解答例

STEP III 2010、第 3 問

純粋数学 ・ 1 の冪根

> **STEP III 2010、問 3**
>
> 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/10-s3-q3

この問題は、*Beyond STEP* の第 6.1 節「**1 の累乗根を根にもつ多項式**」で詳しく解説されている：https://beyondstep.keithmcnulty.org/ja/ch06/cyclotomic.html

鍵となる考え方

1 の冪根（root of unity）a には、それぞれただ一つの**位数**（order）が定まる。すなわち、$a^m = 1$ を満たす最小の正の整数 m である。1 の原始 n 乗根（primitive nth root of unity）であるとは、位数がちょうど n であることにほかならない。したがって $\mathrm{C}_n(x)$ を求めるには、1 の n 乗根 $\mathrm{e}^{2\pi \mathrm{i} k/n}$ を列挙し、それより前の冪ですでに 1 に戻るものを取り除き、残ったものについて $(x-a)$ を掛け合わせればよい。各数の位数がただ一つであるという事実は、最後の小問を解決する鍵でもある。

解答

以下を通じて、1 の n 乗根は $k = 0, 1, \ldots, n-1$ に対する ω^k である。ただし $\omega = \mathrm{e}^{2\pi \mathrm{i}/n}$ であり、$(\omega^k)^m = 1$ となるのは n が km を割り切るとき、かつそのときに限る。C_n はモニック（monic）で重根（repeated roots）をもたず、その根はちょうど 1 の原始 n 乗根であるから、

$$\mathrm{C}_n(x) = \prod_{a \text{ が原始的}} (x-a).$$

4 乗根

1 の 4 乗根は $1, \mathrm{i}, -1, -\mathrm{i}$ である。ここで $1^1 = 1$、$(-1)^2 = 1$ であるから、この二つは原始的ではない。一方、$\mathrm{i}^1 = \mathrm{i}$、$\mathrm{i}^2 = -1$、$\mathrm{i}^3 = -\mathrm{i}$ はいずれも 1 に等しくなく、$-\mathrm{i}$ についても同様である（その冪は共役になる）。よって 1 の原始 4 乗根は i と $-\mathrm{i}$ であり、

$$\mathrm{C}_4(x) = (x - \mathrm{i})(x + \mathrm{i}) = x^2 + 1,$$

となって、求める結果が得られる。

小問 (i)

$n = 1$ のとき。 1 の 1 乗根は 1 のみであり、$0 < m < 1$ を満たす m は存在しないから、1 は原始的である：$\mathrm{C}_1(x) = x - 1$。

$n = 2$ のとき。 1 の平方根は ± 1 である。$1^1 = 1$ より 1 は除かれ、一方 $(-1)^1 \neq 1$ である。よって $\mathrm{C}_2(x) = x + 1$。

$n = 3$ および $n = 5$ のとき。 n が素数（prime）のとき、$1 \leq k \leq n - 1$ なる根 ω^k が $(\omega^k)^m = 1$ を満たすのは $n \mid km$ のときに限る。n は素数で k を割り切らないから、これより $n \mid m$ が従う。したがって、1 以外のすべての 1 の n 乗根は原始的である。これらは

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1,$$

の根であり、この多項式はモニックで相異なる根をもつ。よって

$$\mathrm{C}_3(x) = x^2 + x + 1, \qquad \mathrm{C}_5(x) = x^4 + x^3 + x^2 + x + 1.$$

$n = 6$ のとき。 $\omega = \mathrm{e}^{\pi \mathrm{i}/3}$ とすると、冪 ω^k の位数は $6/\gcd(k, 6)$ である。よって $\omega^0 = 1$ の位数は 1、$\omega^3 = -1$ の位数は 2、ω^2, ω^4 の位数は 3 であり、位数 6 をもつのは ω と $\omega^5 = \overline{\omega}$ のみである。それらの和は $2\cos\frac{\pi}{3} = 1$、積は $|\omega|^2 = 1$ であるから、

$$\mathrm{C}_6(x) = x^2 - x + 1.$$

（検算として、1 の 6 乗根の位数はすべて 1、2、3、6 のいずれかであるから $x^6 - 1 = \mathrm{C}_1\mathrm{C}_2\mathrm{C}_3\mathrm{C}_6$ であり、実際 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = (x^3-1)(x^3+1) = x^6 - 1$ である。）

小問 (ii)

a を $x^4 + 1 = 0$ の任意の根とする。すると $a^4 = -1$ であるから $a^8 = 1$ である。a の位数 d は 8 を割り切る（$0 \leq r < d$ として $8 = qd + r$ と書くと $a^r = a^8(a^d)^{-q} = 1$ となり、d の最小性より $r = 0$ である）。よって $d \in \{1, 2, 4, 8\}$ である。もし d が 1、2、4 のいず

