詳細解答

STEP II 樣本試卷，第 8 題

純數學 • 模群中元素的階

> **STEP II 樣本試卷，第 8 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/spec-s2-q8

關鍵思路

模（modulo）N 之下，$N-1$ 這個數就是 -1，而 $m+n=N$ 表示 $n\equiv -m$。所以 n 的每個冪都是 m 的冪，最多相差一個正負號：$n^k\equiv(-1)^k m^k$。k 是偶數還是奇數，決定了這個正負號是否有影響，而題目的三個部分正好對應兩個階（order）的奇偶性的三種組合方式。最後一部分則利用這些事實求出各元素的階，而無須逐一計算每個冪。

解答

全文中，$\equiv$ 表示模 N 同餘（congruent）。我們按題目的原意，取 G 的單位元（identity）為 1。（事實上，只要 $N-1\in G$，這一點就必然成立：若 e 是單位元，則 $e(N-1)\equiv N-1$，即 $-e\equiv -1$，所以 $e=1$。）

$N-1$ 的階

我們有

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

而且由於 $N\geq 3$，故 $N-1\neq 1$。所以 $(N-1)^1$ 不是單位元，但 $(N-1)^2$ 是：$N-1$ 的階為 2。

各部分的準備工作

由於 $m+n=N$，我們有 $n\equiv -m$，因此對每個正整數 k 都有

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

此外，$N-1 \equiv -1 \equiv n\,m^{-1}$ 屬於 G，因為 G 是一個包含 n 和 m^{-1} 的羣（group）。所以 -1 是 G 的元素，而且由於 $N \geq 3$，故 $-1 \neq 1$。我們還會用到以下的標準結果：若 x 的階為 r 且 $x^k = 1$，則 $r \mid k$（寫成 $k = ar + b$，其中 $0 \leq b < r$；於是 $x^b = 1$，由 r 的最小性得 $b = 0$）。

第 (i) 部分

設 p 和 q 都是偶數。那麼

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

所以 $q \mid p$。同理，$m^q \equiv (-1)^q n^q = n^q \equiv 1$，所以 $p \mid q$。兩個正整數互相整除，必定相等，所以 $p = q$。

第 (ii) 部分

設 p 是偶數而 q 是奇數。由於 p 是偶數，$n^p \equiv m^p \equiv 1$，所以 $q \mid p$。另外 $2q$ 是偶數，所以

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

由此得 $p \mid 2q$。寫成 $p = kq$；於是 $kq \mid 2q$，所以 $k \mid 2$，即 $k = 1$ 或 2。但若 $k = 1$，則 $p = q$ 是奇數，與假設不符。因此 $k = 2$，即 $p = 2q$。

> ? **想一想** 為甚麼不能直接由 $m^q \equiv -n^q \equiv -1$ 推斷「p 必定是 $2q$」？

這個計算是正確的，它說明 $m^q \not\equiv 1$ 而 $m^{2q} \equiv 1$，但單憑這一點只能得出 $p \mid 2q$ 和 $p \nmid q$，並不足以確定 p 的值（例如原則上 p 可以是 2 而 $q = 3$）。要補上這個缺口，還需要另一個整除關係 $q \mid p$，而它正是來自 p 是偶數這個條件。

第 (iii) 部分

用反證法（proof by contradiction）：假設 p 和 q 都是奇數，並設 $r = pq$，它也是奇數。那麼

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

所以 $1 \equiv -1$，即 $N \mid 2$，但 $N \geq 3$，這不可能。因此 p 和 q 不可能同時是奇數。

（根據對稱性，第 (ii) 部分也說明：當 q 是偶數而 p 是奇數時，$q = 2p$。所以在任何情況下，m 和 $N - m$ 的階要麼相等且為偶數，要麼其中一個是另一個的兩倍，而後者是奇數。）

