrt{2}$ 滿足一條簡單方程 $x^2 = 2$ 這個事實。但就我們所知，e 並不滿足任何這樣的方程。我們手上只有它的級數（series）：

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots .$$

一個級數怎能告訴你某個數不是分數？

答案是數論（number theory）中最有用的想法之一：整數（*integer*）不可能嚴格介乎 0 與 1 之間。如果你能證明某個量是整數，同時又嚴格介乎 0 與 1 之間，就得出矛盾（contradiction）。本節的一切，都是這個主題的變奏。

動筆之前

想一想　假設 $e = p/q$。把 e 乘以 q 會得到整數。那麼乘以 $q!$ 又會對 e 的級數的每一項有甚麼影響？

只要 $k \le q$，把 $\dfrac{1}{k!}$ 乘以 $q!$ 都會得到整數。因此 $q!\,e$ 可分成整數部分（首 $q+1$ 項）和「尾部」（tail，即其後的所有項）。若 $e = p/q$，則 $q!\,e$ 本身是整數，所以尾部也必定是整數。我們的計劃，就是證明尾部嚴格介乎 0 與 1 之間。

逐步解題

階段 1　熱身題：e 是無理數

級數 b_n 是等比級數（geometric series），首項和公比都是 $\frac{1}{n+1}$，所以

$$b_n = \frac{1/(n+1)}{1 - 1/(n+1)} = \frac{1}{n}.$$

想一想　逐項比較 a_n 和 b_n。哪一個較大？

兩者的首項相等。其後，$(n+1)(n+2) > (n+1)^2$，而一般來說，當 $k \ge 2$ 時 $(n+1)(n+2)\cdots(n+k) > (n+1)^k$，所以 a_n 其後的每一項都小於 b_n 的對應項。因此 $0 < a_n < b_n = 1/n$。

現在看看 a_n 究竟是甚麼。把 e 的級數乘以 $n!$：

$$n!\,e = \underbrace{\frac{n!}{0!} + \frac{n!}{1!} + \cdots + \frac{n!}{n!}}_{\text{整數}} + \underbrace{\frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \cdots}_{= a_n}.$$

由於 $0 < a_n < 1$，$n!\,e$ 的整數部分就是第一個括號，而 a_n 就是小數部分（fractional part）：$a_n = n!\,e - [n!\,e]$。

停一停，試一試　現在完成證明。假設 $e = p/q$。你應該選取哪個 n 值？

取 $n = q$。那麼 $q!\,e = (q-1)!\,p$ 是整數，所以它的小數部分 a_q 是 0。但 $a_q > 0$。矛盾：e 是無理數。 ■

這個證明出自傅立葉（Joseph Fourier），約於 1815 年提出。

階段 2　為何 e^2 較難

想一想 試把同一個想法用於 e^2。它的級數是 $\sum 2^k/k!$。當你乘以 $n!$ 再看尾部時，哪裏出了問題？

尾部現在是 $\dfrac{2^{n+1}}{n+1}+\dfrac{2^{n+2}}{(n+1)(n+2)}+\cdots$，而 2 的冪把一切都破壞了：尾部不再細小。乘以 $n!$ 對分子中的 2^k 毫無幫助。

2024 年這道題的妙着，是完全避開 e^2。若 $e^2=p/q$，則

$$qe=\frac{p}{e}.$$

現在我們有兩個數 e 和 $1/e$，各自都有一個階乘（factorial）級數，而且沒有麻煩的 2 的冪：

$$e=\sum_{k=0}^{\infty}\frac{1}{k!},\qquad \frac{1}{e}=\sum_{k=0}^{\infty}\frac{(-1)^k}{k!}.$$

階段 3 兩個尾部

第 (i) 部分正正就是熱身題：$0<f(n)<1/n$。

至於第 (ii) 部分，$g(n)$ 是一個各項的大小遞減的交錯級數（alternating series）。

想一想 對於交錯級數 $t_1-t_2+t_3-\cdots$，其中 $t_1>t_2>t_3>\cdots>0$，為何它的和介乎 0 與 t_1 之間？

把各項兩兩配對：$(t_1-t_2)+(t_3-t_4)+\cdots$ 是若干個正括號之和，所以是正數。換另一種方式配對：$t_1-(t_2-t_3)-(t_4-t_5)-\cdots$ 是 t_1 減去若干個正括號，所以小於 t_1。這裏 $t_1=\frac{1}{n+1}$，而各項遞減，因為每一項都是前一項除以一個大於 1 的數。所以 $0<g(n)<\frac{1}{n+1}$。

階段 4 又見整數

把 e 乘以 $(2n)!$，然後分出尾部，做法與熱身題完全一樣：

$$(2n)!\,e=(\text{整數})+f(2n).$$

所以 $(2n)!\,e-f(2n)$ 是整數。現在對 $1/e$ 做同樣的事：

$$\frac{(2n)!}{e}=\sum_{k=0}^{2n}(-1)^k\frac{(2n)!}{k!}+\sum_{k=2n+1}^{\infty}(-1)^k\frac{(2n)!}{k!}.$$

想一想 尾部的首項（即 $k=2n+1$ 的一項）是甚麼符號？尾部與 $g(2n)$ 相比又如何？

尾部首項的 $k = 2n+1$ 是奇數，所以該項是負數。尾部是

$$-\frac{1}{2n+1} + \frac{1}{(2n+1)(2n+2)} - \cdots = -g(2n).$$

所以 $\dfrac{(2n)!}{e} + g(2n)$ 是整數。 ■

這就是題目用 $2n$ 而不用 n 的原因：乘數是偶數的階乘時，$1/e$ 的尾部恰好是 $-g$，符號可以預知。

階段 5　矛盾

假設 $qe = p/e$。把等式兩邊乘以 $(2n)!$，並利用第 4 步：

$$q\big(\text{整數} + f(2n)\big) = p\big(\text{整數} - g(2n)\big).$$

移項整理後，$qf(2n) + pg(2n)$ 等於若干整數的組合，所以它是整數。這就是第 (iv) 部分。

> **停一停，試一試**　現在利用第 3 步的上下界。當 n 非常大時，$qf(2n) + pg(2n)$ 會怎樣？

$f(2n)$ 和 $g(2n)$ 都是正數，所以 $qf(2n) + pg(2n) > 0$。而且

$$qf(2n) + pg(2n) < \frac{q}{2n} + \frac{p}{2n+1} < \frac{p+q}{2n}.$$

選取 $n > (p+q)/2$。那麼 $qf(2n) + pg(2n)$ 就是一個嚴格介乎 0 與 1 之間的整數。這是不可能的，所以 e^2 是無理數。 ■

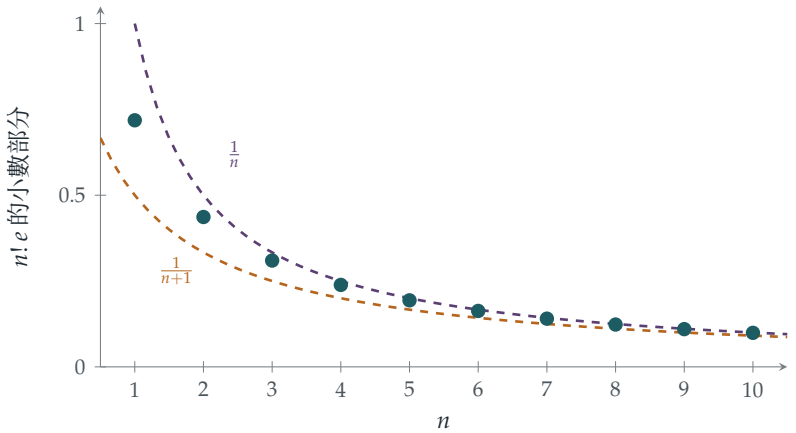


圖 1.4.1　尾部 $a_n = n!\,e - [n!\,e]$（青綠色），即 $n!\,e$ 的小數部分。它總是嚴格介乎 $\frac{1}{n+1}$ 與 $\frac{1}{n}$ 之間：永不為零，但小於 1。假如 e 是分數 $\frac{p}{q}$，那麼對每個 $n \geq q$，$n!\,e$ 都會是整數，青綠色的點就會是 0。

回顧

- **推動整個證明的是「沒有整數嚴格介乎 0 與 1 之間」。**兩個證明都構造出一個必定是整數的量，然後把它困住。
- **階乘令尾部變小。**乘以 $n!$ 把級數的開首部分變成整數，剩下一個像 $1/n$ 那樣縮小的尾部。
- **正面進攻失敗時，就重新整理。**我們沒有正面處理 $e^2 = p/q$，而是把它改寫成 $qe = p/e$，把困難分攤到兩個較易處理的數上。
- **細節很重要。**選用 $2n$ 而非 n，固定了尾部的符號。許多證明的成敗，都取決於這樣的一個小細節。

背後的數學

e 有多「無理」？

劉維爾（Joseph Liouville）在 1840 年證明了 e^2 是無理數，而且事實上它不滿足任何整數係數的二次方程。1873 年，埃爾米特（Charles Hermite）走得遠得多：他證明了 e 是*超越數*（transcendental number），意思是它不是任何整數係數多項式的根。他的證明正是上述論證的精密版本：構造一個整數，再證明它嚴格介乎 0 與 1 之間。九年後，林德曼（Ferdinand von Lindemann）改造了埃爾米特的方法，證明 π 是超越數，終於證實以尺規「化圓為方」這個古老問題是不可能做到的。

我們仍未知道的事

儘管這些方法威力強大，一些簡單得令人尷尬的問題卻仍未解決。$e + \pi$ 是無理數嗎？$e\pi$ 呢？沒有人知道，雖然兩者之中至少有一個必定是超越數（練習 4）。$\zeta(3) = 1 + \frac{1}{8} + \frac{1}{27} + \cdots$ 是無理數嗎？是的：阿培里（Roger Apéry）在 1978 年證明了這一點，震驚了整個數學界。$\zeta(5)$ 呢？沒有人知道。

逼近

這些證明背後有一個更深刻的想法：如果一個數能被分數逼近得*太好*，它就是無理數。e 的級數的部分和（partial sum）都是分數，而且很快就非常接近 e；一個分數不可能被其他分數逼近得那麼好。這就是*丟番圖逼近*（Diophantine approximation）的起點。它是數論的一個分支，你可以在 Section 2.9 進一步探索，那裏會用另一族積分得出更好的分數，步步逼近 e。

思維技巧

困住一個整數

要證明一個數是無理數，先假設它是分數，由此構造一個必定是整數的量，再證明這個量嚴格介乎 0 與 1 之間。

箇中的藝術在於選擇這個量。在這裏，乘以階乘把級數的大部分變成整數，剩下一個細小但為正數的尾部。

延伸練習

1 **只用 $1/e$。**假設 $1/e = p/q$，並只利用 $1/e$ 的交錯級數，證明 e 是無理數。

2 $\sin 1$ **是無理數。**利用 $\sin 1 = 1 - \dfrac{1}{3!} + \dfrac{1}{5!} - \cdots$ 證明 $\sin 1$ 是無理數。（乘以一個合適的奇數的階乘。）

