详细解答

# STEP III 2010，第 3 题

纯数学 · 单位根

> **STEP III 2010，第 3 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/10-s3-q3

本题在 *Beyond STEP* 第 6.1 节以单位根为根的多项式中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch06/cyclotomic.html

## 关键思路

每个单位根 $a$ 都有唯一的阶（order）：即使 $a^m = 1$ 成立的最小正整数 $m$。所谓本原 $n$ 次单位根（primitive $n$th root of unity），就是阶恰好为 $n$ 的单位根。因此，要求 $\mathrm{C}_n(x)$，我们先列出所有 $n$ 次单位根 $\mathrm{e}^{2\pi \mathrm{i}k/n}$，剔除那些在较低次幂时已经回到 1 的根，再把余下的 $(x-a)$ 全部相乘。而每个数只有一个阶这一事实，也正是解决最后一部分的关键。

## 解答

以下各部分中，$n$ 次单位根为 $\omega^k$，其中 $k = 0, 1, \ldots, n-1$，$\omega = \mathrm{e}^{2\pi \mathrm{i}/n}$；并且 $(\omega^k)^m = 1$ 当且仅当 $n$ 整除 $km$。由于 $\mathrm{C}_n$ 是首一（monic）多项式，没有重根，而且其根恰好是所有本原 $n$ 次单位根，故

$$\mathrm{C}_n(x) = \prod_{a \text{ 为本原单位根}} (x-a).$$

### 4 次单位根

4 次单位根为 $1, \mathrm{i}, -1, -\mathrm{i}$。由于 $1^1 = 1$ 及 $(-1)^2 = 1$，这两个根都不是本原的。但 $\mathrm{i}^1 = \mathrm{i}$、$\mathrm{i}^2 = -1$、$\mathrm{i}^3 = -\mathrm{i}$，全部不等于 1；$-\mathrm{i}$ 的情况亦相同（它的各次幂是前者的共轭（conjugate））。所以本原 4 次单位根为 $\mathrm{i}$ 和 $-\mathrm{i}$，从而

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

与题目所求相符。

**第 (i) 部分**

$n = 1$。唯一的 1 次单位根是 1，而不存在满足 $0 < m < 1$ 的 $m$，所以 1 是本原的：$C_1(x) = x - 1$。

$n = 2$。2 次单位根为 $\pm 1$；由于 $1^1 = 1$，1 被剔除，而 $(-1)^1 \neq 1$。所以 $C_2(x) = x + 1$。

$n = 3$ **及** $n = 5$。当 $n$ 为质数（prime）时，对于满足 $1 \leq k \leq n-1$ 的根 $\omega^k$，$(\omega^k)^m = 1$ 只在 $n \mid km$ 时成立；又因 $n$ 是质数且不整除 $k$，这迫使 $n \mid m$。所以除 1 以外的每个 $n$ 次单位根都是本原的。它们正是

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

的根，而这个多项式是首一的，且各根互不相同。因此

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

$n = 6$。设 $\omega = e^{\pi i/3}$，则 $\omega^k$ 的阶为 $6/\gcd(k,6)$。所以 $\omega^0 = 1$ 的阶为 1，$\omega^3 = -1$ 的阶为 2，$\omega^2, \omega^4$ 的阶为 3，只有 $\omega$ 和 $\omega^5 = \overline{\omega}$ 的阶为 6。两者之和为 $2\cos\frac{\pi}{3} = 1$，之积为 $|\omega|^2 = 1$，所以

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

（作为交叉验证：每个 6 次单位根的阶为 1、2、3 或 6，所以 $x^6 - 1 = C_1C_2C_3C_6$；而事实上 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = (x^3-1)(x^3+1) = x^6 - 1$。）

**第 (ii) 部分**

设 $a$ 为 $x^4 + 1 = 0$ 的任一根。则 $a^4 = -1$，所以 $a^8 = 1$。$a$ 的阶 $d$ 整除 8（写 $8 = qd + r$，其中 $0 \leq r < d$；则 $a^r = a^8(a^d)^{-q} = 1$，由 $d$ 的最小性得 $r = 0$）。所以 $d \in \{1, 2, 4, 8\}$。若 $d$ 为 1、2 或 4，则 $a^4 = 1$，与 $a^4 = -1$ 矛盾。因此 $x^4 + 1$ 的每个根都是本原 8 次单位根。

反过来，设 $\omega = e^{\pi i/4}$，则 $\omega^k$ 的阶为 8 当且仅当 $k$ 为奇数（若 $k$ 为偶数，则 $(\omega^k)^4 = 1$），所以本原 8 次单位根恰好有四个：$\omega, \omega^3, \omega^5, \omega^7$。四次多项式 $x^4 + 1$ 有四个互不相同的根（即 $e^{(2j+1)\pi i/4}$，$j = 0, 1, 2, 3$），全部都是本原 8 次单位根，所以它们正正就是这四个根。因此 $C_8(x) = x^4 + 1$。

