詳細解答

STEP I 1992，第 5 題

純數學 • 多項式的重因式

> **STEP I 1992，第 5 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/92-s1-q5

本題在 *Beyond STEP* 第 9.7 節相等的冪和中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch09/equal-power-sums.html

關鍵思路

若一個多項式（polynomial）有重因式（repeated factor）$(1-x)^m$，則對它求導（再乘以 x）之後，仍會留下因式 $(1-x)^{m-1}$。因此 1 是這個多項式的根（root），也是這條鏈中隨後幾個多項式的根。利用各多項式的係數（coefficient）計算它們在 $x=1$ 的值，會得到形如 $\sum k^r c_k$ 的和。當每個係數都是 ± 1 時，每一個這樣的和都表示：兩組整數的 r 次冪之和相等。

解答

因式 $(1-x)^3$

兩次運用平方差（difference of two squares），

$$1-x^2=(1-x)(1+x), \qquad 1-x^4=(1-x^2)(1+x^2)=(1-x)(1+x)(1+x^2),$$

所以

$$p_0(x)=(1-x)^3(1+x)^2(1+x^2),$$

故 $(1-x)^3$ 是 $p_0(x)$ 的因式，正如題目所求。

$p_0'(1)=0$ 與 $p_1'(1)=0$

我們先證明一個小結果，然後重複使用。

引理（*Lemma*）。若 $\mathrm{p}(x) = (1-x)^m \mathrm{q}(x)$，其中 $m \geq 1$，而 q 是多項式，則 $\mathrm{p}'(x)$ 有因式 $(1-x)^{m-1}$，因而 $x\mathrm{p}'(x)$ 亦然。

證明。根據積法則（product rule），

$$\mathrm{p}'(x) = -m(1-x)^{m-1}\mathrm{q}(x) + (1-x)^m \mathrm{q}'(x) = (1-x)^{m-1}\big[(1-x)\mathrm{q}'(x) - m\,\mathrm{q}(x)\big],$$

而方括號內是一個多項式。乘以 x 並不會除去這個因式。□

取 $m = 3$ 應用此引理：$\mathrm{p}_0'(x)$ 有因式 $(1-x)^2$，所以 $\mathrm{p}_0'(1) = 0$。同時 $\mathrm{p}_1(x) = x\mathrm{p}_0'(x)$ 也有因式 $(1-x)^2$。再取 $m = 2$ 應用引理，$\mathrm{p}_1'(x)$ 有因式 $1-x$，所以 $\mathrm{p}_1'(1) = 0$。

想一想 為甚麼不直接對三個括號的乘積求導，然後代入 $x = 1$？

這樣做也可以，但題目要求我們從因式出發論證，而且因式的論證才是可以推廣的那一種。重數（multiplicity）為 m 的根，經過 $m-1$ 次求導後仍然是根，而這正是最後一部分所需要的。

兩個恆等式

展開得

$$(1-x)(1-x^2) = 1 - x - x^2 + x^3,$$

然後

$$\mathrm{p}_0(x) = 1 - x - x^2 + x^3 - x^4 + x^5 + x^6 - x^7.$$

所以 $c_0 = c_3 = c_5 = c_6 = 1$，而 $c_1 = c_2 = c_4 = c_7 = -1$。

現在

$$\mathrm{p}_0'(x) = \sum_{k=1}^{7} k\,c_k x^{k-1}, \qquad \mathrm{p}_1(x) = \sum_{k=0}^{7} k\,c_k x^k, \qquad \mathrm{p}_1'(x) = \sum_{k=1}^{7} k^2 c_k x^{k-1}.$$

代入 $x = 1$，並利用 $\mathrm{p}_0'(1) = 0$：

$$-1 - 2 + 3 - 4 + 5 + 6 - 7 = 0, \quad \text{即} \quad 1 + 2 + 4 + 7 = 3 + 5 + 6.$$

利用 $\mathrm{p}_1'(1) = 0$：

$$-1^2 - 2^2 + 3^2 - 4^2 + 5^2 + 6^2 - 7^2 = 0, \quad \text{即} \quad 1^2 + 2^2 + 4^2 + 7^2 = 3^2 + 5^2 + 6^2.$$

