解答例

# STEP I 1992、第 5 問

純粋数学 • 多項式の重複因数

> **STEP I 1992、問 5**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/92-s1-q5

この問題は、*Beyond STEP* の第 9.7 節「**等しい累乗和**」で詳しく解説されている：
https://beyondstep.keithmcnulty.org/ja/ch09/equal-power-sums.html

## 鍵となる考え方

多項式（polynomial）が重複因数（repeated factor）$(1-x)^m$ をもつとき、それを微分して（$x$ を掛けて）も因数 $(1-x)^{m-1}$ が残る。したがって 1 はその多項式の根（root）であり、さらにそこから続くいくつかの多項式の根でもある。これらの多項式それぞれの $x=1$ における値を係数を用いて計算すると、$\sum k^r c_k$ の形の和が得られる。係数がすべて $\pm 1$ であるとき、これらの和はそれぞれ、二つの整数の集合の $r$ 乗の和が等しいことを表している。

## 解答

**因数** $(1-x)^3$

平方の差の因数分解（difference of two squares）を 2 回用いると、

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

であるから、

$$\mathrm{p}_0(x)=(1-x)^3(1+x)^2(1+x^2),$$

となり、$(1-x)^3$ は $\mathrm{p}_0(x)$ の因数である。これが示すべきことであった。

$p_0'(1) = 0$ **と** $p_1'(1) = 0$

小さな事実を一つ証明し、それを繰り返し用いる。

**補題**（*lemma*）。 $m \geq 1$ で $q$ が多項式であるとき、$p(x) = (1-x)^m q(x)$ ならば、$p'(x)$、したがって $xp'(x)$ は因数 $(1-x)^{m-1}$ をもつ。

**証明。**積の微分法（product rule）により、

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

であり、括弧の中は多項式である。$x$ を掛けてもこの因数は消えない。□

これを $m = 3$ として適用すると、$p_0'(x)$ は因数 $(1-x)^2$ をもつので、$p_0'(1) = 0$ である。また $p_1(x) = xp_0'(x)$ も因数 $(1-x)^2$ をもつ。補題を $m = 2$ として再び適用すると、$p_1'(x)$ は因数 $1-x$ をもつので、$p_1'(1) = 0$ である。

**考えてみよう** 三つの括弧の積をそのまま微分して $x = 1$ を代入すればよいのではないか？

それも可能であるが、問題は因数から議論することを求めており、また一般化できるのは因数による議論のほうである。重複度（multiplicity）$m$ の根は $m-1$ 回の微分を経ても根として残り、最後の小問で必要になるのはまさにこの事実である。

### 二つの恒等式

展開すると、

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

であり、さらに

$$p_0(x) = 1 - x - x^2 + x^3 - x^4 + x^5 + x^6 - x^7.$$

となる。よって $c_0 = c_3 = c_5 = c_6 = 1$、$c_1 = c_2 = c_4 = c_7 = -1$ である。

ここで

$$p_0'(x) = \sum_{k=1}^{7} k\,c_k x^{k-1}, \qquad p_1(x) = \sum_{k=0}^{7} k\,c_k x^k, \qquad p_1'(x) = \sum_{k=1}^{7} k^2 c_k x^{k-1}.$$

$x = 1$ とおき、$p_0'(1) = 0$ を用いると、

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

$p_1'(1) = 0$ を用いると、

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

（両辺はともに 14 に等しく、平方については 70 に等しい。）$c_0$ の項は 0 または $0^2$ が掛けられるので、何も寄与しない。

### 最後の小問

さらに一段階進める。

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

とおく。$1-x^8 = (1-x)(1+x)(1+x^2)(1+x^4)$ であるから、$\mathrm{P}_0(x)$ は因数 $(1-x)^4$ をもつ。$j = 0, 1, 2$ に対して $\mathrm{P}_{j+1}(x) = x\mathrm{P}_j'(x)$ と定める。補題により、$\mathrm{P}_1$、$\mathrm{P}_2$、$\mathrm{P}_3$ はそれぞれ因数 $(1-x)^3$、$(1-x)^2$、$(1-x)$ をもつので、

