詳細解答

STEP III 2010，第 3 題

純數學 • 單位根

> **STEP III 2010，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/10-s3-q3

本題在 *Beyond STEP* 第 6.1 節以單位根爲根的多項式中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch06/cyclotomic.html

關鍵思路

每個單位根 a 都有唯一的階（order）：即使 $a^m = 1$ 成立的最小正整數 m。所謂本原 n 次單位根（primitive nth root of unity），就是階恰好為 n 的單位根。因此，要求 $\mathrm{C}_n(x)$，我們先列出所有 n 次單位根 $\mathrm{e}^{2\pi \mathrm{i}k/n}$，剔除那些在較低次冪時已經回到 1 的根，再把餘下的 $(x-a)$ 全部相乘。而每個數只有一個階這一事實，也正是解決最後一部分的關鍵。

解答

以下各部分中，n 次單位根為 ω^k，其中 $k = 0, 1, \ldots, n-1$，$\omega = \mathrm{e}^{2\pi \mathrm{i}/n}$；並且 $(\omega^k)^m = 1$ 當且僅當 n 整除 km。由於 C_n 是首一（monic）多項式，沒有重根，而且其根恰好是所有本原 n 次單位根，故

$$\mathrm{C}_n(x) = \prod_{a \text{ 為本原單位根}} (x - a).$$

4 次單位根

4 次單位根為 $1, \mathrm{i}, -1, -\mathrm{i}$。由於 $1^1 = 1$ 及 $(-1)^2 = 1$，這兩個根都不是本原的。但 $\mathrm{i}^1 = \mathrm{i}$、$\mathrm{i}^2 = -1$、$\mathrm{i}^3 = -\mathrm{i}$，全部不等於 1；$-\mathrm{i}$ 的情況亦相同（它的各次冪是前者的共軛（conjugate））。所以本原 4 次單位根為 i 和 $-\mathrm{i}$，從而

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

與題目所求相符。

第 (i) 部分

$n = 1$。唯一的 1 次單位根是 1，而不存在滿足 $0 < m < 1$ 的 m，所以 1 是本原的：$C_1(x) = x - 1$。

$n = 2$。2 次單位根為 ± 1；由於 $1^1 = 1$，1 被剔除，而 $(-1)^1 \neq 1$。所以 $C_2(x) = x + 1$。

$n = 3$ **及** $n = 5$。當 n 為質數（prime）時，對於滿足 $1 \leq k \leq n-1$ 的根 ω^k，$(\omega^k)^m = 1$ 只在 $n \mid km$ 時成立；又因 n 是質數且不整除 k，這迫使 $n \mid m$。所以除 1 以外的每個 n 次單位根都是本原的。它們正是

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

的根，而這個多項式是首一的，且各根互不相同。因此

$$C_3(x) = x^2 + x + 1, \qquad C_5(x) = x^4 + x^3 + x^2 + x + 1.$$

$n = 6$。設 $\omega = e^{\pi i/3}$，則 ω^k 的階為 $6/\gcd(k, 6)$。所以 $\omega^0 = 1$ 的階為 1，$\omega^3 = -1$ 的階為 2，ω^2, ω^4 的階為 3，只有 ω 和 $\omega^5 = \overline{\omega}$ 的階為 6。兩者之和為 $2\cos\frac{\pi}{3} = 1$，之積為 $|\omega|^2 = 1$，所以

$$C_6(x) = x^2 - x + 1.$$

（作為交叉驗證：每個 6 次單位根的階為 1、2、3 或 6，所以 $x^6 - 1 = C_1C_2C_3C_6$；而事實上 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = (x^3-1)(x^3+1) = x^6 - 1$。）

第 (ii) 部分

設 a 為 $x^4 + 1 = 0$ 的任一根。則 $a^4 = -1$，所以 $a^8 = 1$。a 的階 d 整除 8（寫 $8 = qd + r$，其中 $0 \leq r < d$；則 $a^r = a^8(a^d)^{-q} = 1$，由 d 的最小性得 $r = 0$）。所以 $d \in \{1, 2, 4, 8\}$。若 d 為 1、2 或 4，則 $a^4 = 1$，與 $a^4 = -1$ 矛盾。因此 $x^4 + 1$ 的每個根都是本原 8 次單位根。

反過來，設 $\omega = e^{\pi i/4}$，則 ω^k 的階為 8 當且僅當 k 為奇數（若 k 為偶數，則 $(\omega^k)^4 = 1$），所以本原 8 次單位根恰好有四個：$\omega, \omega^3, \omega^5, \omega^7$。四次多項式 $x^4 + 1$ 有四個互不相同的根（即 $e^{(2j+1)\pi i/4}$，$j = 0, 1, 2, 3$），全部都是本原 8 次單位根，所以它們正正就是這四個根。因此 $C_8(x) = x^4 + 1$。

