詳細解答

STEP I 2016，第 7 題

純數學 • 模 4 的因式分解

> **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

本題在 *Beyond STEP* 第 1.7 節因數分解失效之時中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch01/factorisation-fails.html

關鍵思路

一切都源於模（modulo）4 運算。奇數必定 $\equiv 1$ 或 $\equiv 3 \equiv -1 \pmod 4$，因此一組奇數的乘積屬於 S 還是 T，取決於其中來自 T 的因數個數是偶數還是奇數。單憑這一條奇偶性（parity）規則，便可解決第 (ii)、(iii) 及 (iv)(a) 部分。第 (iv)(b) 部分則要求你看出 S-質數不一定是質數，而這就令唯一分解（unique factorisation）失效。

解答

第 (i) 部分

每個正奇數除以 4 的餘數都是 1 或 3，而偶數則不會有這樣的餘數。所以 $S \cup T$ 是所有正奇數組成的集合。任何整數都不會有兩個不同的餘數，所以 $S \cap T$ 是空集（empty set）。

第 (ii) 部分

取 S 中的 $4a+1$ 和 $4b+1$，其中 $a, b \geq 0$ 為整數。那麼

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1,$$

這是一個餘數為 1 的正整數，所以它屬於 S。

至於 T，答案是否。例如 $3 \in T$，但 $3 \times 3 = 9 = 4 \times 2 + 1 \in S$，而 $S \cap T$ 是空集。事實

上這種情況必定發生：

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1 \in S.$$

我們亦需要混合的乘積：

$$(4a+1)(4b+3) = 16ab + 12a + 4b + 3 = 4(4ab + 3a + b) + 3 \in T.$$

簡而言之，把 T 中的數寫成 $\equiv -1 \pmod 4$：一組奇數的乘積 $\equiv (-1)^k \pmod 4$，其中 k 是來自 T 的因數個數。所以若 k 為偶數，乘積屬於 S；若 k 為奇數，乘積屬於 T。

第 (iii) 部分

設 $n \in T$ 為合數（composite），並把 $n = p_1 p_2 \cdots p_r$ 寫成質數的乘積。由於 n 是奇數，每個 p_i 都是奇數，所以由第 (i) 部分，每個 p_i 都屬於 S 或 T。

用反證法（proof by contradiction），假設每個 p_i 都屬於 S。反覆應用第 (ii) 部分，得 $p_1 p_2 \in S$，然後 $(p_1 p_2)p_3 \in S$，如此類推，所以 $n \in S$。但 $n \in T$ 而 $S \cap T = \varnothing$，這是矛盾。因此 n 至少有一個質因數屬於 T。（用奇偶性的說法：要令 $n \equiv -1$，需要奇數個、因而至少一個 $\equiv -1$ 的因數。）

第 (iv)(a) 部分

首先留意 $1 \notin T$，所以 T 中每個元素都至少是 3。

每個 $n \in T$ 要麼是 T-質數，要麼是若干個 T-質數的乘積。我們對 n 使用強歸納法（strong induction）。若 n 是 T-質數，則已完成。否則 $n = t_1 t_2 \cdots t_k$，其中 $k \geq 2$ 且每個 $t_i \in T$。每個 $t_i \geq 3$，所以每個 $t_i \leq n/3 < n$，由歸納假設，每個 t_i 要麼是 T-質數，要麼是若干個 T-質數的乘積。把這些代入 $n = t_1 \cdots t_k$，便把 n 寫成 T-質數的乘積。

? **想一想** 我們得到了一個 T-質數的乘積，但為甚麼它們的個數必定是奇數？

每個 T-質數都屬於 T，所以它 $\equiv -1 \pmod 4$。根據第 (ii) 部分末尾的規則，m 個這樣的數的乘積因此 $\equiv (-1)^m \pmod 4$。若 m 為偶數，乘積便 $\equiv 1$，因而屬於 S 而非 T。由於乘積是 $n \in T$，所以 m 是奇數。因此每個 $n \in T$ 要麼是 T-質數，要麼是奇數個 T-質數的乘積，得證。

留意 T-質數不一定是質數：$15 = 3 \times 5$ 是 T-質數，因為 $5 \notin T$，而分解成大於 1 的數的唯一方法是 3×5。

第 (iv)(b) 部分

與上面關於 15 的觀察相同的想法，在 S 中同樣適用：兩個來自 T 的質數的乘積屬於 S，但在 S 之內無法分解。取

$$9 = 3 \times 3, \qquad 21 = 3 \times 7, \qquad 49 = 7 \times 7.$$

每個都屬於 S。每個都是 S-質數：除了 1 和它本身以外，它的因數只有 3 或 7，而這些屬於 T 而非 S。（對於 21，因數是 $1, 3, 7, 21$。）現在

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

而 $441 = 4 \times 110 + 1 \in S$。這是 441 分解成 S-質數的兩種真正不同的方法：第一種用了 9 和 49，第二種用了兩次 21。所以 441 是一個例子。

> ? **想一想** 你會怎樣找到這個例子？

在普通整數中，$441 = 3^2 \times 7^2$，而質數 3, 7 屬於 T。在 S 之內，我們不能單獨分出一個 3 或 7，所以 T 中的質數必須兩兩配對。有兩個 3 和兩個 7 時，配對方法有兩種：$(3 \cdot 3)(7 \cdot 7)$ 或 $(3 \cdot 7)(3 \cdot 7)$。任何 p^2q^2（其中 $p, q \in T$ 為不同質數）都同樣可行，例如 $9 \times 121 = 33 \times 33$。

驗算

- 試試小的例子：$5 \times 9 = 45 \in S$，$3 \times 7 = 21 \in S$，$5 \times 7 = 35 \in T$。
- 對於 (iii)：$15 = 3 \times 5$ 和 $35 = 5 \times 7$ 都屬於 T，而且各自都有一個屬於 T 的質因數（3、7）。
- 用電腦驗證：對每個小於 3000 的 $n \in T$，每種分解成 T-質數的方法都有奇數個因數。T-質數的開頭是 $3, 7, 11, 15, 19, 23, 31, 35, \ldots$。留意 $27 = 3 \times 3 \times 3$ 不是 T-質數：它有三個因數，是奇數。

常見錯誤

- 沒有測試任何例子便聲稱 T 中兩個元素的乘積屬於 T：$3 \times 3 = 9$ 立即否定了這說法。
- 忘記 X-質數不一定是質數。這正是 (iv)(b) 的重點：9 和 21 都是 S-質數。
- 在 (iv)(a) 中只證明了因數個數是奇數，卻忘記證明分解成 T-質數的方法確實存在。

STEP 之外

集合 S 對乘法封閉，而它的「質數」並不能唯一分解。這是一個經典的玩具模型（有時稱為希爾伯特數（Hilbert numbers），以希爾伯特（Hilbert）命名），說明了在 $\mathbb{Z}[\sqrt{-5}]$ 這類環（ring）中出現的問題：在那裏 $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$。為了在這類環中修補唯一分解，數學家發展出理想（ideals）和代數數論（algebraic number theory）。Davenport 的 *The Higher Arithmetic*（《高等算術》）解釋了為甚麼 $\mathbb{Z}$ 中的唯一分解是一條需要證明的定理，而 Allenby 的 *Rings, Fields and Groups*（《環、域與羣》）則討論了唯一分解失效的環。

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。