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

である。

$\mathrm{P}_0(x) = \sum_{k=0}^{15} d_k x^k$ と書く。$x\frac{\mathrm{d}}{\mathrm{d}x}$ を 1 回施すごとに $x^k$ の係数は $k$ 倍されるので、$\mathrm{P}_r(x) = \sum_{k=0}^{15} k^r d_k x^k$ であり、

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

が成り立つ。

$d_k$ を求めるために、$\mathrm{p}_0(x)$ に $1-x^8$ を掛ける。すると

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

となる。第 2 項からは、$\mathrm{p}_0$ の符号を反転させた $x^8, \ldots, x^{15}$ の項が得られる。重なりはないので、すべての $d_k$ は $\pm 1$ である：

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

（実際、$s(k)$ を $k$ の二進展開（binary expansion）に現れる 1 の個数とすると、$d_k = (-1)^{s(k)}$ である。なぜなら、$x^k$ は $k$ の二進数の各桁に対応する括弧から $-x^{2^i}$ を選ぶことで得られるからである。）

$k = 0$ を除くと、係数は $k \in \{1, 2, 4, 7, 8, 11, 13, 14\}$（8 個の数）に対して $d_k = -1$、$k \in \{3, 5, 6, 9, 10, 12, 15\}$（7 個の数）に対して $d_k = +1$ である。これらを合わせるとちょうど $1, 2, \ldots, 15$ になる。そこで

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

とおく。すると $\sum k^r d_k = 0$ はまさに

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

を意味し、これが示すべきことであった。

**考えてみよう** 分け方が一方に 8 個、もう一方に 7 個となるのはなぜか？

$+1$ の側には $k = 0$ も含まれるが、これは $r \geq 1$ に対して $0^r = 0$ しか寄与しないので除いてよい。そのため両辺の項数は等しくなくてよいのである。（$r = 0$ の場合には恒等式に 0 が必要になり、そのとき $8 = 8$ となる。）

## 検算

直接計算すると、和は $r = 1$ で $60 = 60$、$r = 2$ で $620 = 620$、$r = 3$ で $7200 = 7200$ となる。コンピュータで $\mathrm{P}_0$ を展開し、その符号と根 $x = 1$ の重複度が 4 であることを確認し、三つの等式すべてを検証した。$r = 4$ では等式は成り立たない（根の重複度は 4 しかない）。これは議論が最良であることを示すよい兆候である。

## よくある間違い

- $k = 0$ の項を忘れ、両辺の個数が等しくなければならないと考えてしまう。
- $\mathrm{p}_0''(1) = 0$ だけから $\mathrm{p}_1'(1) = 0$ を結論してしまう。$\mathrm{p}_1' = \mathrm{p}_0' + x\mathrm{p}_0''$ であるから、$\mathrm{p}_0'(1) = 0$ と $\mathrm{p}_0''(1) = 0$ の両方が必要である。

## STEP のその先へ

これはプルーエ–タリー–エスコット問題（Prouhet–Tarry–Escott problem）である。$\{0, 1, \ldots, 2^n - 1\}$ を二進数の各桁の和の偶奇（トゥエ–モース数列（Thue–Morse sequence））によって分けると、$r < n$ のすべての $r$ に対して $r$ 乗の和が等しい二つの集合が得られる。その背後にある道具、すなわち重複度 $m$ の根は最初の $m - 1$ 個の導関数の根でもあるという事実は、任意の体（field）上の多項式の代数において中心的な役割を果たす。多項式とその根の代数については、Allenby, *Rings, Fields and Groups*（環・体・群）を参照せよ。より一般に数論（number theory）については、Davenport, *The Higher Arithmetic*（高等算術）を参照せよ。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。