詳細解答

STEP I 1996，第 3 題

純數學 • 整數的整除性

> **STEP I 1996，第 3 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/96-s1-q3

關鍵思路

要處理被合成數（composite number）如 24 整除（divisibility）的問題，最簡單的做法是逐個質數冪（prime power）處理：$24 = 3 \times 8$，而 3 與 8 互質（coprime），所以我們分別證明可被 3 整除和可被 8 整除。因式分解（factorise）之後會得到連續整數之積，而任意 k 個連續整數之中，必有一個是 k 的倍數。其餘兩部分也可用同一習慣解決：因式分解，或者把 n 寫成能顯示其餘數的形式。

解答

第 (i) 部分

抽出公因式，再運用平方差公式（difference of two squares），

$$n^5 - n^3 = n^3(n^2 - 1) = n^3(n-1)(n+1) = n^2\,(n-1)\,n\,(n+1).$$

可被 3 整除。$n-1$、n、$n+1$ 是三個連續整數，所以其中恰好有一個是 3 的倍數。因此 $3 \mid (n-1)n(n+1)$，從而 $3 \mid n^5 - n^3$。

可被 8 整除。我們按 n 的奇偶性（parity）分情況討論。

- 若 n 是偶數，設 $n = 2m$，則 $n^3 = 8m^3$，是 8 的倍數。
- 若 n 是奇數，則 $n-1$ 和 $n+1$ 是連續偶數。任意兩個連續偶數之中，一個是 4 的倍數，另一個是 2 的倍數，所以 $8 \mid (n-1)(n+1)$。

無論哪種情況，都有 $8 \mid n^3(n-1)(n+1) = n^5 - n^3$。

想一想 為甚麼知道 $3 \mid N$ 和 $8 \mid N$ 就可以推出 $24 \mid N$？換成 $4 \mid N$ 和 $6 \mid N$，結論還成立嗎？

由於 3 和 8 沒有公因數，$8 \mid N$ 表示 $N = 8a$，於是 $3 \mid 8a$ 迫使 $3 \mid a$（因為 3 是質數，而且不整除 8）。所以 $N = 24b$。這個論證對 4 和 6 並不成立，因為兩者有公因數 2：12 可同時被兩者整除，卻不能被 24 整除。

因此，對每個正整數 n，$n^5 - n^3$ 都可被 24 整除，證畢。

第 (ii) 部分

寫成 $2^{2n} = 4^n$。運用因式分解 $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$，取 $x = 4$，

$$2^{2n} - 1 = 4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right) = 3\left(4^{n-1} + \cdots + 1\right).$$

括號內是整數，所以 $2^{2n} - 1$ 可被 3 整除。

用模算術（modular arithmetic）來說，這等價於：$4 \equiv 1 \pmod 3$，所以 $4^n \equiv 1^n = 1 \pmod 3$。用歸納法（induction）證明也可以：若 $4^k - 1 = 3a$，則 $4^{k+1} - 1 = 4(4^k - 1) + 3 = 3(4a + 1)$。

第 (iii) 部分

由於 $3 \mid n - 1$，可寫 $n = 3k + 1$，其中 $k \geq 0$ 為某個整數。因式分解得

$$n^3 - 1 = (n-1)(n^2 + n + 1).$$

第一個因式是 $n - 1 = 3k$。至於第二個，

$$\begin{aligned} n^2 + n + 1 &= (9k^2 + 6k + 1) + (3k + 1) + 1 \\ &= 9k^2 + 9k + 3 \\ &= 3(3k^2 + 3k + 1). \end{aligned}$$

所以每個因式各提供一個 3：

$$n^3 - 1 = 3k \cdot 3(3k^2 + 3k + 1) = 9k(3k^2 + 3k + 1),$$

它可被 9 整除，證畢。（當 $n = 1$ 時，$k = 0$，$n^3 - 1 = 0$，同樣可被 9 整除。）

重點在於 $n - 1$ 只提供一個因數 3；第二個來自 $n^2 + n + 1$。要看出這第二個因數，有一個巧妙的方法：$n^2 + n + 1 = (n-1)^2 + 3n$，只要 $3 \mid n - 1$，這就是兩個 3 的倍數之和。

驗算

- 第 (i) 部分：$n = 2$ 給出 $32 - 8 = 24$，$n = 3$ 給出 $243 - 27 = 216 = 9 \times 24$。由於 $n = 2$ 時剛好得到 24，沒有更大的數能整除每一個 $n^5 - n^3$，所以 24 已是最佳結果。
- 第 (ii) 部分：$n = 1, 2, 3$ 分別給出 3、15、63。
- 第 (iii) 部分：$n = 4$ 給出 $63 = 7 \times 9$，$n = 7$ 給出 $342 = 38 \times 9$，與 $9k(3k^2 + 3k + 1)$ 在 $k = 1$ 和 $k = 2$ 時的值吻合。

我們用電腦對所有小於 5000 的 n 驗證了全部三個結果（第 (ii) 部分則驗證了 $n < 2000$），並確認 $n^5 - n^3$ 各個值的最大公因數（highest common factor）恰好是 24。

常見錯誤

- 論證時寫「$(n-1)n(n+1)$ 可被 6 整除，而 n^2 是 ...」，結果弄不清因數 8 從何而來。偶數的情況需要用到 n^3，而不只是 n。
- 由可被 4 整除和可被 6 整除推斷可被 24 整除；兩個因數必須互質。
- 在第 (iii) 部分，寫到「$n - 1$ 可被 3 整除，所以 $n^3 - 1 = (n-1)(\dots)$ 可被 3 整除」便停下來，這樣只得到一個因數 3。

STEP 之外

這三部分其實都是模算術中的命題：模 m 的整數構成一個環（ring），而第 (iii) 部分說的是：若 $n \equiv 1 \pmod 3$，則 $n^3 \equiv 1 \pmod 9$。這是一個稱為*指數提升*（*lifting the exponent*）的一般現象的第一步：若 $p \mid n - 1$，則 $p^{j+1} \mid n^{p^j} - 1$。費馬小定理（Fermat's little theorem，$n^p \equiv n \pmod p$）也能解釋第 (i) 部分，因為它直接給出 $3 \mid n^3 - n$。Davenport 的 *The Higher Arithmetic*（一本講高等算術的數論入門書）是這些思想的一本優美入門讀物。

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。