详细解答

# STEP II 样本试卷，第 8 题

纯数学 · 模群中元素的阶

> **STEP II 样本试卷，第 8 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/spec-s2-q8

## 关键思路

模（modulo）$N$ 之下，$N-1$ 这个数就是 $-1$，而 $m+n=N$ 表示 $n\equiv -m$。所以 $n$ 的每个幂都是 $m$ 的幂，最多相差一个正负号：$n^k\equiv(-1)^k m^k$。$k$ 是偶数还是奇数，决定了这个正负号是否有影响，而题目的三个部分正好对应两个阶（order）的奇偶性的三种组合方式。最后一部分则利用这些事实求出各元素的阶，而无须逐一计算每个幂。

## 解答

全文中，$\equiv$ 表示模 $N$ 同余（congruent）。我们按题目的原意，取 $G$ 的单位元（identity）为 1。（事实上，只要 $N-1\in G$，这一点就必然成立：若 $e$ 是单位元，则 $e(N-1)\equiv N-1$，即 $-e\equiv -1$，所以 $e=1$。）

### $N-1$ 的阶

我们有

$$(N-1)^2=N^2-2N+1\equiv 1,$$

而且由于 $N\geq 3$，故 $N-1\neq 1$。所以 $(N-1)^1$ 不是单位元，但 $(N-1)^2$ 是：$N-1$ 的阶为 2。

### 各部分的准备工作

由于 $m+n=N$，我们有 $n\equiv -m$，因此对每个正整数 $k$ 都有

$$n^k\equiv(-1)^k m^k,\qquad \text{等价地}\qquad m^k\equiv(-1)^k n^k.$$

此外，$N-1 \equiv -1 \equiv n\,m^{-1}$ 属于 $G$，因为 $G$ 是一个包含 $n$ 和 $m^{-1}$ 的群（group）。所以 $-1$ 是 $G$ 的元素，而且由于 $N \geq 3$，故 $-1 \neq 1$。我们还会用到以下的标准结果：若 $x$ 的阶为 $r$ 且 $x^k = 1$，则 $r \mid k$（写成 $k = ar + b$，其中 $0 \leq b < r$；于是 $x^b = 1$，由 $r$ 的最小性得 $b = 0$）。

### 第 (i) 部分

设 $p$ 和 $q$ 都是偶数。那么

$$n^p \equiv (-1)^p m^p = m^p \equiv 1,$$

所以 $q \mid p$。同理，$m^q \equiv (-1)^q n^q = n^q \equiv 1$，所以 $p \mid q$。两个正整数互相整除，必定相等，所以 $p = q$。

### 第 (ii) 部分

设 $p$ 是偶数而 $q$ 是奇数。由于 $p$ 是偶数，$n^p \equiv m^p \equiv 1$，所以 $q \mid p$。另外 $2q$ 是偶数，所以

$$m^{2q} \equiv n^{2q} = (n^q)^2 \equiv 1,$$

由此得 $p \mid 2q$。写成 $p = kq$；于是 $kq \mid 2q$，所以 $k \mid 2$，即 $k = 1$ 或 2。但若 $k = 1$，则 $p = q$ 是奇数，与假设不符。因此 $k = 2$，即 $p = 2q$。

> ? **想一想** 为甚么不能直接由 $m^q \equiv -n^q \equiv -1$ 推断“$p$ 必定是 $2q$”?

这个计算是正确的，它说明 $m^q \neq 1$ 而 $m^{2q} \equiv 1$，但单凭这一点只能得出 $p \mid 2q$ 和 $p \nmid q$，并不足以确定 $p$ 的值（例如原则上 $p$ 可以是 2 而 $q = 3$）。要补上这个缺口，还需要另一个整除关系 $q \mid p$，而它正是来自 $p$ 是偶数这个条件。

### 第 (iii) 部分

用反证法（proof by contradiction）：假设 $p$ 和 $q$ 都是奇数，并设 $r = pq$，它也是奇数。那么

$$n^r = (n^q)^p \equiv 1, \qquad \text{但同时} \qquad n^r \equiv (-1)^r m^r = -(m^p)^q \equiv -1.$$

所以 $1 \equiv -1$，即 $N \mid 2$，但 $N \geq 3$，这不可能。因此 $p$ 和 $q$ 不可能同时是奇数。

（根据对称性，第 (ii) 部分也说明：当 $q$ 是偶数而 $p$ 是奇数时，$q = 2p$。所以在任何情况下，$m$ 和 $N - m$ 的阶要么相等且为偶数，要么其中一个是另一个的两倍，而后者是奇数。）

