详细解答

STEP I 1992，第 5 题

纯数学 · 多项式的重因式

> **STEP I 1992，第 5 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/92-s1-q5

本题在 *Beyond STEP* 第 9.7 节相等的幂和中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch09/equal-power-sums.html

关键思路

若一个多项式（polynomial）有重因式（repeated factor）$(1-x)^m$，则对它求导（再乘以 x）之后，仍会留下因式 $(1-x)^{m-1}$。因此 1 是这个多项式的根（root），也是这条链中随后几个多项式的根。利用各多项式的系数（coefficient）计算它们在 $x=1$ 的值，会得到形如 $\sum k^r c_k$ 的和。当每个系数都是 ± 1 时，每一个这样的和都表示：两组整数的 r 次幂之和相等。

解答

因式 $(1-x)^3$

两次运用平方差（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，正如题目所求。

$p_0'(1)=0$ 与 $p_1'(1)=0$

我们先证明一个小结果，然后重复使用。

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

证明。根据积法则（product rule），

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

而方括号内是一个多项式。乘以 x 并不会除去这个因式。□

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

想一想 为甚么不直接对三个括号的乘积求导，然后代入 $x = 1$?

这样做也可以，但题目要求我们从因式出发论证，而且因式的论证才是可以推广的那一种。重数（multiplicity）为 m 的根，经过 $m-1$ 次求导后仍然是根，而这正是最后一部分所需要的。

两个恒等式

展开得

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

然后

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

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

现在

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

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

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

利用 $\mathrm{p}_1'(1) = 0$:

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

（两边都等于 14；平方的情况则都等于 70。）c_0 一项没有任何贡献，因为它乘上了 0 或 0^2。

最后一部分

再多走一步。设

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

由于 $1-x^8=(1-x)(1+x)(1+x^2)(1+x^4)$，$\mathrm{P}_0(x)$ 有因式 $(1-x)^4$。对 $j=0,1,2$，定义 $\mathrm{P}_{j+1}(x)=x\mathrm{P}_j'(x)$。根据引理，$\mathrm{P}_1$、$\mathrm{P}_2$ 和 P_3 分别有因式 $(1-x)^3$、$(1-x)^2$ 和 $(1-x)$，所以

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

记 $\mathrm{P}_0(x)=\sum_{k=0}^{15}d_kx^k$。每施行一次 $x\frac{\mathrm{d}}{\mathrm{d}x}$，$x^k$ 的系数便乘以 k，所以 $\mathrm{P}_r(x)=\sum_{k=0}^{15}k^rd_kx^k$，于是

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

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

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

第二项给出 $x^8,\ldots,x^{15}$ 各项，其正负号与 p_0 的相反。两部分没有重叠，所以每个 d_k 都是 ±1：

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

（事实上 $d_k=(-1)^{s(k)}$，其中 $s(k)$ 是 k 的二进制展开式（binary expansion）中 1 的个数，因为 x^k 是按 k 的二进制数字，从对应的括号中选取 $-x^{2^i}$ 而得出的。）

撇除 $k=0$，当 $k\in\{1,2,4,7,8,11,13,14\}$（八个数）时系数 $d_k=-1$，当 $k\in\{3,5,6,9,10,12,15\}$（七个数）时 $d_k=+1$。这些数合起来恰好是 $1,2,\ldots,15$。于是取

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

那么 $\sum k^rd_k=0$ 所说的正是

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

这就是我们要证明的结果。

想一想 为甚么这个分法一边有八个数，另一边只有七个?

$+1$ 的一边其实还包含 $k=0$，而当 $r\geq1$ 时它的贡献是 $0^r=0$，所以可以略去。这就是两边的项数不必相同的原因。（若 $r=0$，恒等式便需要这个 0：这时是 $8=8$。）

验算

直接计算：$r=1$ 时两边之和为 $60=60$，$r=2$ 时为 $620=620$，$r=3$ 时为 $7200=7200$。我们用电脑展开了 P_0，确认了它各项的正负号，以及根 $x=1$ 的重数为 4，并验证了全部三个等式。当 $r=4$ 时等式不成立（该根的重数只有 4），这正好显示上述论证已是最佳的。

常见错误

- 忘记了 $k = 0$ 一项，因而以为两边的项数必须相同。
- 单凭 $\mathrm{p}_0''(1) = 0$ 便断定 $\mathrm{p}_1'(1) = 0$。由于 $\mathrm{p}_1' = \mathrm{p}_0' + x\mathrm{p}_0''$，你需要 $\mathrm{p}_0'(1) = 0$ 和 $\mathrm{p}_0''(1) = 0$ 两者同时成立。

STEP 之外

这就是 Prouhet–Tarry–Escott 问题：按二进制数字和的奇偶性（parity）把 $\{0, 1, \ldots, 2^n - 1\}$ 分成两组（即 Thue–Morse 数列），所得的两个集合对所有 $r < n$ 都有相等的 r 次幂之和。它背后的工具——重数为 m 的根同时是首 $m - 1$ 阶导数（derivative）的根——在任何域（field）上的多项式代数中都占有核心地位。关于多项式及其根的代数，可参阅 Allenby 的 *Rings, Fields and Groups*（环、域与群）。至于更广泛的数论（number theory），可参阅 Davenport 的 *The Higher Arithmetic*（高等算术）。

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。