1.7 因数分解失效之时

工作纸

题目

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

提示

请先自行尝试解题。如果遇到困难，请逐一阅读提示，每读完一个便回到题目再试。标有“停一停”或“试一试”的提示是关键步骤。每个提示之后均留有空位供你演算。

> **想一想**　列出 S 和 T 的首几个元素。按照第 (iv) 部分的定义，S 的哪些元素是 S-质数？

阶段 1 并集、交集与乘积

涵盖：第 (i) 及 (ii) 部分

想一想 S 和 T 的元素除以 4 时，余数（remainder）分别是甚么？哪些正整数会有这些余数？

想一想 把 $(4a+1)(4b+1)$ 乘开，并把结果写成 $4\times(\text{某数})+1$ 的形式。

停一停，试一试 对于 T，试一个简单的例子，例如 3×3。另外也值得计算 $(4a+3)(4b+3)$ 和 $(4a+1)(4b+3)$，因为后面的部分会用到。

阶段 2　属于 T 的质因数

涵盖：第 (iii) 部分

想一想　T 中任何一个数的质因数（prime factor）都是奇数，所以每个质因数不是属于 S，就是属于 T。

停一停，试一试　假如所有质因数都属于 S，会怎样？重复运用第 (ii) 部分的结果。

阶段 3 奇数个因数

涵盖：第 (iv)(a) 部分

想一想 T 的每个元素都至少是 3。用强归纳法（strong induction）证明每个 $n \in T$ 不是 T-质数，就是若干个 T-质数的乘积。

停一停，试一试 为甚么乘积中 T-质数的个数必定是奇数？想想偶数个 T 的元素相乘后，除以 4 的余数是甚么。

阶段 4　两种因数分解

涵盖：第 (iv)(b) 部分

想一想　15 是 T-质数吗？它是质数吗？同样的情况也会在 S 中出现：S 的哪些元素是两个属于 T 的普通质数的乘积？

停一停，试一试　从 T 中取两个质数，例如 3 和 7。若两者各有两个，把它们配对成 S 的元素，共有多少种方法？

背后的数学

整数有何特别之处

为甚么分解在普通整数中确实行得通？关键在于欧几里得引理（Euclid's lemma）：如果质数 p 整除乘积 ab，那么 p 整除 a 或 p 整除 b。这条引理是用辗转相除法（Euclidean algorithm）证明的，而它正正是在 S 中失效的地方。在那里，S-质数 9 整除 $21 \times 21 = 441$（因为 $441 = 9 \times 49$），但 9 在 S 中并不整除 21。到了大学一年级，你会严谨地证明欧几里得引理，并看到唯一分解如何由它推导出来。

费马最后定理的失败证明

1847 年 3 月 1 日，拉梅（Gabriel Lamé）向巴黎科学院宣布，他已证明了费马最后定理。他的想法是利用复数单位根（roots of unity）把 $x^n + y^n$ 分解，

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

（其中 n 为奇数），然后就每个括号的质因数进行论证。刘维尔（Joseph Liouville）随即提出质疑：由 ζ 构成的数，凭甚么一定有唯一分解？数星期后，人们才知道库默尔（Ernst Kummer）早已证明这类数往往没有唯一分解。最先失效的情况是 $n = 23$。

库默尔尽力补救，发明了“理想数”（ideal numbers），这些额外的对象能够恢复唯一分解，他并借此对一大类指数证明了费马最后定理。戴德金（Richard Dedekind）把库默尔的理想数发展成*理想*（ideal），成为近世代数的核心概念之一。

一个值得记住的较小例子

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

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

而这四个因数在该数系中全都是“质数”（练习 3）。试把这个例子与 Section 1.6 的高斯整数（Gaussian integers）比较，后者的分解*确实*是唯一的。这类数系之中哪些具有唯一分解，是一个很深刻的问题。高斯（Gauss）猜想，在形如 $\mathbb{Z}[\sqrt{-d}]$ 的数系及与其相近的数系之中，只有九个具有唯一分解。这个猜想最终由黑格纳（Heegner）、贝克（Baker）和斯塔克（Stark）在 1952 年至 1967 年间证明。

延伸练习

---

1 **另一个例子。** 证明 693 有两种不同的 S-质数分解。你能找出一个制造这类例子的通用方法吗？

2 **偶数。** 设 $E = \{2, 4, 6, 8, \ldots\}$。哪些数是 E-质数？证明 60 有多于一种 E-质数分解。

3 **$\mathbb{Z}[\sqrt{-5}]$。** 定义*范数*（norm）$N(a + b\sqrt{-5}) = a^2 + 5b^2$。证明 $N(zw) = N(z)N(w)$。先证明没有任何元素的范数是 2 或 3，由此推导出 2、3 和 $1 \pm \sqrt{-5}$ 在 $\mathbb{Z}[\sqrt{-5}]$ 中不能再分解。

4 **欧几里得引理的应用。** 较难 假设欧几里得引理成立（如果一个质数整除 ab，它就整除 a 或 b），证明每个大于 1 的整数都只有一种质数分解，因数的次序不计。

延伸阅读

- **Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem***（CRC Press）。开首几章讲述拉梅、库默尔与理想的故事，程度适合好学的大学一年级学生。
- **John Stillwell, *Elements of Number Theory***。把整数的唯一分解与高斯整数的唯一分解并列比较。
- **Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction***（Springer）。适合有志挑战的读者：循历史发展解说库默尔的工作。

完整的引导式解答见第 1.7 节：

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

每星期一道 STEP 题目，完整讲解：The STEP Up，以电子邮件免费发送，订阅网址：keithmcnulty.substack.com