3 **為何 π 不行？**解釋為何這個方法不能直接用於 π。然後查閱 Ivan Niven 在 1947 年發表、只有一頁的 π 是無理數的證明，當中用的是積分而不是級數。能力強的高級程度（A-level）學生應可讀懂。

4 **其中一個是超越數。**較難 證明 e 和 π 是 $x^2 - (e+\pi)x + e\pi = 0$ 的根。你可以假設：若一個多項式的係數都是代數數（algebraic number），則它的根本身也是代數數；以及 π 不是代數數（林德曼）。由此推出 $e+\pi$ 和 $e\pi$ 之中至少有一個是超越數。

延伸閱讀

- **Aigner & Ziegler,** ***Proofs from THE BOOK***，第 8 章「Some irrational numbers」（一些無理數）。正是用這些想法，證明 e、e^2、e^4 和 π^2 都是無理數。
- **Ivan Niven,** ***Irrational Numbers***（Mathematical Association of America）。一本篇幅不長的經典，內容由 $\sqrt{2}$ 一直談到超越性。
- **Julian Havil,** ***The Irrationals***（Princeton University Press）。一本淺白易讀的無理數歷史。

1.5 無窮遞降法

題目

STEP III 2022，第 2 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2022 年 STEP 試卷（zip 檔案）內的 STEP III 試卷：

`www.ocr.org.uk/Images/696587-2022-past-papers.zip`

引子

怎樣才能證明一條方程沒有整數解？你不可能逐一試遍所有可能，因為可能性有無窮多個。費馬（Pierre de Fermat）在 1630 年代找到了一個方法：證明任何一個解都會產生另一個數字更小的解，然後又產生一個更小的，如此無休止地繼續下去。可是正整數不可能永無止境地愈變愈小。所以，從一開始就根本沒有解。

費馬把這個方法稱為*無窮遞降法*（method of infinite descent），並且深以為傲。它是 Section 1.3 中良序原理（well-ordering principle）的另一面，至今仍是證明方程無解的主要工具之一。

動筆之前

四個部分的格局都一樣：假設有解，把解縮小，得出矛盾（contradiction）。問題在於怎樣縮小。

想一想 在第 (i) 部分，看看 $a^3 + 2b^3 + 4c^3 = 0$。三項之中有兩項明顯是偶數。這告訴你第三項有甚麼性質？

每一次遞降都是由這類觀察開始的：某種整除性（divisibility）是你無法迴避的。

逐步解題

階段 1　第一次遞降

由於 $a^3 = -2b^3 - 4c^3$，a^3 這個數是偶數，所以 a 是偶數（奇數的立方是奇數）。設 $a = 2p$。那麼 $|p| = |a|/2 < |a|$，代入後得

$$8p^3 + 2b^3 + 4c^3 = 0 \quad \Longrightarrow \quad 4p^3 + b^3 + 2c^3 = 0.$$

想一想 新的方程是 $4p^3 + b^3 + 2c^3 = 0$。它的係數和原來一樣，只是輪換了位置。你可以再用同一招嗎？

現在 $b^3 = -4p^3 - 2c^3$ 是偶數，所以 $b = 2q$，其中 $|q| < |b|$，再除以 2 便得 $2p^3 + 4q^3 + c^3 = 0$。同樣地，c 必定是偶數：$c = 2r$，其中 $|r| < |c|$，再除以 2，

$$p^3 + 2q^3 + 4r^3 = 0.$$

這正是原來的方程，只是以 p、q、r 取代了 a、b、c。每個數的大小都減半，而且沒有一個是零，因為把非零的數減半不可能得到零。

停一停，試一試 把以上論證寫成一個證明（proof），說明非零解並不存在。你究竟應該假設甚麼是「最小」的？

在所有非零整數解之中，選取 $|a|$ 最小的一個。（只要有解存在，良序原理就容許我們這樣做。）上述論證會產生另一個非零解，並且 $|p| < |a|$，與最小性矛盾。所以沒有非零解。 ■

另一個等價的說法是：由一個解出發，我們可以構造出無窮多個解，它們滿足 $|a| > |p| > \cdots$，即一個嚴格遞減的無窮正整數數列，而這是不可能的。

階段 2　換一個質數

想一想 在 $9a^3 + 10b^3 + 6c^3 = 0$ 中，奇偶性（parity）看來幫不上忙。看看係數 9、10、6。哪一個質數（prime）整除其中兩個？

質數 3 整除 9 和 6，所以 3 整除 $10b^3$，因此 3 整除 b。設 $b = 3q$ 並除以 3：

$$3a^3 + 90q^3 + 2c^3 = 0.$$

現在 3 整除 $2c^3$，所以 $c = 3r$；再除以 3 得 $a^3 + 30q^3 + 18r^3 = 0$。於是 3 整除 a：$a = 3p$，再除以 3 一次，

$$9p^3 + 10q^3 + 6r^3 = 0.$$

這與原來的方程完全相同，只是換成了較小的非零數。根據同樣的遞降論證，方程沒有非零解。 ■

階段 3　模 3 下的平方數

想一想 每個整數都可寫成 $3n$、$3n+1$ 或 $3n-1$ 的形式。它們的平方模（modulo）3 是甚麼？

$(3n \pm 1)^2 = 9n^2 \pm 6n + 1 = 3(3n^2 \pm 2n) + 1$，比 3 的倍數多一。而 $(3n)^2$ 是 3 的倍數。所以平方數除以 3 的餘數（remainder）是 0 或 1，永遠不會是 2。

現在如果 $a^2 + b^2$ 是 3 的倍數，餘數的可能組合是 $0+0$、$0+1$、$1+0$ 和 $1+1$，分別得出 0、1、1、2。只有第一種是 3 的倍數，所以 a 和 b 都必定是 3 的倍數。

想一想 如果 $a^2 + b^2 = 3c^2$，而 $a = 3p$、$b = 3q$，你對 c 有甚麼結論？

我們得到 $9p^2 + 9q^2 = 3c^2$，所以 $c^2 = 3(p^2 + q^2)$ 是 3 的倍數，因此 $c = 3r$。於是 $9p^2 + 9q^2 = 27r^2$，即 $p^2 + q^2 = 3r^2$：同一條方程，較小的數。又是遞降。 ■

階段 4 變奏：方程變了

想一想 在 $a^2 + b^2 + c^2 = 4abc$ 中，右邊是 4 的倍數。平方數模 4 是甚麼？

偶數的平方是 4 的倍數，奇數的平方則比 4 的倍數多一（$(2n+1)^2 = 4n^2 + 4n + 1$）。所以 $a^2 + b^2 + c^2$ 除以 4 的餘數是 0、1、2 或 3，視乎 a、b、c 之中有多少個是奇數。由於右邊是 4 的倍數，它們*沒有一個*可以是奇數。設 $a = 2p$、$b = 2q$、$c = 2r$：

$$4(p^2 + q^2 + r^2) = 32\,pqr \quad \Longrightarrow \quad p^2 + q^2 + r^2 = 8\,pqr.$$

想一想 這並不是同一條方程：4 變成了 8。遞降法還行得通嗎？

竅門在這裏：*證明一個更強的命題*。考慮所有以下形式的方程

$$x^2 + y^2 + z^2 = 2^m\,xyz \qquad \text{其中} m \geq 2.$$

對任何這樣的 m，右邊都是 4 的倍數，所以完全相同的論證顯示 x、y、z 全是偶數。把它們減半，便得到含 2^{m+1} 的方程的一個解，而這條方程仍屬這種形式。因此，由 m 方程的一個非零解，我們得到 $m+1$ 方程的一個較小的非零解。在這個方程族中*任何一條*方程的所有解之中，取 $|x|$ 最小的一個，便得出矛盾。特別地，$a^2 + b^2 + c^2 = 4abc$ 沒有非零解。 ■

有時候，你想證明的命題太弱，不足以支撐它自身的歸納（induction），補救的方法是證明一個更一般、能夠自我支撐的命題。這個技巧在大學裏出奇地常見。

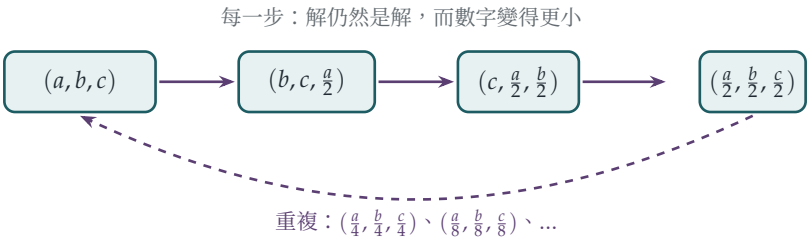


圖 1.5.1　第 (i) 部分的遞降。由 $a^3+2b^3+4c^3=0$ 的一個解出發，三步之後得到另一個解，每個分量都減半。無休止地重複下去，便會得出一個沒有盡頭的遞減正整數數列 $|a|>|\frac{a}{2}|>|\frac{a}{4}|>\cdots$，而這是不可能的。所以一開始就沒有解。

回顧

- **遞降需要整除性的來源。**每一次，我們都找到一個質數 p（這裏是 2 或 3），它必然整除所有變數，然後把它除去。
- **模 n 運算正是找出它的方法。**考察模 2、3 或 4 的餘數，把「有沒有任何可能行得通？」變成一個簡短的有限驗證。
- **如果方程變了，就推廣。**第 (iv) 部分需要一整族方程，而這一族方程在遞降步驟下是封閉的。

背後的數學

費馬、遞降法與他的最後定理

費馬用無窮遞降法證明了 $x^4+y^4=z^2$ 沒有正整數解。在他著名的「最後定理」之中，這是他唯一留下證明的情況，它解決了 $x^n+y^n=z^n$ 在 $n=4$ 時的情形。歐拉（Euler）其後用遞降法處理 $n=3$ 的情形，當中有一個漏洞，後來才被補上。遞降法至今仍是現代理論的起點：關於 Section 1.9 中那類曲線的莫德爾–韋伊定理（Mordell–Weil theorem），其證明就是一個精密的遞降。

局部障礙

本節的每一個證明，都是靠考察模某個數的餘數來完成的。如果一條方程對某個 n 而言模 n 無解，或者沒有實數解，它當然沒有整數解。這類理由稱為*局部障礙*（local obstructions）；到了大學，你會遇到 p 進數（p-adic numbers），那是一種同時研究模 $p, p^2, p^3, \ldots$ 所有餘數的方法。

哈塞（Hasse）與閔可夫斯基（Minkowski）有一個精彩的定理：對於像 $a^2+b^2=3c^2$ 這樣的二次方程，局部障礙就是僅有的障礙——如果沒有任何「局部」的理由令它無解，它就確實有有理數解。對三次方程而言，這個結論卻徹底失效。Ernst Selmer 在 1951 年證明了

$$3x^3+4y^3+5z^3=0$$

模任何整數都有解，在實數中也有解，但沒有非零整數解。解釋「局部到整體」原理何時失效、為何失效，是現代數論的一大主題。

一條確實有解的方程

第 (iv) 部分有一個著名的近親：$x^2+y^2+z^2=3xyz$，即**馬爾可夫方程**（Markov equation）。它有無窮多個正整數解，由 $(1,1,1)$、$(1,1,2)$、$(1,2,5)$、$(1,5,13)$ 和 $(2,5,29)$ 開始，而這些解與無理數能被分數逼近到甚麼程度有關。見練習 4。

