详细解答

# STEP III 1987，第 1 题

纯数学 · 阶乘的整除性

> **STEP III 1987，第 1 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/87-s3-q1

## 关键思路

阶乘（factorial）$(n-1)! = 1 \times 2 \times \cdots \times (n-1)$ 包含了每一个小于 $n$ 的正整数。如果 $n$ 可以写成两个小于 $n$ 的不同数的乘积，这两个数都会在阶乘中出现，于是 $n$ 整除这个阶乘。所以问题的核心其实是：哪些 $n$ 不能这样拆开？质数（prime）显然不能，而质数的平方则要仔细看看。亲手试算最初十来个数值，答案便呼之欲出。

## 解答

### 先做实验

值得先列一个简单的表：

| $n$ | 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 |

不成立的情况是 $2, 3, 4, 5, 7$：即目前为止的质数，再加上 4。我们现在证明这个规律会一直延续下去。

**断言。** $n$ 不整除 $(n-1)!$，当且仅当 $n$ 是质数或 $n = 4$。

$n = 1$

这时 $(n-1)! = 0! = 1$，而 1 整除 1。所以 $n = 1$ 不属于这个集合。

### $n = p$ 为质数

$(p-1)!$ 的每个因子 $1, 2, \ldots, p-1$ 都是小于 $p$ 的正数，所以没有一个能被 $p$ 整除。由于 $p$ 是质数，假如 $p$ 整除这个乘积，它就必须整除其中一个因子（欧几里得引理，Euclid's lemma）。因此 $p \nmid (p-1)!$，即每个质数都属于这个集合。

### $n$ 为合成数

设 $p$ 为 $n$ 的最小质因数，并写成 $n = pm$。因为 $n$ 是合成数（composite），所以 $m > 1$，而且 $m$ 的每个质因数都不小于 $p$，故 $m \geq p$。以下分两种情况。

**情况 1：** $m > p$。 这时 $1 < p < m < n$，所以 $p$ 和 $m$ 是数列 $1, 2, \ldots, n-1$ 中两个不同的数。因此它们的乘积 $pm = n$ 整除 $(n-1)!$。

**情况 2：** $m = p$，**即** $n = p^2$。

> **想一想** 为甚么情况 1 的论证在这里行不通？可以用甚么来代替？

因子 $p$ 在数列 $1, \ldots, n-1$ 中只出现一次，所以不能把它用两次。我们改用 $p$ 和 $2p$。若 $p \geq 3$，则

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

所以 $p$ 和 $2p$ 是数列 $1, 2, \ldots, n-1$ 中两个不同的数。因此它们的乘积 $2p^2 = 2n$ 整除 $(n-1)!$，于是 $n$ 也整除它。

若 $p = 2$，这个论证便失效，因为 $2p = 4 = n$ 不在数列之中。事实上，$n = 4$ 时得 $3! = 6$，而 $4 \nmid 6$。所以 4 属于这个集合。

### 结论

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

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

## 验算

上面的表在 $n \leq 8$ 时与断言吻合。再试一个质数的平方：$n = 9$ 时得 $8! = 40320 = 9 \times 4480$，正如情况 2 所预测（用的是因子 3 和 6）。用电脑对每个 $n \leq 2000$ 直接计算 $(n-1)! \bmod n$，结果找不到任何违反断言的例外。

## 常见错误

- 论证“写成 $n = ab$，其中 $a, b < n$，所以 $ab \mid (n-1)!$”时，没有坚持要求 $a \neq b$。这个论证会错误地“证明” $4 \mid 3!$。
- 忘记了 $n = 1$。由于 $0! = 1$，它不属于这个集合。
- 说质数 $p$ 不整除 $(p-1)!$ 是“因为 $p$ 不是其中一个因子”。真正的原因是 $p$ 是质数，而且不整除任何一个因子；合成数即使不是乘积中的因子，也可以整除该乘积。

## STEP 之外

对于质数，有一个更精确的结果，称为威尔逊定理（Wilson's theorem）：$(p-1)! \equiv -1 \pmod{p}$。它与本题合起来，便得出一个（非常慢的）质性测试（primality test）：$n > 1$ 是质数，当且仅当 $(n-1)! \equiv -1 \pmod{n}$。威尔逊定理的证明方法，是把每个数与它模 $p$ 的逆元（inverse）配对，这让人初尝整数模 $p$ 的群（group）结构。Davenport 的 *The Higher Arithmetic* 对此有十分精彩的论述。

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。