れかならば $a^4 = 1$ となり、$a^4 = -1$ に矛盾する。したがって、$x^4 + 1$ のすべての根は 1 の原始 8 乗根である。

逆に、$\omega = \mathrm{e}^{\pi \mathrm{i}/4}$ として ω^k の位数が 8 となるのは、k が奇数のとき、かつそのときに限る（k が偶数ならば $(\omega^k)^4 = 1$ である）。したがって原始 8 乗根はちょうど四つ、すなわち $\omega, \omega^3, \omega^5, \omega^7$ である。4 次式 $x^4 + 1$ は相異なる四つの根（それらは $\mathrm{e}^{(2j+1)\pi \mathrm{i}/4}$、$j = 0, 1, 2, 3$ である）をもち、それらはすべて原始 8 乗根であるから、まさにこの四つである。よって $\mathrm{C}_8(x) = x^4 + 1$ である。

ほかの n は条件を満たさない。C_n の根はすべて位数 n をもち、$x^4 + 1$ の根は位数 8 をもつからである。よって答えは $n = 8$ である。

小問 (iii)

小問 (i) で $n = 3$ と $n = 5$ に対して用いた議論は、任意の素数 p に適用できる。すなわち、1 以外のすべての 1 の p 乗根は原始的である。したがって

$$\mathrm{C}_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

（$p = 2$ のとき、これは $x + 1$ となり、小問 (i) と一致する。）

小問 (iv)

背理法（proof by contradiction）により、ある正の整数 q, r, s に対して $\mathrm{C}_q(x) \equiv \mathrm{C}_r(x)\mathrm{C}_s(x)$ が成り立つと仮定する。

まず、C_s は少なくとも一つの根をもつ。$\mathrm{e}^{2\pi \mathrm{i}/s}$ が 1 の原始 s 乗根だからである：$(\mathrm{e}^{2\pi \mathrm{i}/s})^m = \mathrm{e}^{2\pi \mathrm{i} m/s} = 1$ となるのは $s \mid m$ のときに限る。C_r についても同様である。よって C_r と C_s の次数（degree）はともに 1 以上である。

C_r の任意の根 a をとる。恒等式（identity）より $\mathrm{C}_q(a) = \mathrm{C}_r(a)\mathrm{C}_s(a) = 0$ であるから、a は 1 の原始 q 乗根であると同時に、1 の原始 r 乗根でもある。

> **考えてみよう** 一つの数が、$r \neq q$ でありながら 1 の原始 r 乗根であり、かつ 1 の原始 q 乗根でもあることはありうるだろうか？

ありえない。例えば $r < q$ ならば、$0 < r < q$ で $a^r = 1$ となり、a が原始 q 乗根であることに矛盾する。$q < r$ のときは役割を入れ替えればよい。よって $r = q$ であり、同様に（C_s の根を用いて）$s = q$ である。

しかしこのとき、恒等式は $\mathrm{C}_q = \mathrm{C}_q^2$ となる。次数を比較すると $\deg \mathrm{C}_q = 2 \deg \mathrm{C}_q$ であるから $\deg \mathrm{C}_q = 0$ となり、C_q が根をもつことに矛盾する。（あるいは、C_q^2 は重根をもつが、C_q はもたない、と論じてもよい。）したがって、そのような q, r, s は存在しない。

検算

- C_n の次数は、$1 \le k \le n$ かつ $\gcd(k,n) = 1$ を満たす k の個数に等しい。$n = 1,\dots,6$ に対して次数は $1,1,2,2,4,2$、$n = 8$ に対して 4 であり、すべて一致する。
- 1 の n 乗根はいずれも n を割り切るある位数 d をもつから、$x^n - 1$ は n の約数 d にわたる C_d の積である。$n = 4$ のとき：$(x-1)(x+1)(x^2+1) = x^4 - 1$。$n = 8$ のとき：$(x^4-1)(x^4+1) = x^8 - 1$。
- 数値的に、$n \le 40$ について原始根にわたって $(x - a)$ を掛け合わせると、上のすべての多項式が再現され、$x^4 + 1$ が得られるのは $n = 8$ のときのみであり、$q, r, s \le 30$ の範囲では恒等式 $C_q = C_r C_s$ は見つからない。

よくある間違い

- 原始根の中に 1（あるいは -1）を含めてしまう：C_n は $x^n - 1$ ではない。
- 小問 (ii) で、$x^4 + 1$ が $x^8 - 1$ を割り切ることだけを確認し、より小さい位数を排除しない：要点は $a^4 = -1 \neq 1$ であることである。
- 小問 (iv) で、次数だけから論じる：$\deg C_q = \deg C_r + \deg C_s$ は起こりうる（例えば $4 = 2 + 2$）ので、矛盾を導くのは次数ではなく根である。

STEP のその先へ

C_n は**円分多項式**（cyclotomic polynomials）である。恒等式 $x^n - 1 = \prod_{d \mid n} C_d(x)$ から、これらが常に整数係数をもつことがわかる。さらに深い定理によれば、いずれも有理数体上で既約（irreducible）である。円分多項式はガロア理論（Galois theory）の中心にあり、また定規とコンパスでどの正多角形が作図可能かというガウス（Gauss）の発見においても中心的な役割を果たす。Allenby の *Rings, Fields and Groups*（環・体・群）はこの代数を展開しており、Needham の *Visual Complex Analysis*（ビジュアル複素解析）は 1 の冪根の幾何学的な描像を与えている。

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。