思維技巧

無窮遞降法

要證明一條方程無解，可證明任何一個解都會產生一個嚴格更小的解。這樣，最小的解便不可能存在。

把它與模 n 運算配合使用，找出推動遞降的整除性；如果命題在遞降步驟下不能保持，就要準備把命題推廣。

延伸練習

1 **STEP I 熱身題。**（*STEP I 2010 第 8 題。*）證明 $a^3+3b^3=9c^3$ 的唯一整數解是 $a=b=c=0$。然後，藉考慮末位數字，證明 $p^4+2q^4=5r^4$ 也有同樣的結論。

2 **只用模運算，毋須遞降。**只用模 4 運算，證明 $x^2+y^2=4z+3$ 完全沒有整數解。

3 **有理點。**利用第 (iii) 部分，證明圓 $x^2+y^2=3$ 上沒有坐標為有理數的點。（試與 $x^2+y^2=2$ 對比，後者包含 $(1,1)$。）

4 **馬爾可夫三元組。**證明若 (x,y,z) 滿足 $x^2+y^2+z^2=3xyz$，則 $(x,y,3xy-z)$ 亦滿足。由 $(1,1,1)$ 出發，生成上文列出的三元組。（這個「跳躍」技巧正好與遞降相反。）

延伸閱讀

- **Harold Davenport, *The Higher Arithmetic***，第 2 及第 5 章。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***（Pearson）。非常易讀；包括費馬對 $x^4 + y^4 = z^2$ 的遞降證明。
- **Simon Singh, *Fermat's Last Theorem***（Fourth Estate）。為一般讀者而寫的故事，由費馬的頁邊筆記講到懷爾斯（Wiles）的證明。

1.6 兩個平方數之和

題目

STEP II 2023，第 7 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2023 年 STEP 試卷（zip 檔案）內的 STEP II 試卷：

`www.ocr.org.uk/Images/707102-2023-past-papers.zip`

引子

哪些整數可以寫成兩個平方數之和？$5 = 1^2 + 2^2$ 和 $13 = 2^2 + 3^2$ 可以，但 3、7 和 21 卻不行。這裏有一個奇怪的事實：$65 = 5 \times 13$ 可以用兩種不同的方法寫成兩個平方數之和，即 $1^2 + 8^2$ 和 $4^2 + 7^2$。為甚麼兩個這樣的數相乘，會得出另一個這樣的數？又為甚麼會有兩種寫法？

答案來自一個意想不到的方向。這道題目要你放下整數，改用複數（complex number）來思考。在複數的世界裏，兩平方和變得很簡單，一些看似令人摸不着頭腦的算術也變得近乎機械化。

動筆之前

? **想一想** 若 $z = a + \mathrm{i}b$，其中 a 和 b 為整數，那麼 $|z|^2$ 是甚麼？

它是 $a^2 + b^2$，即兩個平方數之和。所以「N 是兩個平方數之和」的意思正正就是「存在某個實部（real part）和虛部（imaginary part）皆為整數的複數 z，使得 $N = |z|^2$」。這樣的複數稱為高斯整數（Gaussian integer）。請牢記這個轉譯；整道題目都建基於此。

逐步解題

階段 1　模相乘

想一想 以 a、b、c、d 寫出 zw。關於 $|zw|^2$，你需要證明甚麼？

我們有 $zw = (ac - bd) + \mathrm{i}(ad + bc)$，所以

$$|zw|^2 = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2,$$

因為交叉項 $-2abcd$ 和 $+2abcd$ 互相抵消。而這個式子可以因式分解（factorise）：

$$a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = |z|^2|w|^2.$$

取平方根，得 $|zw| = |z||w|$。 ■

現在把它看成一個關於整數的命題：

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (\star)$$

兩個兩平方和的乘積，仍是一個兩平方和，而複數更確切地告訴你那兩個平方數是甚麼。

階段 2　學以致用

第 (ii) 部分：$5 = |2 + \mathrm{i}|^2$，而 $221 = 10^2 + 11^2 = |10 + 11\mathrm{i}|^2$。於是相乘：

$$(2 + \mathrm{i})(10 + 11\mathrm{i}) = 20 + 22\mathrm{i} + 10\mathrm{i} - 11 = 9 + 32\mathrm{i},$$

得出 $5 \times 221 = 9^2 + 32^2$。（驗算：$81 + 1024 = 1105$。）

想一想 如果改為把 $10 + 11\mathrm{i}$ 乘以 $2 - \mathrm{i}$，會怎麼樣？它的模（modulus）與 $2 + \mathrm{i}$ 的相同。

$(2 - \mathrm{i})(10 + 11\mathrm{i}) = 20 + 22\mathrm{i} - 10\mathrm{i} + 11 = 31 + 12\mathrm{i}$，所以同樣有 $1105 = 31^2 + 12^2$。選用 $2 + \mathrm{i}$ 還是它的共軛（conjugate），會得出不同的表示法。這就解釋了引子中 65 的兩種寫法（圖 1.6.1）：$65 = |(2 + \mathrm{i})(3 + 2\mathrm{i})|^2 = |4 + 7\mathrm{i}|^2$ 以及 $65 = |(2 - \mathrm{i})(3 + 2\mathrm{i})|^2 = |8 + \mathrm{i}|^2$。

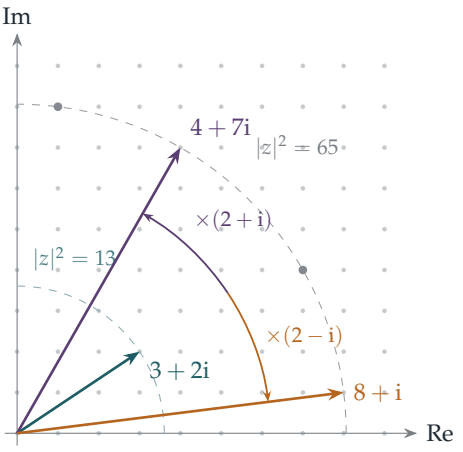


圖 1.6.1　乘以 $2 \pm \mathrm{i}$ 會把長度放大 $\sqrt{5}$ 倍，並旋轉約 26.6°：$2 + \mathrm{i}$ 為逆時針方向，$2 - \mathrm{i}$ 為順時針方向。由圓 $|z|^2 = 13$ 上的 $3 + 2\mathrm{i}$ 出發，兩種選擇會落在圓 $|z|^2 = 65$ 上不同的格點（lattice point）。灰色的點是它們對直線 $y = x$ 的反射。

階段 3　先作因式分解

想一想　8045 的末位數字是 5。這提示了甚麼？

$8045 = 5 \times 1609$。我們需要把 1609 寫成兩個平方數之和；試試略小於 1609 的平方數，很快便找到 $1609 = 40^2 + 3^2$。於是

$$(2 + \mathrm{i})(40 + 3\mathrm{i}) = 77 + 46\mathrm{i}, \qquad \text{所以} \qquad 8045 = 77^2 + 46^2,$$

而共軛亦給出 $8045 = 83^2 + 34^2$。

第 (iv) 部分更快：$36 = 6^2 + 0^2$，而乘以 6 只是按比例放大：$36 \times 50805 = 612^2 + 1206^2$。

階段 4　三種寫法

想一想　25 可以用多於一種方法寫成兩個平方數之和。若不計正負號和次序對調，有多少個高斯整數的模為 5？

$25 = 5^2 + 0^2 = 3^2 + 4^2$，分別對應 5、$3 + 4\mathrm{i}$ 和 $3 - 4\mathrm{i}$。接着看 1002082：由於 $1001^2 = 1002001$，我們有 $1002082 = 1001^2 + 9^2$。把 $1001 + 9\mathrm{i}$ 分別乘以這三個數，得：

$$5\,(1001 + 9\mathrm{i}) = 5005 + 45\mathrm{i},$$
$$(3 + 4\mathrm{i})(1001 + 9\mathrm{i}) = 2967 + 4031\mathrm{i},$$
$$(3 - 4\mathrm{i})(1001 + 9\mathrm{i}) = 3039 - 3977\mathrm{i}.$$

所以三對 (r, s) 是 $(45, 5005)$、$(2967, 4031)$ 和 $(3039, 3977)$。

階段 5　除法

> **停一停，試一試**　第 (vi) 部分把這部機器倒過來運轉。我們知道 $109 = 10^2 + 3^2$ 和 $1002037 = 1001^2 + 6^2$。怎樣才能不靠搜尋，就把 9193 寫成兩個平方數之和？

既然高斯整數相乘時模會相乘，那麼相除時模就應該相除。試試

$$\frac{1001 + 6\mathrm{i}}{10 + 3\mathrm{i}} = \frac{(1001 + 6\mathrm{i})(10 - 3\mathrm{i})}{109} = \frac{10028 - 2943\mathrm{i}}{109} = 92 - 27\mathrm{i}.$$

剛好整除，所以 $9193 = 92^2 + 27^2$。（驗算：$8464 + 729 = 9193$。）

> **想一想**　如果改為除以 $10 - 3\mathrm{i}$，會怎麼樣？

你會得到 $(1001 + 6\mathrm{i})(10 + 3\mathrm{i})/109 = (9992 + 3063\mathrm{i})/109$，這不是高斯整數，因為 9992/109 不是整數。在 109 的兩個「因數」之中，只有一個能整除 $1001 + 6\mathrm{i}$，正如只有某些質數（prime）能整除一個給定的整數。高斯整數有它們自己的質數，也有它們自己的因式分解。

回顧

- **轉譯、求解、再譯回來。**「兩個平方數之和」變成了「高斯整數的模的平方」。用這種語言來說，問題就變得容易。
- **先作因式分解。**每一部分都是先把一個大數拆成較小的數，而這些較小的數的表示法很容易找到。
- **共軛帶來新答案。**表示法的數目，取決於有多少種方法選擇一個因數或它的共軛。

背後的數學

費馬二平方和定理

哪些質數是兩個平方數之和？$2 = 1^2 + 1^2$、5、13、17、29、37、41 是；3、7、11、19、23、31 則不是。規律是：除 2 以外，一個質數是兩個平方數之和，當且僅當它除以 4 的餘數為 1。費馬（Fermat）於 1640 年提出這個結果；歐拉（Euler）於 1749 年給出證明。用高斯整數的語言來說：質數 $p \equiv 1 \pmod 4$ 會分裂（split）成 $p = (a + b\mathrm{i})(a - b\mathrm{i})$，而質數 $p \equiv 3 \pmod 4$ 則仍然是質數。例如 $5 = (2 + \mathrm{i})(2 - \mathrm{i})$，但 3 完全無法分解。

1990 年，Don Zagier 發表了二平方和定理的一個證明，它以全長只有一句而聞名。這

個證明連同解說收錄於 *Proofs from THE BOOK*。

一個擁有自己質數的新數系

高斯（Gauss）發現，高斯整數的表現與普通整數極為相似。它們有除法算法（division algorithm）和歐幾里得算法（Euclidean algorithm），而且每個高斯整數都可以唯一地分解成高斯質數（Gaussian prime）的乘積（不計乘以 ± 1 或 $\pm i$ 的差別）。結合 $(\star)$，你只需知道一個數的質因數分解，就能準確數出它有多少種方法寫成兩個平方數之和。