（兩邊都等於 14；平方的情況則都等於 70。）c_0 一項沒有任何貢獻，因為它乘上了 0 或 0^2。

最後一部分

再多走一步。設

$$\mathrm{P}_0(x) = (1-x)(1-x^2)(1-x^4)(1-x^8) = \mathrm{p}_0(x)(1-x^8).$$

由於 $1-x^8 = (1-x)(1+x)(1+x^2)(1+x^4)$，$\mathrm{P}_0(x)$ 有因式 $(1-x)^4$。對 $j=0,1,2$，定義 $\mathrm{P}_{j+1}(x) = x\mathrm{P}_j'(x)$。根據引理，$\mathrm{P}_1$、$\mathrm{P}_2$ 和 P_3 分別有因式 $(1-x)^3$、$(1-x)^2$ 和 $(1-x)$，所以

$$\mathrm{P}_1(1) = \mathrm{P}_2(1) = \mathrm{P}_3(1) = 0.$$

記 $\mathrm{P}_0(x) = \sum_{k=0}^{15} d_k x^k$。每施行一次 $x\frac{\mathrm{d}}{\mathrm{d}x}$，$x^k$ 的係數便乘以 k，所以 $\mathrm{P}_r(x) = \sum_{k=0}^{15} k^r d_k x^k$，於是

$$\sum_{k=1}^{15} k^r d_k = 0 \qquad \text{其中} r = 1,2,3.$$

要求出各個 d_k，把 $\mathrm{p}_0(x)$ 乘以 $1-x^8$，得

$$\mathrm{P}_0(x) = \mathrm{p}_0(x) - x^8\mathrm{p}_0(x).$$

第二項給出 $x^8,\ldots,x^{15}$ 各項，其正負號與 p_0 的相反。兩部分沒有重疊，所以每個 d_k 都是 ±1：

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d_k	+	−	−	+	−	+	+	−	−	+	+	−	+	−	−	+

（事實上 $d_k = (-1)^{s(k)}$，其中 $s(k)$ 是 k 的二進制展開式（binary expansion）中 1 的個數，因為 x^k 是按 k 的二進制數字，從對應的括號中選取 $-x^{2^i}$ 而得出的。）

撇除 $k=0$，當 $k \in \{1,2,4,7,8,11,13,14\}$（八個數）時係數 $d_k = -1$，當 $k \in \{3,5,6,9,10,12,15\}$（七個數）時 $d_k = +1$。這些數合起來恰好是 $1,2,\ldots,15$。於是取

$$(a_1,\ldots,a_8) = (1,2,4,7,8,11,13,14), \qquad (a_9,\ldots,a_{15}) = (3,5,6,9,10,12,15).$$

那麼 $\sum k^r d_k = 0$ 所說的正是

$$a_1^r + \cdots + a_8^r = a_9^r + \cdots + a_{15}^r \qquad (r = 1,2,3),$$

這就是我們要證明的結果。

想一想 為甚麼這個分法一邊有八個數，另一邊只有七個？

$+1$ 的一邊其實還包含 $k=0$，而當 $r \geq 1$ 時它的貢獻是 $0^r = 0$，所以可以略去。這就是兩邊的項數不必相同的原因。（若 $r=0$，恆等式便需要這個 0：這時是 $8=8$。）

驗算

直接計算：$r = 1$ 時兩邊之和為 $60 = 60$，$r = 2$ 時為 $620 = 620$，$r = 3$ 時為 $7200 = 7200$。我們用電腦展開了 P_0，確認了它各項的正負號，以及根 $x = 1$ 的重數為 4，並驗證了全部三個等式。當 $r = 4$ 時等式不成立（該根的重數只有 4），這正好顯示上述論證已是最佳的。

常見錯誤

- 忘記了 $k = 0$ 一項，因而以為兩邊的項數必須相同。
- 單憑 $\mathrm{p}_0''(1) = 0$ 便斷定 $\mathrm{p}_1'(1) = 0$。由於 $\mathrm{p}_1' = \mathrm{p}_0' + x\mathrm{p}_0''$，你需要 $\mathrm{p}_0'(1) = 0$ 和 $\mathrm{p}_0''(1) = 0$ 兩者同時成立。

STEP 之外

這就是 Prouhet–Tarry–Escott 問題：按二進制數字和的奇偶性（parity）把 $\{0, 1, \ldots, 2^n - 1\}$ 分成兩組（即 Thue–Morse 數列），所得的兩個集合對所有 $r < n$ 都有相等的 r 次冪之和。它背後的工具——重數為 m 的根同時是首 $m - 1$ 階導數（derivative）的根——在任何域（field）上的多項式代數中都佔有核心地位。關於多項式及其根的代數，可參閱 Allenby 的 *Rings, Fields and Groups*（環、域與羣）。至於更廣泛的數論（number theory），可參閱 Davenport 的 *The Higher Arithmetic*（高等算術）。

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。