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

### 第 (iii) 部分

第 (i) 部分中用于 $n=3$ 及 $n=5$ 的论证，适用于任何质数 $p$：除 1 以外的每个 $p$ 次单位根都是本原的。因此

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

（当 $p=2$ 时，此式给出 $x+1$，与第 (i) 部分一致。）

### 第 (iv) 部分

用反证法（proof by contradiction），假设对某些正整数 $q,r,s$，有 $\mathrm{C}_q(x)\equiv\mathrm{C}_r(x)\mathrm{C}_s(x)$。

首先，$\mathrm{C}_s$ 至少有一个根，因为 $\mathrm{e}^{2\pi\mathrm{i}/s}$ 是本原 $s$ 次单位根：$(\mathrm{e}^{2\pi\mathrm{i}/s})^m=\mathrm{e}^{2\pi\mathrm{i}m/s}=1$ 只在 $s\mid m$ 时成立。$\mathrm{C}_r$ 亦同理。所以 $\mathrm{C}_r$ 和 $\mathrm{C}_s$ 的次数（degree）都至少为 1。

取 $\mathrm{C}_r$ 的任一根 $a$。由恒等式，$\mathrm{C}_q(a)=\mathrm{C}_r(a)\mathrm{C}_s(a)=0$，所以 $a$ 既是本原 $q$ 次单位根，也是本原 $r$ 次单位根。

> ? **想一想** 同一个数能否在 $r\neq q$ 的情况下，既是本原 $r$ 次单位根，又是本原 $q$ 次单位根?

不能。假如 $r<q$，则 $a^r=1$ 且 $0<r<q$，这与 $a$ 是本原 $q$ 次单位根矛盾。若 $q<r$，则把两者的角色对调即可。所以 $r=q$；同理（利用 $\mathrm{C}_s$ 的一个根）可得 $s=q$。

但这样一来，恒等式就变成 $\mathrm{C}_q=\mathrm{C}_q^2$。比较次数，得 $\deg\mathrm{C}_q=2\deg\mathrm{C}_q$，所以 $\deg\mathrm{C}_q=0$，与 $\mathrm{C}_q$ 有根这一事实矛盾。（另一做法：$\mathrm{C}_q^2$ 有重根，而 $\mathrm{C}_q$ 没有。）因此不存在这样的 $q$、$r$、$s$。

## 验算

- $\mathrm{C}_n$ 的次数等于在 $1\le k\le n$ 中满足 $\gcd(k,n)=1$ 的 $k$ 的个数：当 $n=1,\ldots,6$ 时，次数为 $1,1,2,2,4,2$；当 $n=8$ 时为 4，全部吻合。
- 每个 $n$ 次单位根都有某个整除 $n$ 的阶 $d$，所以 $x^n-1$ 等于 $\mathrm{C}_d$ 对 $n$ 的所有因数 $d$ 之积。当 $n=4$：$(x-1)(x+1)(x^2+1)=x^4-1$；当 $n=8$：$(x^4-1)(x^4+1)=x^8-1$。
- 以数值方法，对 $n\le 40$ 把各本原根的 $(x-a)$ 相乘，可重现上述每一个多项式，只有在 $n=8$ 时得到 $x^4+1$，并且在 $q,r,s\le 30$ 的范围内找不到任何恒等式 $\mathrm{C}_q=\mathrm{C}_r\mathrm{C}_s$。

## 常见错误

- 把 1（或 $-1$）算作本原根：$\mathrm{C}_n$ 并不是 $x^n-1$。

- 在第 (ii) 部分，只验证 $x^4+1$ 整除 $x^8-1$，却没有排除较小的阶：重点在于 $a^4=-1\neq 1$。
- 在第 (iv) 部分，单凭次数论证：$\deg \mathrm{C}_q=\deg \mathrm{C}_r+\deg \mathrm{C}_s$ 是可能成立的（例如 $4=2+2$），所以导出矛盾的是根，而不是次数。

## STEP 之外

这些 $\mathrm{C}_n$ 就是分圆多项式（cyclotomic polynomials）。恒等式 $x^n-1=\prod_{d\mid n}\mathrm{C}_d(x)$ 说明它们的系数必定是整数；而一个更深入的定理指出，每个分圆多项式在有理数上都是不可约（irreducible）的。它们在伽罗瓦理论（Galois theory）中占核心地位，亦是高斯（Gauss）发现哪些正多边形可以用尺规作图（ruler and compass construction）作出的关键。Allenby 的 *Rings, Fields and Groups*（《环、域与群》）发展了这方面的代数，而 Needham 的 *Visual Complex Analysis*（《可视化复分析》）则为单位根提供了几何图像。

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。