在大學裏，這是通往代數數論（algebraic number theory）的大門：研究 $\mathbb{Z}[i]$ 或 $\mathbb{Z}[\sqrt{-5}]$ 這類數系，藉此了解普通的整數。Section 1.7 說明了為甚麼需要創立這門學科：並非每個這樣的數系都像高斯整數那樣規矩。

四個平方數及其他

每個正整數都是四個平方數之和（拉格朗日（Lagrange），1770 年）。證明依賴 $(\star)$ 的四平方版本，它源自哈密頓（Hamilton）的四元數（quaternion），情形就如 $(\star)$ 源自複數一樣。你會在 Section 7.8 見到它。

思維技巧

轉換場景

一個問題在某個數系中顯得棘手，在一個更大的數系中卻可能十分自然。

兩平方和在整數中很棘手，在複數中卻不過是模而已。數學家經常這樣擴大數系：由整數到有理數，由有理數到實數，由實數到複數。每次擴大，都會令一些舊問題變得容易。

延伸練習

1. **一個障礙。**證明沒有任何形如 $4k+3$ 的數是兩個平方數之和。（平方數模 4 是甚麼？）
2. **兩種寫法。**把 65 和 85 各自用兩種不同的方法寫成兩個平方數之和，並用高斯整數解釋你的答案。
3. **四種寫法。**$1105 = 5 \times 13 \times 17$。找出四種不同的方法，把 1105 寫成兩個正平方數之和。為甚麼是四種？

4 **高斯質數。** 較難 證明若 $3 = (a + bi)(c + di)$，其中 a, b, c, d 為整數，則其中一個因數的模為 1。（取模的平方。）這說明 3 是高斯質數。

延伸閱讀

- **John Stillwell, *Elements of Number Theory***（Springer）。循序漸進講到高斯整數及更深入的內容，並附歷史背景。
- **Aigner & Ziegler, *Proofs from THE BOOK***，第 4 章，“Representing numbers as sums of two squares”（把數表示為兩個平方數之和）。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***，有關平方和與高斯整數的各章。

1.7 因數分解失效之時

題目

STEP I 2016，第 7 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/16-s1-q7`

引子

每個大於 1 的整數都可以寫成質數（prime）的乘積，而且寫法只有一種：$60 = 2 \times 2 \times 3 \times 5$，再沒有別的寫法。這個事實你大概已經用過無數次，熟悉得讓人覺得顯然成立，根本不用證明。

這道題構造了一個小小的數字世界，看上去完全合情合理，但在這個世界裏，那個「顯然」的事實卻是錯的。這是一道 STEP I 的題目，所用的數學並不艱深，但當中的教訓卻十分深刻。1847 年，一個著名的費馬最後定理（Fermat's Last Theorem）證明嘗試，正是敗在這個教訓之上，而代數學的一個全新分支亦因此誕生。

動筆之前

想一想 列出 S 和 T 的首幾個元素。按照第 (iv) 部分的定義，S 的哪些元素是S-質數？

$S = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$，而 $T = \{3, 7, 11, 15, 19, 23, \ldots\}$。$S$ 中的一個數如果不能寫成 S 中較小元素（1 除外）的乘積，它就是 S-質數。留意 9 是 S-質數，儘管在普通整數中 $9 = 3 \times 3$，因為 3 並不在 S 之中。一個數是否「質數」，取決於你獲准使用哪些數。

逐步解題

階段 1　併集、交集與乘積

$S \cup T$ 是所有正奇數組成的集合，即兩者的併集（union），因為每個奇數除以 4 的餘數不是 1 就是 3。$S \cap T$ 是空集，即兩者的交集（intersection）沒有任何元素，因為沒有一個數會有兩個不同的餘數。

> **想一想**　S 的一般元素應該怎樣寫？兩個這樣的元素相乘，乘積是甚麼？

S 的元素是 $4a+1$，其中 $a \geq 0$，而

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1 \in S.$$

所以 S 在乘法下封閉（closed）。至於 T：

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1,$$

這個數屬於 S，而不屬於 T。例如 $3 \times 7 = 21 \in S$。所以 T 在乘法下並不封閉。

階段 2　屬於 T 的質因數

> **想一想**　在 T 中取一個不是質數的數。它的質因數（prime factor）全是奇數。假如這些質因數全都屬於 S，會有甚麼後果？

這個數是奇數，所以它的質因數全是奇數，各自屬於 S 或 T。假如它們全部屬於 S，那麼由於 S 在乘法下封閉，它們的乘積也會屬於 S。但這個乘積就是我們原來的數，而它屬於 T。所以至少有一個質因數屬於 T。 ■

階段 3　奇數個因數

> **想一想**　把偶數個 T 的元素乘起來，乘積會落在哪裏？奇數個又如何？

每一對 T-數相乘都得到一個 S-數，而 S-數相乘仍然是 S-數，所以偶數個 T-因數的乘積屬於 S。奇數個的話，乘積就是（S 中的某個數）$\times$（T 的一個元素），用同類的計算可知它屬於 T。

現在取 $t \in T$。如果 t 是 T-質數，那就完成了。否則，把 t 寫成 T 的元素的乘積，其中每個元素都大於 1，因而小於 t。當中任何不是 T-質數的因數都可以再分解下去，如此類推。因數每次都變小，所以這個過程必會停止（這裏再次用到良序性質（well-ordering）），最後 t 就寫成了 T-質數的乘積。由於乘積屬於 T，因數的個數必定是奇數。 ■

階段 4　兩種分解

> **停一停，試一試** 在 S 中找一個數，它有兩種真正不同的 S-質數分解。提示：利用像 9 這樣的數，它們之所以是 S-質數，只因為它們在普通整數中的質因數並不在 S 之中。

S-質數依次為 $5, 9, 13, 17, 21, 29, 33, 37, 41, 49, \ldots$。$21 = 3 \times 7$、$9 = 3 \times 3$ 和 $49 = 7 \times 7$ 全都是 S-質數，因為 3 和 7 都不在 S 之中。而且

$$441 = 21 \times 21 = 9 \times 49.$$

這就是 441 的兩種不同的 S-質數分解（圖 1.7.1）。唯一分解（unique factorisation）在 S 中並不成立。 ■

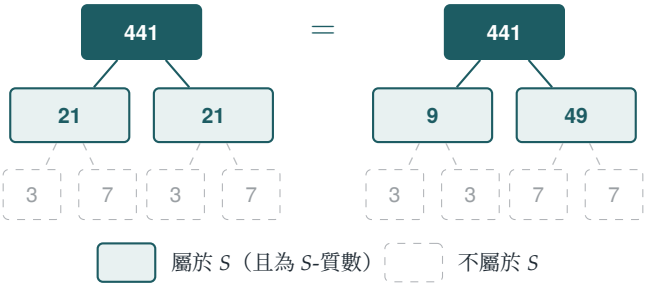


圖 1.7.1 441 的兩種 S-質數分解。在普通整數中，兩棵樹都會繼續向下分解至 $3 \times 3 \times 7 \times 7$，但 3 和 7 都不在 S 之中，所以在 S 之內，分解到第二行便停止，而兩種分解並不相同。

回顧

- **是否「質數」取決於所在的系統。**9 和 21 在整數中是合數（composite），在 S 中卻是質數，因為分解它們所需的數並不存在。
- **封閉性很重要。**S 在乘法下封閉；T 則不然。第 (iii) 和第 (iv) 部分的論證，全靠這一點分別。
- **顯然的事實也可以是一條定理。**整數的唯一分解是需要證明的。這道題說明了原因：在一個看上去非常相似的系統中，它並不成立。

背後的數學

整數有何特別之處

為甚麼分解在普通整數中確實行得通？關鍵在於歐幾里得引理（Euclid's lemma）：如果質數 p 整除乘積 ab，那麼 p 整除 a 或 p 整除 b。這條引理是用輾轉相除法（Euclidean

algorithm）證明的，而它正正是在 S 中失效的地方。在那裏，S-質數 9 整除 $21 \times 21 = 441$（因為 $441 = 9 \times 49$），但 9 在 S 中並不整除 21。到了大學一年級，你會嚴謹地證明歐幾里得引理，並看到唯一分解如何由它推導出來。

費馬最後定理的失敗證明

1847 年 3 月 1 日，拉梅（Gabriel Lamé）向巴黎科學院宣布，他已證明了費馬最後定理。他的想法是利用複數單位根（roots of unity）把 $x^n + y^n$ 分解，

$$x^n + y^n = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y), \qquad \zeta = e^{2\pi \mathrm{i}/n}$$

（其中 n 為奇數），然後就每個括號的質因數進行論證。劉維爾（Joseph Liouville）隨即提出質疑：由 ζ 構成的數，憑甚麼一定有唯一分解？數星期後，人們才知道庫默爾（Ernst Kummer）早已證明這類數往往沒有唯一分解。最先失效的情況是 $n = 23$。

庫默爾盡力補救，發明了「理想數」（ideal numbers），這些額外的對象能夠恢復唯一分解，他並藉此對一大類指數證明了費馬最後定理。戴德金（Richard Dedekind）把庫默爾的理想數發展成*理想*（ideal），成為近世代數的核心概念之一。

一個值得記住的較小例子

在數系 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ 中，

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

而這四個因數在該數系中全都是「質數」（練習 3）。試把這個例子與 Section 1.6 的高斯整數（Gaussian integers）比較，後者的分解*確實*是唯一的。這類數系之中哪些具有唯一分解，是一個很深刻的問題。高斯（Gauss）猜想，在形如 $\mathbb{Z}[\sqrt{-d}]$ 的數系及與其相近的數系之中，只有九個具有唯一分解。這個猜想最終由黑格納（Heegner）、貝克（Baker）和斯塔克（Stark）在 1952 年至 1967 年間證明。

思維技巧

> **質疑你視為理所當然的事**
>
> *當一個事實看來顯然得不用證明時，問問它依賴甚麼，並找出一個令它失效的情境。*
>
> 構造反例（counterexample），也就是構造一個令「顯然」的事實不成立的世界，是弄清一個證明真正需要甚麼的最佳方法之一。大學本科代數有很大部分，就是

在探問整數那些熟悉的性質，有哪些能在更一般的系統中保留下來。

延伸練習

1 **另一個例子。**證明 693 有兩種不同的 S-質數分解。你能找出一個製造這類例子的通用方法嗎？

2 **偶數。**設 $E = \{2, 4, 6, 8, \ldots\}$。哪些數是 E-質數？證明 60 有多於一種 E-質數分解。

3 $\mathbb{Z}[\sqrt{-5}]$。定義範數（norm）$N(a + b\sqrt{-5}) = a^2 + 5b^2$。證明 $N(zw) = N(z)N(w)$。先證明沒有任何元素的範數是 2 或 3，由此推導出 2、3 和 $1 \pm \sqrt{-5}$ 在 $\mathbb{Z}[\sqrt{-5}]$ 中不能再分解。

4 **歐幾里得引理的應用。**較難 假設歐幾里得引理成立（如果一個質數整除 ab，它就整除 a 或 b），證明每個大於 1 的整數都只有一種質數分解，因數的次序不計。