### 模 21 的群

2 和 5 的各次幂模 21 化简后，依次为

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $2^k$ | 2 | 4 | 8 | 16 | 11 | 1 |
| $5^k$ | 5 | 4 | 20 | 16 | 17 | 1 |

（例如 $2^5 = 32 \equiv 11$，$5^2 = 25 \equiv 4$，$5^4 \equiv 4^2 = 16$，$5^5 \equiv 80 \equiv 17$）。两行中的 1 都是在 $k = 6$ 时首次出现，所以 2 和 5 的阶都是 6。

现在从表中读出各元素的阶：若 $x$ 的阶为 6，则 $x^k$ 的阶为 $6/\gcd(k,6)$。所以

- $11 = 2^5$ 和 $17 = 5^5$ 的阶为 6；
- $4 = 2^2$ 和 $16 = 2^4$ 的阶为 3；
- $8 = 2^3$ 和 $20 = 5^3$ 的阶为 2（由于 $20 = N - 1$，题目的第一部分已经告诉我们这一点）；
- 1 的阶为 1。

余下的是 10、13 和 19，它们各自与一个已知的元素相加得 21：

- $13 = 21 - 8$，而 8 的阶是偶数 2。根据 (iii) 及其后的备注，13 的阶要么是 2（相等且为偶数），要么是 1（即 2 的一半）。它不是 1，因为 $13 \neq 1$，所以 13 的阶为 2。（验算：$13^2 = 169 = 8 \cdot 21 + 1$。）
- $19 = 21 - 2$ 及 $10 = 21 - 11$，而 2 和 11 的阶都是 6。所以 19 和 10 各自的阶是 6 或 3。

所以 $G$ 的每个元素的阶都不超过 6。阶为 12 的循环群（cyclic group）有一个生成元（generator），即一个阶为 12 的元素，而同构（isomorphism）保持元素的阶不变。由于 $G$ 没有阶为 12 的元素，它与阶为 12 的循环群并不同构。

还有另一种方法完成这一步：$G$ 有三个阶为 2 的元素，即 8、13 和 20，而阶为 12 的循环群恰好只有一个（若 $g$ 是它的生成元，则 $g^k$ 的阶为 2 仅当 $k = 6$）。

## 验算

用电脑验算，可得 $G$ 中各元素的阶的完整列表：1 的阶为 1；$8, 13, 20$ 的阶为 2；$4, 16$ 的阶为 3；而 $2, 5, 10, 11, 17, 19$ 的阶为 6。（直接计算，$10^3 = 1000 \equiv 13$ 及 $19^3 \equiv (-2)^3 = -8 \equiv 13$，所以两者的阶都不是 3。）各类元素的数目 $1 + 3 + 2 + 6 = 12$ 与 $G$ 的大小吻合。我们亦对所有 $N < 60$，在单位群中由最多两个元素生成的每个子群（subgroup）里，就每一对 $m$、$N - m$ 检验了第 (i) 至 (iii) 部分：共近 1900 对，无一例外。

## 常见错误

- 假设 $N-1 \in G$ 而不说明原因。题目并没有给出这一点，但它可由 $m, n \in G$ 推出，因为 $N-1 \equiv n\,m^{-1}$。
- 在 (ii) 中只证明了 $p \mid 2q$；还需要多一个整除关系才能得到等式。
- 在古怪的情况下把单位元视为理所当然：例如模 6 之下的子集 $\{3\}$ 对乘法封闭，其单位元为 3，而取 $m = n = 3$ 时便会违反 (iii)。本题的论证依赖单位元是 1，而这显然正是题目的原意。

## STEP 之外

$G$ 是模 21 的单位群（group of units），根据中国剩余定理（Chinese remainder theorem），它同构于模 3 和模 7 的单位群的直积，即 $C_2 \times C_6$：这就是为甚么它有三个阶为 2 的元素，却没有阶为 12 的元素。判断模 $N$ 的单位在甚么时候构成循环群（恰好是 $N = 2, 4, p^k, 2p^k$ 的情况，其中 $p$ 是奇质数，亦即存在“原根”（primitive root）的情况），是大学一年级数论的经典结果。Davenport 的 *The Higher Arithmetic* 讲述了原根，而 Allenby 的 *Rings, Fields and Groups* 则讨论了相关的群论。

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。