模 21 的羣

2 和 5 的各次冪模 21 化簡後，依次為

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 $2^5 = 32 \equiv 11$，$5^2 = 25 \equiv 4$，$5^4 \equiv 4^2 = 16$，$5^5 \equiv 80 \equiv 17$）。兩行中的 1 都是在 $k = 6$ 時首次出現，所以 2 和 5 的階都是 6。

現在從表中讀出各元素的階：若 x 的階為 6，則 x^k 的階為 $6/\gcd(k, 6)$。所以

- $11 = 2^5$ 和 $17 = 5^5$ 的階為 6；
- $4 = 2^2$ 和 $16 = 2^4$ 的階為 3；
- $8 = 2^3$ 和 $20 = 5^3$ 的階為 2（由於 $20 = N - 1$，題目的第一部分已經告訴我們這一點）；
- 1 的階為 1。

餘下的是 10、13 和 19，它們各自與一個已知的元素相加得 21：

- $13 = 21 - 8$，而 8 的階是偶數 2。根據 (iii) 及其後的備註，13 的階要麼是 2（相等且為偶數），要麼是 1（即 2 的一半）。它不是 1，因為 $13 \neq 1$，所以 13 的階為 2。（驗算：$13^2 = 169 = 8 \cdot 21 + 1$。）
- $19 = 21 - 2$ 及 $10 = 21 - 11$，而 2 和 11 的階都是 6。所以 19 和 10 各自的階是 6 或 3。

所以 G 的每個元素的階都不超過 6。階為 12 的循環羣（cyclic group）有一個生成元（generator），即一個階為 12 的元素，而同構（isomorphism）保持元素的階不變。由於 G 沒有階為 12 的元素，它與階為 12 的循環羣並不同構。

還有另一種方法完成這一步：G 有三個階為 2 的元素，即 8、13 和 20，而階為 12 的循環羣恰好只有一個（若 g 是它的生成元，則 g^k 的階為 2 僅當 $k = 6$）。

驗算

用電腦驗算，可得 G 中各元素的階的完整列表：1 的階為 1；$8, 13, 20$ 的階為 2；$4, 16$ 的階為 3；而 $2, 5, 10, 11, 17, 19$ 的階為 6。（直接計算，$10^3 = 1000 \equiv 13$ 及 $19^3 \equiv (-2)^3 = -8 \equiv 13$，所以兩者的階都不是 3。）各類元素的數目 $1 + 3 + 2 + 6 = 12$ 與 G 的大小吻合。我們亦對所有 $N < 60$，在單位羣中由最多兩個元素生成的每個子羣（subgroup）裏，就每一對 m、$N - m$ 檢驗了第 (i) 至 (iii) 部分：共近 1900 對，無一例外。

常見錯誤

- 假設 $N-1 \in G$ 而不說明原因。題目並沒有給出這一點，但它可由 $m, n \in G$ 推出，因為 $N-1 \equiv n\,m^{-1}$。
- 在 (ii) 中只證明了 $p \mid 2q$；還需要多一個整除關係才能得到等式。
- 在古怪的情況下把單位元視為理所當然：例如模 6 之下的子集 $\{3\}$ 對乘法封閉，其單位元為 3，而取 $m = n = 3$ 時便會違反 (iii)。本題的論證依賴單位元是 1，而這顯然正是題目的原意。

STEP 之外

G 是模 21 的單位羣（group of units），根據中國剩餘定理（Chinese remainder theorem），它同構於模 3 和模 7 的單位羣的直積，即 $C_2 \times C_6$：這就是為甚麼它有三個階為 2 的元素，卻沒有階為 12 的元素。判斷模 N 的單位在甚麼時候構成循環羣（恰好是 $N = 2, 4, p^k, 2p^k$ 的情況，其中 p 是奇質數，亦即存在「原根」（primitive root）的情況），是大學一年級數論的經典結果。Davenport 的 *The Higher Arithmetic* 講述了原根，而 Allenby 的 *Rings, Fields and Groups* 則討論了相關的羣論。

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。