延伸閱讀

- **Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem***（CRC Press）。開首幾章講述拉梅、庫默爾與理想的故事，程度適合好學的大學一年級學生。
- **John Stillwell, *Elements of Number Theory***。把整數的唯一分解與高斯整數的唯一分解並列比較。
- **Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction***（Springer）。適合有志挑戰的讀者：循歷史發展解說庫默爾的工作。

1.8 點算有理數

題目

STEP III 2020，第 8 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2020 年 STEP 試卷（zip 檔案）內的 STEP III 試卷：

`www.ocr.org.uk/Images/696589-2020-past-papers.zip`

引子

你能否把所有正分數逐一列出，使每個分數都恰好出現一次？這看來是不可能的：任意兩個分數之間還有無窮多個分數，根本沒有「下一個」分數可以寫下來。然而，康托爾（Georg Cantor）在 1870 年代證明了這是做得到的。這表示，在某個精確的意義下，分數並不比整數多。

康托爾的列表頗為笨拙：表中既有 $\frac{1}{2}$，也有 $\frac{2}{4}$，重複的項要逐一刪去。本題要構造的列表卻完全沒有重複，而且來自一個規則簡單得出奇的數列（sequence）。這個列表由 Neil Calkin 和 Herbert Wilf 於 2000 年發表，不過數列本身早在 1858 年已由 Moritz Stern 研究過。

動筆之前

想一想 在證明任何東西之前，先計算最初十五項左右。你留意到比值 u_n/u_{n+1} 有甚麼特別之處？

數列的開首幾項是

$$1,\ 1,\ 2,\ 1,\ 3,\ 2,\ 3,\ 1,\ 4,\ 3,\ 5,\ 2,\ 5,\ 3,\ 4,\ 1,\ 5,\ \ldots$$

而比值 u_n/u_{n+1} 依次是

$$\frac{1}{1},\ \frac{1}{2},\ \frac{2}{1},\ \frac{1}{3},\ \frac{3}{2},\ \frac{2}{3},\ \frac{3}{1},\ \frac{1}{4},\ \frac{4}{3},\ \frac{3}{5},\ \frac{5}{2},\ \frac{2}{5},\ \frac{5}{3},\ \frac{3}{4},\ \frac{4}{1},\ \ldots$$

每個分數都以最簡分數（lowest terms）的形式出現，而且沒有一個重複。題目要你證明

這個現象會一直持續下去，並且每個正分數遲早都會出現。

逐步解題

階段 1　奇數項勝過偶數項

相鄰兩項不是 (u_{2k}, u_{2k+1})，就是 (u_{2k+1}, u_{2k+2})。

> **想一想**　試用 u_k 和 u_{k+1} 表示這兩種數對。哪一項較大？

$(u_{2k}, u_{2k+1}) = (u_k,\ u_k + u_{k+1})$，而 $(u_{2k+1}, u_{2k+2}) = (u_k + u_{k+1},\ u_{k+1})$。由於每一項都是正整數（用歸納法（induction）不難證明），$u_k + u_{k+1}$ 比 u_k 和 u_{k+1} 都大。唯一的例外是第一對 $(u_1, u_2) = (1, 1)$，它不符合上述任何一種形式，因為 u_1 是直接定義的。 ■

階段 2　相鄰兩項互質

> **想一想**　假設 $d > 1$ 同時整除 u_{2k} 和 u_{2k+1}，即同時整除 u_k 和 $u_k + u_{k+1}$。那麼 d 還整除甚麼？

d 整除 $(u_k + u_{k+1}) - u_k = u_{k+1}$，所以 d 整除相鄰數對 u_k, u_{k+1}，而這一對在數列中的位置較前。另一種情況完全相同：若 d 整除 $u_k + u_{k+1}$ 和 u_{k+1}，它便整除 u_k。

因此，相鄰數對的公因數會傳回較前的一對，然後再傳回更前的一對，如此類推。位置不可能無止境地減小（又是良序性（well-ordering)），所以 d 最終必須整除第一對 $u_1 = u_2 = 1$。當 $d > 1$ 時這是不可能的。所以每一對相鄰項都互質（coprime）。 ■

階段 3　沒有數對出現兩次

> **停一停，試一試**　階段 1 告訴你一件有用的事：看到一個相鄰數對 (a, b) 時，你可以判斷 a 位於奇數位置還是偶數位置。怎樣判斷？然後，你能否還原出階段 2 所指的、在它之前的那個數對？

若 $a < b$，則（由階段 1）b 位於奇數位置，所以對某個 k，這個數對是 $(u_{2k}, u_{2k+1}) = (u_k, u_k + u_{k+1})$，而它的「父」數對 (u_k, u_{k+1}) 就是 $(a,\ b - a)$。若 $a > b$，這個數對是 (u_{2k+1}, u_{2k+2})，其父數對是 $(a - b,\ b)$。若 $a = b$，階段 1 表明這個數對必定是最初的一對 $(1, 1)$。

所以除第一對外，每個相鄰數對都決定了它的父數對，以及父數對的位置（這個結構可以看成一棵樹，見圖 1.8.1）：當子數對位於 $2k$ 或 $2k + 1$ 時，父數對位於位置 k。現在假設 (a, b) 出現在兩個不同的位置。它們的父數對便是出現在兩個位置的同一數對，而這

些父數對的父數對亦然，如此類推。這樣一直追溯上去，我們最終會在 1 以外的位置找到 $(1,1)$，而階段 1 已排除了這個可能。 ■

階段 4 每個互質數對都會出現

> **想一想** 假設某個互質數對 (a,b) 從未以相鄰兩項的形式出現。你應該考慮哪一個這樣的數對？

在所有「缺席」的互質數對之中，取 $a+b$ 的值最小的一個：這就是極小反例（minimal counterexample）。它不可能是 $(1,1)$，因為這一對確實出現了，所以 $a \neq b$（互質而又相等，必有 $a=b=1$）。

- 若 $a > b$：數對 $(a-b,b)$ 互質（$a-b$ 和 b 的任何公因數都整除 a），而它的和 a 小於 $a+b$。由極小性，這個數對確實出現，設它位於位置 $k,k+1$。但這樣便有 $u_{2k+1} = u_k + u_{k+1} = a$ 和 $u_{2k+2} = u_{k+1} = b$，所以 (a,b) 終究還是出現了。
- 若 $a < b$：同理，$(a,b-a)$ 出現在某個 $k,k+1$，於是 $(u_{2k},u_{2k+1}) = (a,b)$。

無論哪種情況都得出矛盾。所以每一對互質的正整數都會以相鄰兩項的形式出現。 ■

（題目把第 (iv) 部分寫成遞降法（descent）：一個缺席的數對會產生一個更小的缺席數對。這其實是同一個論證，只是倒過來讀而已。）

階段 5 所有分數的列表

每個正有理數（rational number）都可以唯一地寫成最簡分數 a/b，其中 a,b 互質。由階段 4，(a,b) 會以某個相鄰數對 (u_n,u_{n+1}) 的形式出現，所以 $f(n) = a/b$：f 的值域（range）是全體正有理數。由階段 3，它只出現一次；又由階段 2，每個值 $f(n)$ 本身已是最簡分數，所以兩個不同的 n 不可能給出同一個分數。因此 f 是由正整數到正有理數的雙射（bijection），並且有逆函數（inverse）。 ■

回顧

- **遞降與它的逆向。**公因數和重複的數對都是往回追溯到數列的起點。缺席的數對則用極小反例處理，向前構造。
- **雙射要證兩半。**「每個分數都出現」（滿射，onto）和「沒有分數出現兩次」（單射，one-to-one）是兩個獨立的命題，要分開證明。
- **先動手計算。**寫出十五項之後，這些命題便顯得可信，同時也提示了推動整個證明的父子結構。

背後的數學

Calkin–Wilf 樹

把正分數排成一棵樹：把 $\frac{1}{1}$ 放在頂端，並給每個分數 $\frac{a}{b}$ 兩個子節點，左邊是 $\frac{a}{a+b}$，右邊是 $\frac{a+b}{b}$。逐行由左至右讀這棵樹，得到的正是本題的列表 $f(1), f(2), f(3), \ldots$（圖 1.8.1）。階段 3 說明每個分數都有唯一的父節點，階段 4 說明每個分數都在樹中。2003 年，Moshe Newman 發現連這棵樹也不需要：列表中每個分數都可以由前一個分數算出，公式是

$$x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}.$$

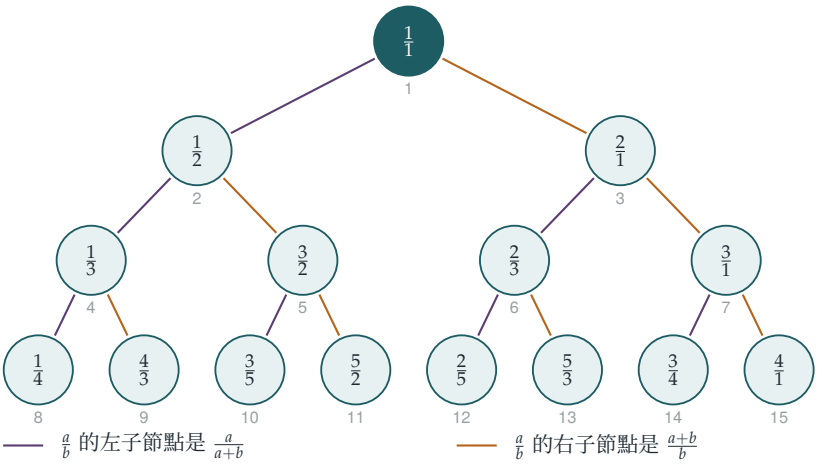


圖 1.8.1　Calkin–Wilf 樹的首四行。逐行由左至右讀，便得到 $f(1), f(2), f(3), \ldots$；灰色小數字是位置 n。每個正分數都以最簡分數的形式恰好出現一次。

不同大小的無窮

可以這樣逐一列出的集合稱為可數（countable）集合。分數是可數的，這令人意外，因為分數看來比整數多得多。在大學的第一個學期，你還會遇到康托爾的對角論證法（diagonal argument），它證明實數（real numbers）是不可數的：任何實數列表都必定有所遺漏。所以無窮確實有不同的大小，而實數所構成的無窮嚴格地大於有理數所構成的無窮。這是你在大學一年級課程中會遇到的最令人震驚的結果之一。

Stern 數列

數列 u_n 稱為 *Stern 雙原子數列*（Stern's diatomic sequence），它還有許多其他面貌。例如，u_{n+1} 等於把 n 寫成 2 的冪之和、而每個冪最多用兩次的方法數目。它與 *Stern–Brocot 樹*以及連分數（continued fractions）關係密切，而連分數能給出無理數的最佳有理逼近。

思維技巧

構造雙射

要證明兩個集合大小相同，就要把它們的元素準確地一一配對：證明目標集合的每個元素都被對應到（滿射），而且沒有元素被對應兩次（單射）。

雙射是計數的基礎，不論有限還是無窮，你在大學裏會經常用到。在本題中，兩半的證明都是把一個結構追溯回它的起點。

延伸練習

1 **找出分數。**對哪一個 n 有 $f(n) = \frac{3}{5}$？又 $f(n) = \frac{5}{3}$ 呢？利用父節點的規則倒推回 $\frac{1}{1}$。

