详细解答

STEP I 2016，第 7 题

纯数学 • 模 4 的因式分解

> **STEP I 2016，第 7 题**
>
> 继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：
>
> step.maths.org/questions/16-s1-q7

本题在 *Beyond STEP* 第 1.7 节因数分解失效之时中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch01/factorisation-fails.html

关键思路

一切都源于模（modulo）4 运算。奇数必定 $\equiv 1$ 或 $\equiv 3 \equiv -1 \pmod 4$，因此一组奇数的乘积属于 S 还是 T，取决于其中来自 T 的因数个数是偶数还是奇数。单凭这一条奇偶性（parity）规则，便可解决第 (ii)、(iii) 及 (iv)(a) 部分。第 (iv)(b) 部分则要求你看出 S-质数不一定是质数，而这就令唯一分解（unique factorisation）失效。

解答

第 (i) 部分

每个正奇数除以 4 的余数都是 1 或 3，而偶数则不会有这样的余数。所以 $S \cup T$ 是所有正奇数组成的集合。任何整数都不会有两个不同的余数，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 $a, b \geq 0$ 为整数。那么

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

这是一个余数为 1 的正整数，所以它属于 S。

至于 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。事实

上这种情况必定发生：

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

我们亦需要混合的乘积：

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

简而言之，把 T 中的数写成 $\equiv -1 \pmod 4$：一组奇数的乘积 $\equiv (-1)^k \pmod 4$，其中 k 是来自 T 的因数个数。所以若 k 为偶数，乘积属于 S；若 k 为奇数，乘积属于 T。

第 (iii) 部分

设 $n \in T$ 为合数（composite），并把 $n = p_1 p_2 \cdots p_r$ 写成质数的乘积。由于 n 是奇数，每个 p_i 都是奇数，所以由第 (i) 部分，每个 p_i 都属于 S 或 T。

用反证法（proof by contradiction），假设每个 p_i 都属于 S。反复应用第 (ii) 部分，得 $p_1 p_2 \in S$，然后 $(p_1 p_2)p_3 \in S$，如此类推，所以 $n \in S$。但 $n \in T$ 而 $S \cap T = \varnothing$，这是矛盾。因此 n 至少有一个质因数属于 T。（用奇偶性的说法：要令 $n \equiv -1$，需要奇数个、因而至少一个 $\equiv -1$ 的因数。）

第 (iv)(a) 部分

首先留意 $1 \notin T$，所以 T 中每个元素都至少是 3。

*每个 $n \in T$ 要么是 T-质数，要么是若干个 T-质数的乘积。*我们对 n 使用强归纳法（strong induction）。若 n 是 T-质数，则已完成。否则 $n = t_1 t_2 \cdots t_k$，其中 $k \geq 2$ 且每个 $t_i \in T$。每个 $t_i \geq 3$，所以每个 $t_i \leq n/3 < n$，由归纳假设，每个 t_i 要么是 T-质数，要么是若干个 T-质数的乘积。把这些代入 $n = t_1 \cdots t_k$，便把 n 写成 T-质数的乘积。

> ? **想一想** 我们得到了一个 T-质数的乘积，但为甚么它们的个数必定是奇数？

每个 T-质数都属于 T，所以它 $\equiv -1 \pmod 4$。根据第 (ii) 部分末尾的规则，m 个这样的数的乘积因此 $\equiv (-1)^m \pmod 4$。若 m 为偶数，乘积便 $\equiv 1$，因而属于 S 而非 T。由于乘积是 $n \in T$，所以 m 是奇数。因此每个 $n \in T$ 要么是 T-质数，要么是奇数个 T-质数的乘积，得证。

留意 T-质数不一定是质数：$15 = 3 \times 5$ 是 T-质数，因为 $5 \notin T$，而分解成大于 1 的数的唯一方法是 3×5。

第 (iv)(b) 部分

与上面关于 15 的观察相同的想法，在 S 中同样适用：两个来自 T 的质数的乘积属于 S，但在 S 之内无法分解。取

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

每个都属于 S。每个都是 S-质数：除了 1 和它本身以外，它的因数只有 3 或 7，而这些属于 T 而非 S。（对于 21，因数是 $1, 3, 7, 21$。）现在

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

而 $441 = 4 \times 110 + 1 \in S$。这是 441 分解成 S-质数的两种真正不同的方法：第一种用了 9 和 49，第二种用了两次 21。所以 441 是一个例子。

? **想一想** 你会怎样找到这个例子?

在普通整数中，$441 = 3^2 \times 7^2$，而质数 3, 7 属于 T。在 S 之内，我们不能单独分出一个 3 或 7，所以 T 中的质数必须两两配对。有两个 3 和两个 7 时，配对方法有两种：$(3 \cdot 3)(7 \cdot 7)$ 或 $(3 \cdot 7)(3 \cdot 7)$。任何 p^2q^2（其中 $p, q \in T$ 为不同质数）都同样可行，例如 $9 \times 121 = 33 \times 33$。

验算

- 试试小的例子：$5 \times 9 = 45 \in S$，$3 \times 7 = 21 \in S$，$5 \times 7 = 35 \in T$。
- 对于 (iii)：$15 = 3 \times 5$ 和 $35 = 5 \times 7$ 都属于 T，而且各自都有一个属于 T 的质因数（3、7）。
- 用电脑验证：对每个小于 3000 的 $n \in T$，每种分解成 T-质数的方法都有奇数个因数。T-质数的开头是 $3, 7, 11, 15, 19, 23, 31, 35, \ldots$。留意 $27 = 3 \times 3 \times 3$ 不是 T-质数：它有三个因数，是奇数。

常见错误

- 没有测试任何例子便声称 T 中两个元素的乘积属于 T：$3 \times 3 = 9$ 立即否定了这说法。
- 忘记 X-质数不一定是质数。这正是 (iv)(b) 的重点：9 和 21 都是 S-质数。
- 在 (iv)(a) 中只证明了因数个数是奇数，却忘记证明分解成 T-质数的方法确实存在。

STEP 之外

集合 S 对乘法封闭，而它的“质数”并不能唯一分解。这是一个经典的玩具模型（有时称为希尔伯特数（Hilbert numbers），以希尔伯特（Hilbert）命名），说明了在 $\mathbb{Z}[\sqrt{-5}]$ 这类环（ring）中出现的问题：在那里 $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$。为了在这类环中修补唯一分解，数学家发展出理想（ideals）和代数数论（algebraic number theory）。Davenport 的 *The Higher Arithmetic*（《高等算术》）解释了为甚么 $\mathbb{Z}$ 中的唯一分解是一条需要证明的定理，而 Allenby 的 *Rings, Fields and Groups*（《环、域与群》）则讨论了唯一分解失效的环。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。