1.7 因數分解失效之時

工作紙

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

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**　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？

階段 1 併集、交集與乘積

涵蓋：第 (i) 及 (ii) 部分

想一想 S 和 T 的元素除以 4 時，餘數（remainder）分別是甚麼？哪些正整數會有這些餘數？

想一想 把 $(4a+1)(4b+1)$ 乘開，並把結果寫成 $4\times(\text{某數})+1$ 的形式。

停一停，試一試 對於 T，試一個簡單的例子，例如 3×3。另外也值得計算 $(4a+3)(4b+3)$ 和 $(4a+1)(4b+3)$，因為後面的部分會用到。

階段 2　屬於 T 的質因數

涵蓋：第 (iii) 部分

想一想　T 中任何一個數的質因數（prime factor）都是奇數，所以每個質因數不是屬於 S，就是屬於 T。

停一停，試一試　假如所有質因數都屬於 S，會怎樣？重複運用第 (ii) 部分的結果。

階段 3 奇數個因數

涵蓋：第 (iv)(a) 部分

想一想 T 的每個元素都至少是 3。用強歸納法（strong induction）證明每個 $n \in T$ 不是 T-質數，就是若干個 T-質數的乘積。

停一停，試一試 為甚麼乘積中 T-質數的個數必定是奇數？想想偶數個 T 的元素相乘後，除以 4 的餘數是甚麼。

階段 4　兩種因數分解

涵蓋：第 (iv)(b) 部分

想一想　15 是 T-質數嗎？它是質數嗎？同樣的情況也會在 S 中出現：S 的哪些元素是兩個屬於 T 的普通質數的乘積？

停一停，試一試　從 T 中取兩個質數，例如 3 和 7。若兩者各有兩個，把它們配對成 S 的元素，共有多少種方法？

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。

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。

完整的引導式解答見第 1.7 節：

https://beyondstep.keithmcnulty.org/zh-hant/ch01/factorisation-fails.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