2 **Newman 公式。**驗證由 $x_1 = 1$ 開始，Newman 公式能給出列表中的首十個分數。

3 **康托爾的對角論證法。**假設你有一個列表，以小數形式列出了 0 與 1 之間的所有實數。構造一個小數，使它與列表中第 n 個數在第 n 位數字上不同。為甚麼這就說明列表並不完整？（對於像 $0.0999\ldots = 0.1$ 這樣的小數，需要留意甚麼？）

4 **可數並集。** 較難 給出一個與正整數之間的明確雙射，從而證明由全體正整數數對 (m, n) 組成的集合是可數的。（試試 $2^{m-1}(2n-1)$。）

延伸閱讀

- **Neil Calkin & Herbert Wilf, "Recounting the rationals"**（*American Mathematical Monthly*，2000 年；〈重新數算有理數〉）。全文四頁，完全讀得懂。
- **Aigner & Ziegler, *Proofs from THE BOOK***（《數學天書中的證明》），第 17 章 "Sets, functions, and the continuum hypothesis"（集合、函數與連續統假設），當中包括 Calkin–Wilf 樹。

- **Ian Stewart & David Tall, *The Foundations of Mathematics***（《數學基礎》，Oxford University Press）。可數性、康托爾與實數，內容與大學一年級課程相若。

1.9 三次曲線的切線

題目

STEP I 2009，第 2 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/09-s1-q2`

引子

這題看來只是一道例行的坐標幾何（coordinate geometry）題：求導、找切線、解三次方程。可是最後一行卻要你找出一個立方數，它是另外三個立方數之和，而幾何竟像變魔術一樣把它變了出來。

這個竅門是過曲線上一個已知點作直線，從而找出新的點，它可追溯至公元三世紀亞歷山大港的丟番圖（Diophantus）。到了現代數學家手上，它發展成橢圓曲線（elliptic curves）的理論。這套理論位於當今數論的核心，是費馬最後定理（Fermat's Last Theorem）證明的基礎，也保障着全球一大部分互聯網通訊的安全。

動筆之前

? **想一想** 點 $(-a, b)$ 在曲線上。為甚麼？這跟立方和又有甚麼關係？

代入：$(-a)^3 + a^3 + b^3 = b^3$，所以確實在曲線上。在 $y^3 = x^3 + a^3 + b^3$ 上坐標為有理數（rational）的點正是我們想要的：若 $x = q/s'$ 而 $y = p/s'$，去分母後便得到一條立方數之間的關係式。我們的計劃是從一個容易找到的點出發，利用幾何找出一個沒那麼明顯的點。

逐步解題

階段 1　切線

對 $y^3 = x^3 + a^3 + b^3$ 作隱函數求導（implicit differentiation）：$3y^2\dfrac{dy}{dx} = 3x^2$，所以 $\dfrac{dy}{dx} = \dfrac{x^2}{y^2}$。在 $(-a, b)$ 處斜率（gradient）為 a^2/b^2，所以切線（tangent）是

$$y - b = \frac{a^2}{b^2}(x + a) \quad\Longrightarrow\quad b^2y - b^3 = a^2x + a^3 \quad\Longrightarrow\quad b^2y - a^2x = a^3 + b^3. \qquad \blacksquare$$

階段 2　切線與曲線再次相交之處

取 $a = 1$、$b = 2$，曲線是 $y^3 = x^3 + 9$，而在 $(-1, 2)$ 的切線是 $4y - x = 9$，即 $y = \dfrac{x+9}{4}$。代入曲線方程：

$$\frac{(x+9)^3}{64} = x^3 + 9 \quad\Longrightarrow\quad x^3 + 27x^2 + 243x + 729 = 64x^3 + 576,$$

整理後得 $63x^3 - 27x^2 - 243x - 153 = 0$，再除以 9 便得 $7x^3 - 3x^2 - 27x - 17 = 0$。 $\blacksquare$

階段 3　解三次方程

> **想一想**　不用做任何代數運算，你已經知道這個三次方程的一個根。是哪一個？它為甚麼應該出現兩次？

切線在 $x = -1$ 處與曲線相切（圖 1.9.1），而「相切」意味着重根（repeated root），正如拋物線的切線與拋物線相交於某個二次方程的二重根。所以 $(x+1)^2$ 應該是一個因式。驗算：$7(-1)^3 - 3(1) - 27(-1) - 17 = -7 - 3 + 27 - 17 = 0$，而導數 $21x^2 - 6x - 27$ 在 $x = -1$ 處也等於零。相除後得

$$7x^3 - 3x^2 - 27x - 17 = (x+1)^2(7x - 17).$$

> **停一停，試一試**　所以切線與曲線再次相交於 $x = \frac{17}{7}$ 之處。求出 y，然後把這個點化為一條立方數之間的關係式。

$y = \dfrac{17/7 + 9}{4} = \dfrac{80/7}{4} = \dfrac{20}{7}$。點 $\left(\frac{17}{7}, \frac{20}{7}\right)$ 在 $y^3 = x^3 + 9$ 上，所以

$$\frac{20^3}{7^3} = \frac{17^3}{7^3} + 9 \quad\Longrightarrow\quad 20^3 = 17^3 + 9 \times 7^3.$$

> **想一想**　我們希望 9×7^3 是兩個立方數之和。回想一下那個 9 是怎樣來的。

$9 = a^3 + b^3 = 1^3 + 2^3$，所以 $9 \times 7^3 = 7^3 + 14^3$。因此

$$20^3 = 17^3 + 14^3 + 7^3.$$

驗算：$8000 = 4913 + 2744 + 343$。 ■

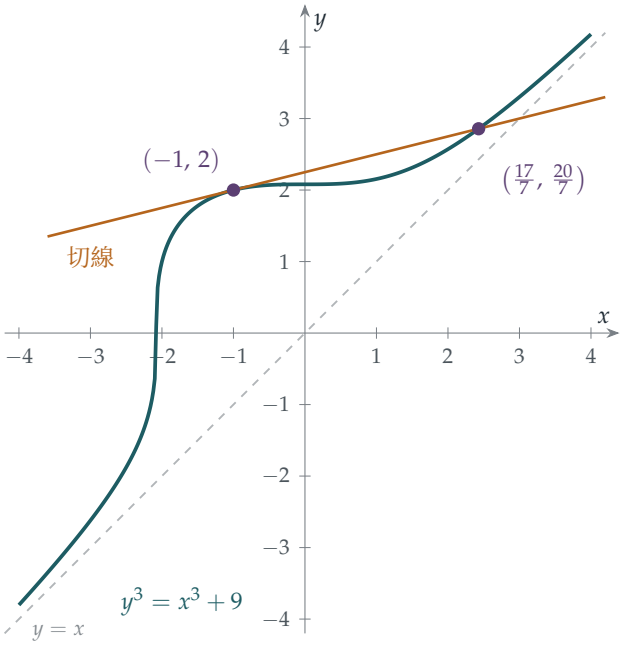


圖 1.9.1　曲線 $y^3 = x^3 + 9$（藍綠色）在遠離原點處趨近直線 $y = x$。在有理點 $(-1, 2)$ 的切線（琥珀色）在該處與曲線相切，這算作二重交點，並在另一個有理點 $\left(\frac{17}{7}, \frac{20}{7}\right)$ 再與曲線相交一次。

回顧

- **相切即二重根。**這令一個沒有明顯根的三次方程，變成可以即時因式分解的方程。
- **新的根自動是有理數。**三個根之中一旦有兩個是有理數（這裏兩個都是 -1），第三個也必定是有理數，因為各根之和 $\frac{3}{7}$ 是有理數。這正是整個方法的精髓。
- **幾何帶來了算術。**我們從沒有刻意搜尋立方數；是一條切線把它們找了出來。

背後的數學

弦切法

取一條三次曲線（cubic curve），例如 $y^3 = x^3 + 9$，或者更標準的形式 $y^2 = x^3 + Ax + B$。假如你知道曲線上兩個坐標為有理數的點，那麼過這兩點的直線恰好與曲線再相交於一點，而該點的坐標也是有理數（理由見回顧中的論證）。假如你只知道一個點，就

改用該點的切線。無論哪種情況，舊的有理點都能產生新的有理點。

值得注意的是，這個「弦切」（chord–tangent）作圖法可以變成一種把曲線上的點相加的方法，於是有理點便構成一個羣（group），這是你在大學一年級會學到的一種代數結構。莫德爾（Louis Mordell）在 1922 年證明了這個羣由有限個點生成：所有有理點，不論有多少個，都可以由一個有限集合出發，利用弦和切線構造出來。他的證明是 Section 1.5 中費馬（Fermat）下降法的一個版本。

今日的橢圓曲線

這類曲線稱為橢圓曲線（並非因為它們是橢圓，而是因為歷史上它們與橢圓的弧長有關）。它們在現代數學中無處不在。

- **費馬最後定理。**在 1980 年代，Gerhard Frey 留意到 $x^n + y^n = z^n$ 的一個解會產生一條非常古怪的橢圓曲線。懷爾斯（Andrew Wiles）在 1994 年證明了這樣古怪的曲線不可能存在，從而證明了費馬最後定理。
- **貝赫與斯維訥通－戴爾猜想（Birch and Swinnerton-Dyer conjecture）。**有理點所構成的羣需要多少個生成元（generators）？在 1960 年代，有人憑藉劍橋一些數學史上最早的電腦實驗提出了一個猜想，它用一個函數來預測答案，而這個函數是由點算曲線在模質數之下的點數構造出來的。它是七條千禧年大獎難題（Millennium Prize Problems）之一。
- **密碼學（cryptography）。**在有限數系上的橢圓曲線上，把一個點 P 自己相加 n 次是很快的，即使 n 有數百位數字也一樣（把 P 反覆加倍，就像你用反覆平方來計算高次冪那樣）。但已知 P 和結果 nP，要找出 n 卻似乎極之困難：這就是橢圓曲線離散對數問題（elliptic-curve discrete logarithm problem）。這種不對稱性保護着今日大部分的網上通訊。

同次冪之和

能寫成三個正立方數之和的最小立方數是 $6^3 = 3^3 + 4^3 + 5^3$；切線法找到的是 $20^3 = 7^3 + 14^3 + 17^3$，它並非前者的倍數，而重複使用這個方法會不斷產生新的恆等式（雖然有些會涉及負數）。要多少個 k 次冪才能湊成另一個 k 次冪？歐拉（Euler）在 1769 年猜想，至少需要 k 個 k 次冪才能湊成另一個 k 次冪。對於四次冪和五次冪，他錯了：1966 年 Leon Lander 和 Thomas Parkin 以電腦搜尋找到

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

而在 1988 年，Noam Elkies 利用橢圓曲線找到了四次冪的反例（counterexamples）。

思維技巧

以幾何解決算術

要找出一個方程的整數解或有理數解，不妨把它看成一條曲線，然後尋找過已知點的直線。

背後的代數很簡單：若一個有理係數多項式（polynomial）除了一個根之外其餘的根都是有理數，那麼最後一個根也是有理數。這樣在圖像與方程之間來回轉換，是數學家所能擁有的最強大的習慣之一。

