詳細解答

STEP III 1987，第 1 題

純數學 • 階乘的整除性

> **STEP III 1987，第 1 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/87-s3-q1

關鍵思路

階乘（factorial）$(n-1)! = 1 \times 2 \times \cdots \times (n-1)$ 包含了每一個小於 n 的正整數。如果 n 可以寫成兩個小於 n 的不同數的乘積，這兩個數都會在階乘中出現，於是 n 整除這個階乘。所以問題的核心其實是：哪些 n 不能這樣拆開？質數（prime）顯然不能，而質數的平方則要仔細看看。親手試算最初十來個數值，答案便呼之欲出。

解答

先做實驗

值得先列一個簡單的表：

n	1	2	3	4	5	6	7	8
$(n-1)!$	1	1	2	6	24	120	720	5040
$n \mid (n-1)!$?	是	否	否	否	否	是	否	是

不成立的情況是 $2, 3, 4, 5, 7$：即目前為止的質數，再加上 4。我們現在證明這個規律會一直延續下去。

斷言。 n 不整除 $(n-1)!$，當且僅當 n 是質數或 $n = 4$。

$n = 1$

這時 $(n-1)! = 0! = 1$，而 1 整除 1。所以 $n = 1$ 不屬於這個集合。

$n = p$ 為質數

$(p-1)!$ 的每個因子 $1, 2, \ldots, p-1$ 都是小於 p 的正數，所以沒有一個能被 p 整除。由於 p 是質數，假如 p 整除這個乘積，它就必須整除其中一個因子（歐幾里得引理，Euclid's lemma）。因此 $p \nmid (p-1)!$，即每個質數都屬於這個集合。

n 為合成數

設 p 為 n 的最小質因數，並寫成 $n = pm$。因為 n 是合成數（composite），所以 $m > 1$，而且 m 的每個質因數都不小於 p，故 $m \geq p$。以下分兩種情況。

情況 1： $m > p$。 這時 $1 < p < m < n$，所以 p 和 m 是數列 $1, 2, \ldots, n-1$ 中兩個不同的數。因此它們的乘積 $pm = n$ 整除 $(n-1)!$。

情況 2： $m = p$，**即** $n = p^2$。

> **想一想** 為甚麼情況 1 的論證在這裏行不通？可以用甚麼來代替？

因子 p 在數列 $1, \ldots, n-1$ 中只出現一次，所以不能把它用兩次。我們改用 p 和 $2p$。若 $p \geq 3$，則

$$2p < p \cdot p = n,$$

所以 p 和 $2p$ 是數列 $1, 2, \ldots, n-1$ 中兩個不同的數。因此它們的乘積 $2p^2 = 2n$ 整除 $(n-1)!$，於是 n 也整除它。

若 $p = 2$，這個論證便失效，因為 $2p = 4 = n$ 不在數列之中。事實上，$n = 4$ 時得 $3! = 6$，而 $4 \nmid 6$。所以 4 屬於這個集合。

結論

除 4 以外，每個合成數 n 都整除 $(n-1)!$，而 $n = 1$ 亦然。因此所求的集合是

$$\{ n : n \text{ 是質數} \} \cup \{4\} = \{2, 3, 4, 5, 7, 11, 13, 17, \ldots\}.$$

驗算

上面的表在 $n \leq 8$ 時與斷言吻合。再試一個質數的平方：$n = 9$ 時得 $8! = 40320 = 9 \times 4480$，正如情況 2 所預測（用的是因子 3 和 6）。用電腦對每個 $n \leq 2000$ 直接計算 $(n-1)! \bmod n$，結果找不到任何違反斷言的例外。

常見錯誤

- 論證「寫成 $n = ab$，其中 $a, b < n$，所以 $ab \mid (n-1)!$」時，沒有堅持要求 $a \neq b$。這個論證會錯誤地「證明」$4 \mid 3!$。
- 忘記了 $n = 1$。由於 $0! = 1$，它不屬於這個集合。
- 說質數 p 不整除 $(p-1)!$ 是「因為 p 不是其中一個因子」。真正的原因是 p 是質數，而且不整除任何一個因子；合成數即使不是乘積中的因子，也可以整除該乘積。

STEP 之外

對於質數，有一個更精確的結果，稱為威爾遜定理（Wilson's theorem）：$(p-1)! \equiv -1 \pmod{p}$。它與本題合起來，便得出一個（非常慢的）質性測試（primality test）：$n > 1$ 是質數，當且僅當 $(n-1)! \equiv -1 \pmod{n}$。威爾遜定理的證明方法，是把每個數與它模 p 的逆元（inverse）配對，這讓人初嘗整數模 p 的羣（group）結構。Davenport 的 *The Higher Arithmetic* 對此有十分精彩的論述。

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。