其他 n 均不成立：C_n 的根的階全部是 n，而 $x^4 + 1$ 的根的階是 8。所以答案是 $n = 8$。

第 (iii) 部分

第 (i) 部分中用於 $n = 3$ 及 $n = 5$ 的論證，適用於任何質數 p：除 1 以外的每個 p 次單位根都是本原的。因此

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

（當 $p = 2$ 時，此式給出 $x + 1$，與第 (i) 部分一致。）

第 (iv) 部分

用反證法（proof by contradiction），假設對某些正整數 q, r, s，有 $\mathrm{C}_q(x) \equiv \mathrm{C}_r(x)\mathrm{C}_s(x)$。

首先，C_s 至少有一個根，因為 $\mathrm{e}^{2\pi\mathrm{i}/s}$ 是本原 s 次單位根：$(\mathrm{e}^{2\pi\mathrm{i}/s})^m = \mathrm{e}^{2\pi\mathrm{i}m/s} = 1$ 只在 $s \mid m$ 時成立。C_r 亦同理。所以 C_r 和 C_s 的次數（degree）都至少為 1。

取 C_r 的任一根 a。由恆等式，$\mathrm{C}_q(a) = \mathrm{C}_r(a)\mathrm{C}_s(a) = 0$，所以 a 既是本原 q 次單位根，也是本原 r 次單位根。

> **想一想** 同一個數能否在 $r \neq q$ 的情況下，既是本原 r 次單位根，又是本原 q 次單位根？

不能。假如 $r < q$，則 $a^r = 1$ 且 $0 < r < q$，這與 a 是本原 q 次單位根矛盾。若 $q < r$，則把兩者的角色對調即可。所以 $r = q$；同理（利用 C_s 的一個根）可得 $s = q$。

但這樣一來，恆等式就變成 $\mathrm{C}_q = \mathrm{C}_q^2$。比較次數，得 $\deg \mathrm{C}_q = 2 \deg \mathrm{C}_q$，所以 $\deg \mathrm{C}_q = 0$，與 C_q 有根這一事實矛盾。（另一做法：C_q^2 有重根，而 C_q 沒有。）因此不存在這樣的 q、r、s。

驗算

- C_n 的次數等於在 $1 \le k \le n$ 中滿足 $\gcd(k, n) = 1$ 的 k 的個數：當 $n = 1, \ldots, 6$ 時，次數為 $1, 1, 2, 2, 4, 2$；當 $n = 8$ 時為 4，全部吻合。
- 每個 n 次單位根都有某個整除 n 的階 d，所以 $x^n - 1$ 等於 C_d 對 n 的所有因數 d 之積。當 $n = 4$：$(x-1)(x+1)(x^2+1) = x^4 - 1$；當 $n = 8$：$(x^4-1)(x^4+1) = x^8 - 1$。
- 以數值方法，對 $n \le 40$ 把各本原根的 $(x - a)$ 相乘，可重現上述每一個多項式，只有在 $n = 8$ 時得到 $x^4 + 1$，並且在 $q, r, s \le 30$ 的範圍內找不到任何恆等式 $\mathrm{C}_q = \mathrm{C}_r\mathrm{C}_s$。

常見錯誤

- 把 1（或 -1）算作本原根：C_n 並不是 $x^n - 1$。

- 在第 (ii) 部分，只驗證 x^4+1 整除 x^8-1，卻沒有排除較小的階：重點在於 $a^4 = -1 \neq 1$。
- 在第 (iv) 部分，單憑次數論證：$\deg C_q = \deg C_r + \deg C_s$ 是可能成立的（例如 $4 = 2+2$），所以導出矛盾的是根，而不是次數。

STEP 之外

這些 C_n 就是分圓多項式（cyclotomic polynomials）。恆等式 $x^n - 1 = \prod_{d|n} C_d(x)$ 說明它們的係數必定是整數；而一個更深入的定理指出，每個分圓多項式在有理數上都是不可約（irreducible）的。它們在伽羅瓦理論（Galois theory）中佔核心地位，亦是高斯（Gauss）發現哪些正多邊形可以用尺規作圖（ruler and compass construction）作出的關鍵。Allenby 的 *Rings, Fields and Groups*（《環、域與羣》）發展了這方面的代數，而 Needham 的 *Visual Complex Analysis*（《可視化複分析》）則為單位根提供了幾何圖像。

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。