延伸練習

1 **圓上的有理點。**過 $(-1,0)$ 而斜率為 t 的直線與圓 $x^2+y^2=1$ 再次相交。證明另一個交點是 $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$，並由此得出無窮多組畢氏三元數（Pythagorean triples）。

2 **一條落空的弦。**點 $(1,2)$ 和 $(2,1)$ 在 $x^3+y^3=9$ 上。證明過這兩點的直線與曲線再沒有其他交點。那個「第三點」到哪裏去了？（查一查無窮遠點（point at infinity）。）

3 **故技重施。**求 $y^3=x^3+9$ 在 $\left(\frac{17}{7}, \frac{20}{7}\right)$ 的切線，以及它與曲線相交的第三點。（使用電腦代數系統會有幫助；留意數字增長得有多快。）

4 **的士數（taxicab numbers）。**$1729 = 1^3+12^3 = 9^3+10^3$。求過 $(1,12)$ 和 $(9,10)$ 的直線與曲線 $x^3+y^3=1729$ 相交的第三點，並由此推導出一條形如 $p^3=q^3+r^3+s^3$ 的新恆等式。

延伸閱讀

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves***（Springer）。為大學本科生而寫；第 1 章所需的知識不超出英國高考（A-level）程度。
- **Avner Ash & Robert Gross, *Elliptic Tales***（Princeton University Press）。一本普及讀物，一路講到貝赫與斯維訥通－戴爾猜想。
- **Simon Singh, *Fermat's Last Theorem***。講述橢圓曲線如何解決一個有 350 年歷史的難題。

我們學到了甚麼

在本章開首，我們就整數提出了三個問題，並預告還有第四個主題貫穿其中：怎樣證明（prove）一件事。現在是時候看看，九道 STEP 題目把我們帶到了多遠。

1. 質數有多少個？它們是怎樣分佈的？

在 Section 1.1 中，我們證明了質數（prime）有無窮多個，卻連一個新的質數也沒有找出來。我們構造了一族無窮多個的數，即費馬數（Fermat numbers），它們兩兩之間沒有公因數，所以每一個都需要一個屬於自己的質數。這個證明談的是*結構*，而不是大小。

在 Section 1.2 中，我們更進一步，證明了不超過 n 的所有質數之積小於 4^n。這是我們第一個定量的結論：它限制了質數可以排得多密。取對數後，它說的是 $\sum_{p \le n} \ln p < 1.39\,n$，而質數定理（Prime Number Theorem）指出真實的值大約是 n。我們這個 STEP 程度的論證，已經相當接近了。

我們*沒有*做到的，是確切找出質數怎樣分佈。這由黎曼 ζ 函數（Riemann zeta function）所支配，而把這件事說得精確，就是黎曼猜想（Riemann Hypothesis），也就是數學中最著名的未解決問題。你現在所知的，已足以明白它在說甚麼。

2. 怎樣證明一個數不是分數？

我們找到了三種截然不同的方法。

- **取最小的那一個**（Section 1.3）。假如 $\sqrt{2}$ 是分數，就會有一個最小的正整數 k 使 $k\sqrt{2}$ 為整數；但這樣一來，$(\sqrt{2}-1)k$ 就是一個更小的。同樣的論證也適用於立方根。
- **把一個整數困在 0 與 1 之間**（Section 1.4）。假如 e 或 e^2 是分數，乘以一個階乘（factorial）後，就會得出一個嚴格介乎 0 與 1 之間的整數。埃爾米特（Hermite）和林德曼（Lindemann）證明 e 和 π 是超越數（transcendental），背後正是這個想法。
- **找出一個不可能成立的整除關係**（Section 1.5，習題 3）。證明 $x^2 + y^2 = 3$ 上沒有有理點（rational point），等同於證明當 x 是有理數時，$\sqrt{3 - x^2}$ 永遠不是有理數。

我們也認識到還有多少事情仍然未知：至今沒有人能證明 $e + \pi$ 是無理數（irrational）。

3. 哪些方程有整數解？

有時答案是*沒有*，而 Section 1.5 展示了費馬（Fermat）證明這一點的方法：任何一個解都會產生一個更小的解，如此無休無止。以一個精心挑選的質數為模（modulo）來運算，就能告訴我們該利用哪一個整除關係。

有時答案是*有*，*而且這裏有一部製造解的機器*。在 Section 1.6 中，複數（complex numbers）把二平方和變成了一條乘法法則。在 Section 1.9 中，三次曲線（cubic curve）的一條切線給出了 $20^3 = 17^3 + 14^3 + 7^3$。

還有些時候，正確的一步是*換一個數系*。高斯整數（Gaussian integers）令二平方和變得容易。但 Section 1.7 提出了一個警告：在一個看來完全合理的數系中，數可以用兩種不同的方式分解成「質數」。這個警告在 1847 年被人忽視，結果催生了理想（ideals）和近世代數。

Section 1.8 還另添了一重轉折：分數看似遠比整數多，卻可以逐一列舉出來。無窮比乍看之下有更豐富的結構。

4. 證明的工具箱

以下是你在本章用過的方法。每一種都會在大學數學課程中一再出現。

方法	你在哪裏用過
歸納法（induction）與強歸納法（strong induction）	費馬數（1.1）；質數之積（1.2）
良序性（well-ordering）、最小反例（minimal counterexample）	$\sqrt{2}$ 與 $\sqrt[3]{2}$（1.3）；列舉分數（1.8）
無窮遞降法（infinite descent）	不可能成立的方程（1.5）；互質（coprime）數對（1.8）
反證法（proof by contradiction）	貫穿全章，尤其是 1.3 和 1.4
模 n 運算	1.5；1.7
估界與夾逼（bounding and squeezing）	1.2；1.4
構造雙射（bijection）	1.8
構造反例（counterexample）	非唯一分解（1.7）
轉換場景	複數（1.6）；幾何（1.9）

回頭看看這些題目，你會留意到 STEP 的擬題人往往替你走了第一步：「考慮二項展開式（binomial expansion）…」、「考慮複數 $2 + \mathrm{i}$ 和 $10 + 11\mathrm{i}$…」。到了大學，這種幫助會逐漸消失，而找出正確的第一步就成了真正的本領。最好的準備正是你一直在做的事：每做完一道題，問問自己那個提示*爲甚麼*奏效，下次你就能自己想到。

下一步

本章有好幾條線索會在書中其他地方延續下去。

- 以分數逼近 e 的課題會在 Section 2.9 再次出現，而黎曼 ζ 函數則見於 Section 2.4，那裏有 $\zeta(2) = \pi^2/6$。
- 單位根（roots of unity）曾在拉梅（Lamé）那個失敗的證明中出現，它是 Chapter 5 的主題；而在 Section 1.1 中預告過的高斯（Gauss）正十七邊形作圖法，就是 Section 6.2。
- Section 1.6 中那條恆等式的四平方版本，會透過四元數（quaternions）在 Section 7.8 中出現。

如果你想在上大學前走得更遠

- **Harold Davenport, *The Higher Arithmetic***：初等數論入門書中最好的一本。
- **Aigner & Ziegler, *Proofs from THE BOOK***：第 1–4、8 和 17 章與本章直接相關。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***：幾乎涵蓋本章的全部內容，而且還有更多，節奏平緩。
- **Marcus du Sautoy, *The Music of the Primes*** 和 **Simon Singh, *Fermat's Last Theorem***：數學背後的人物故事。

數論總有辦法把人吸引進去。它的問題簡單得第一天就可以提出，卻又深奧得足以耗上一生。如果其中某些章節令你很想知道接下來會怎樣，那正是本書的用意所在。

延伸練習答案

以下只是簡短的答案和提示，並非完整解答：只列出結果和關鍵步驟，方便你核對自己的做法。請先認真做過每一道練習，然後才看答案。

1.1 質數工廠

1. 假設 $p_1, \dots, p_k$ 就是全部的質數（prime）；那麼 $p_1 \cdots p_k + 1$ 有一個不在此列之中的質因數（prime factor），矛盾（contradiction）。用費馬數（Fermat number）的證明則是構造性（constructive）的：它具體給出無窮多個兩兩互質（pairwise coprime）的數 $F_0, F_1, \dots$，每一個都提供一個新的質數。

2. 當 $n \geq 2$ 時，2^n 是 4 的倍數，所以 $2^{2^n} = 16^{2^{n-2}}$，而 16 的任何次冪的末位數字都是 6。因此 F_n 的末位數字是 7。

3. (a) 用歸納法（induction）：$a_{n+1} - 1 = a_n(a_n - 1) = a_n \cdot a_1 \cdots a_{n-1}$。(b) a_m 與 a_n（$m < n$）的公因數必整除 $a_1 \cdots a_{n-1} = a_n - 1$ 和 a_n，所以只能是 1；每一項都有一個不與其他項共有的質因數。(c) $\frac{1}{a_n} = \frac{1}{a_n - 1} - \frac{1}{a_{n+1} - 1}$；求和時各項裂項相消（telescope），得 $1 - \frac{1}{a_{n+1} - 1}$。

4. (a) 由 $p \mid F_n$ 得 $2^{2^n} \equiv -1$；兩邊平方得 $2^{2^{n+1}} \equiv 1$。(b) 凡滿足 $2^e \equiv 1$ 的 e 都能被 d 整除，所以 $d \mid 2^{n+1}$；又因為 $2^{2^n} \equiv -1 \not\equiv 1$（因 p 是奇數），所以 $d \nmid 2^n$。故 $d = 2^{n+1}$。(c) $2^{p-1} \equiv 1$，所以 $2^{n+1} \mid p - 1$。(d) $641 = 64 \times 10 + 1$。小於 641 而形如 $64k + 1$ 的質數有 193、257、449 和 577：只需試四個候選數，歐拉（Euler）正是這樣找到 641 的。

5. 第 n 個質數不會超過 $F_0, \dots, F_{n-1}$ 之中任何一個數的最大質因數，所以 $p_n \leq F_{n-1} = 2^{2^{n-1}} + 1$。當 $n = 5$ 時，這個上界是 65 537，而 $p_5 = 11$：結論正確，但極為粗疏。

1.2 質數分佈得有多稀疏？

1. $P_{1,10} = 210$，$P_{1,20} = 9\,699\,690$，$P_{1,30} = 6\,469\,693\,230$。與 $4^{30} \approx 1.15 \times 10^{18}$ 和 $e^{30} \approx 1.07 \times 10^{13}$ 比較：這個乘積遠小於 4^n，增長速度大致與 e^n 相若（事實上 $\ln P_{1,n} \sim n$，這是質數定理（Prime Number Theorem）的一種形式）。

2. $\binom{2m}{k+1} / \binom{2m}{k} = \frac{2m-k}{k+1}$，此值大於 1 當且僅當 $k < m$，所以各係數先遞增至中間一項，

然後遞減。$2m+1$ 項之和為 4^m，其中最大的一項至少等於它們的平均值。

3. 區間 $(\sqrt{n}, n]$ 內的質數每個都大於 $\sqrt{n}$，而它們的乘積小於 4^n，所以 $(\sqrt{n})^{\pi(n)-\pi(\sqrt{n})} < 4^n$；兩邊取對數（logarithm）。由於 $2\ln 4 \approx 2.77$ 且 $\pi(\sqrt{n}) \le \sqrt{n}$，即得所求的上界。它具有正確的形式 $n/\ln n$，只是常數為 2.8，而非真正的 1。

4. 取質數 $2, 3, 5, 7, 13, 23, 43, 83$，其中每一個都小於前一個的兩倍。對任意 $n \le 50$，此列中第一個大於 n 的質數小於前一個質數的兩倍，而前一個質數不超過 n，所以它介乎 n 與 $2n$ 之間。

1.3 最小反例

1. 設 k 是使 $k\sqrt{3}$ 為整數的最小正整數，則 $k' = (\sqrt{3}-1)k$ 是一個更小的正整數，而且 $k'\sqrt{3} = 3k - k\sqrt{3}$ 是整數。這裏 $\sqrt{3}-1$ 所起的作用，與 $\sqrt{2}-1$ 相同。

2. 由於 $0 < \sqrt{N} - m < 1$，$k' = (\sqrt{N}-m)k$ 是一個小於 k 的正整數，而 $k'\sqrt{N} = kN - mk\sqrt{N}$ 是整數：矛盾。

3. 當 $N = 4$ 時，$m = 2 = \sqrt{4}$，所以 $\sqrt{N} - m = 0$，而 $k' = 0$ 並非正整數。「$0 < \sqrt{N} - m$」這一步不成立。

4. 在圖中，邊長為 a 的正方形內有兩個邊長為 b 的正方形互相重疊，它們把中央一個邊長為 $2b-a$ 的正方形覆蓋了兩次，並留下兩個邊長為 $a-b$ 的正方形未被覆蓋。用代數表示，就是 $(2b-a)^2 - 2(a-b)^2 = 2b^2 - a^2 = 0$。

1.4 e 是無理數，e^2 也是

1. 若 $\frac{1}{e} = \frac{p}{q}$，把 $\frac{1}{e} = \sum_{k\ge 0} \frac{(-1)^k}{k!}$ 乘以 $q!$。$k \le q$ 的各項都是整數，而尾部 $\sum_{k>q}(-1)^k q!/k!$ 是各項遞減的交錯級數（alternating series），所以其絕對值嚴格介乎 0 與 $\frac{1}{q+1}$ 之間。因此 $q!/e$ 不是整數：矛盾。

2. 若 $\sin 1 = \frac{p}{q}$，取 $2n+1 \ge q$，兩邊乘以 $(2n+1)!$。左邊是整數，級數中直至 $\frac{1}{(2n+1)!}$ 的各項也是整數；尾部是交錯級數，首項的大小為 $\frac{1}{(2n+2)(2n+3)} < 1$，所以它不是整數。

3. 這個方法需要一個各項均為有理數（rational）的級數，而且其尾部縮小的速度要比分母增長的速度快，就像 $\frac{1}{k!}$ 那樣；對於 π，目前並不知道有這樣的級數。Niven 的證明用到 $\int_0^\pi \frac{x^n(\pi-x)^n}{n!}\sin x\,\mathrm{d}x$：假如 π 是有理數，當 n 足夠大時，這個積分就會是一個小於 1 的正整數。

4. $x^2 - (e+\pi)x + e\pi$ 的根是 e 和 π。假如 $e+\pi$ 和 $e\pi$ 都是代數數(algebraic number)，π 就是一個代數係數多項式的根，因而也是代數數，這與林德曼（Lindemann）定理矛盾。

1.5 無窮遞降法

1. $3 \mid a$；設 $a = 3a_1$，得 $9a_1^3 + b^3 = 3c^3$，所以 $3 \mid b$，於是 $3a_1^3 + 9b_1^3 = c^3$，所以 $3 \mid c$，而 (a_1, b_1, c_1) 是一個更小的解：這就是遞降（descent）。至於 $p^4 + 2q^4 = 5r^4$：四次方數模（modulo）5 只能是 0 或 1（它們的末位數字是 0、1、5 或 6），所以 $p^4 + 2q^4 \equiv 0$ 迫使 $5 \mid p$ 且 $5 \mid q$；於是 $5^4 \mid 5r^4$，所以 $5 \mid r$，同樣可以遞降。
2. 平方數模 4 只能是 0 或 1，所以 $x^2 + y^2$ 只能是 0、1 或 2，絕不會是 3。
3. 若有有理點 $(\frac{a}{c}, \frac{b}{c})$，便會得到 $a^2 + b^2 = 3c^2$，其中 $c \neq 0$，而第 (iii) 部分已排除這個可能。
4. 固定 x、y 時，方程是二次方程 $z^2 - 3xyz + (x^2 + y^2) = 0$，其兩根之和為 $3xy$。由 $(1,1,1)$ 出發：得 $(1,1,2)$；把 $(1,2)$ 所對的那個 1 換掉，得 $3 \cdot 1 \cdot 2 - 1 = 5$，即 $(1,2,5)$；然後是 $(1,5,13)$ 和 $(2,5,29)$。

1.6 兩個平方數之和

1. 平方數模 4 只能是 0 或 1，所以兩個平方數之和模 4 絕不會是 3。
2. $65 = 1^2 + 8^2 = 4^2 + 7^2$ 及 $85 = 2^2 + 9^2 = 6^2 + 7^2$。利用 $65 = (2+\mathrm{i})(2-\mathrm{i})(3+2\mathrm{i})(3-2\mathrm{i})$：$(2+\mathrm{i})(3+2\mathrm{i}) = 4 + 7\mathrm{i}$ 及 $(2+\mathrm{i})(3-2\mathrm{i}) = 8 - \mathrm{i}$。同理，對於 85，$(2+\mathrm{i})(4 \pm \mathrm{i})$ 給出 $7 + 6\mathrm{i}$ 和 $9 - 2\mathrm{i}$。
3. $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$。5、13、17 各自都可分解為一個高斯整數（Gaussian integer）與其共軛（conjugate）之積；從每一對中各選一個因數，共得 8 個乘積，它們兩兩互為共軛（給出相同的平方和），所以剩下 4 個。
4. 取模的平方，得 $9 = (a^2 + b^2)(c^2 + d^2)$。由於 3 不是兩個平方數之和，其中一個因數必為 1。

1.7 因數分解失效之時

1. $693 = 9 \times 77 = 21 \times 33$，四個因數全是 S-質數。方法：取四個形如 $4k+3$ 的質數 p, q, r, s；那麼 $(pq)(rs) = (pr)(qs)$ 就給出兩種分解為 S-質數的方式。
2. E-質數就是形如 $2 \pmod 4$ 的數（它們不可能是兩個偶數之積）。$60 = 2 \times 30 = 6 \times 10$。
3. 展開 $(ac - 5bd)^2 + 5(ad + bc)^2$ 即得 $N(zw) = N(z)N(w)$。$a^2 + 5b^2$ 絕不會等於 2 或 3。由於 $N(2) = 4$、$N(3) = 9$ 及 $N(1 \pm \sqrt{-5}) = 6$，若要分解為非單位（non-unit）之積，就需要一個範數（norm）為 2 或 3 的因數。
4. 設 n 是具有兩種不同分解 $p_1 \cdots p_r = q_1 \cdots q_s$ 的最小的數。根據歐幾里得（Euclid）

引理，p_1 整除某個 q_j，所以 $p_1 = q_j$；約去後得到一個更小而又有兩種不同分解的數，矛盾。

1.8 點算有理數

1. $\frac{3}{5}$：逐級追溯其父節點，$(3,5) \leftarrow (3,2) \leftarrow (1,2) \leftarrow (1,1)$，對應的位置為 $1 \to 2 \to 5 \to 10$，所以 $f(10) = \frac{3}{5}$。$\frac{5}{3}$：$(5,3) \leftarrow (2,3) \leftarrow (2,1) \leftarrow (1,1)$，位置為 $1 \to 3 \to 6 \to 13$，所以 $f(13) = \frac{5}{3}$。

2. Newman 的法則 $x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}$ 給出 1、$\frac{1}{2}$、2、$\frac{1}{3}$、$\frac{3}{2}$、$\frac{2}{3}$、3、$\frac{1}{4}$、$\frac{4}{3}$、$\frac{3}{5}$，與 $f(1), \ldots, f(10)$ 吻合。

3. 第 n 位數字一律取 5，除非第 n 個數的第 n 位數字是 5，這時則取 4。新的小數與列表中每一個數都不相同，而且由於避開了 0 和 9，它只有一種小數展開式，所以確實是一個不同的數。

4. 每個正整數都可唯一地寫成 2 的冪乘以一個奇數，即 $2^{m-1}(2n-1)$，所以 $(m,n) \mapsto 2^{m-1}(2n-1)$ 是一個雙射（bijection）。

1.9 三次曲線的切線

1. 把 $y = t(x+1)$ 代入 $x^2 + y^2 = 1$，得 $(1+t^2)x^2 + 2t^2 x + t^2 - 1 = 0$，其根為 -1 和 $\frac{1-t^2}{1+t^2}$。取 $t = \frac{q}{p}$，該點為 $\left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$，由此得到三元數組 $(p^2-q^2, 2pq, p^2+q^2)$。

2. 該直線為 $x + y = 3$，而 $x^3 + (3-x)^3 = 9$ 可化簡為 $9x^2 - 27x + 18 = 0$：三次項互相抵消，只剩下 $x = 1, 2$。這條直線與漸近線（asymptote）$y = -x$ 平行，第三個交點在無窮遠處。

3. 切線(tangent)的斜率(gradient)為 $\frac{x^2}{y^2} = \frac{289}{400}$，它與曲線再相交於 $\left(-\frac{188479}{90391}, -\frac{36520}{90391}\right)$。去分母後，得 $188479^3 = 36520^3 + 90391^3 + 180782^3$。

4. 該直線與 $x^3 + y^3 = 1729$ 再相交於 $\left(-\frac{37}{3}, \frac{46}{3}\right)$，所以 $46^3 = 37^3 + 27 \times 1729 = 37^3 + 3^3 + 36^3$（這裏用到 $27 = 3^3$ 和 $27 \times 1728 = 36^3$）。

Beyond STEP

STEP 是大多數中學生一生中應考過最艱深的數學考試，也是最出色的考試之一：題目簡短、陌生而深刻，當中最精彩的，其實是喬裝了的大學數學小品。

本書精選最有趣的 STEP 試題，由 1987 年首次開考之前的樣本試卷（specimen papers），到 2025 年的試卷，並以每一道題目作為一扇門。每道題目都會仔細解答，沿途提出優秀學生會問的問題，然後帶你穿過這扇門：這個想法從何而來，到了大學會演變成甚麼，以及接下來該讀些甚麼。

本書為正在準備 STEP、有天分又有志投身數學的學生而寫。他們想要的不止是模擬試卷：他們想開始像數學系本科生那樣思考，並一探前方有甚麼正等着自己。

- 共 13 章，涵蓋純數學（pure mathematics）、力學（mechanics）、概率（probability）與統計（statistics）
- 136 道 STEP 歷屆試題，每題均附引導式解答
- 每道題目背後的大學數學
- 附答案的延伸練習，以及延伸閱讀

全書共 13 章，本冊為第 1 章。 全書各章及所有詳細解答均可免費閱讀、下載及分享，網址為

beyondstep.keithmcnulty.org

文字內容已貢獻予公有領域（CC0 1.0）。STEP 試題 © Cambridge University Press & Assessment。