詳細解答

# STEP I 1990，第 2 題

純數學 • 單位根篩選法

> **STEP I 1990，第 2 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/90-s1-q2

本題在 *Beyond STEP* 第 5.2 節單位根篩選法中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch05/roots-filter.html

## 關鍵思路

單位立方根（cube roots of unity）在這裏起着篩選器的作用。當我們用二項式定理（binomial theorem）展開 $(1+\omega^r)^n$，再把 $r=1,2,3$ 的結果相加時，每個二項式係數 $\binom{n}{j}$ 都會乘上 $1+\omega^j+\omega^{2j}$；當 3 整除 $j$ 時這個數是 3，否則是 0。因此這個和剛好只保留我們想要的係數。計算每個 $(1+\omega^r)^n$ 的另一個方法，是把 $1+\omega^r$ 寫成模—輻角形式（modulus–argument form），再用棣美弗定理（de Moivre's theorem）。

## 解答

### 單位立方根

由於 $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$，我們有 $\omega^3=\mathrm{e}^{2\pi\mathrm{i}}=1$，但 $\omega\neq 1$。於是

$$0=\omega^3-1=(\omega-1)(1+\omega+\omega^2),$$

而因為 $\omega-1\neq 0$，可以把它約去，得到 $1+\omega+\omega^2=0$。

由此可知 $1+\omega^2=-\omega$。乘以 $-1=\mathrm{e}^{-\mathrm{i}\pi}$ 相當於旋轉 $-\pi$，所以

$$1+\omega^2=\mathrm{e}^{-\mathrm{i}\pi}\,\mathrm{e}^{2\pi\mathrm{i}/3}=\mathrm{e}^{-\mathrm{i}\pi/3}.$$

因此 $1+\omega^2$ 的模是 1，輻角是 $-\frac{\pi}{3}$。（驗算一下：$1+\omega^2=1+\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}\right)=\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$。）同理，$1+\omega=-\omega^2=\mathrm{e}^{\mathrm{i}\pi/3}$，即它的共軛複數（complex conjugate）。

### 恆等式

*方法一：二項式定理。*對 $r = 1, 2, 3$，

$$(1+\omega^r)^n = \sum_{j=0}^{n} \binom{n}{j} \omega^{rj}.$$

把三種情況相加，

$$(1+\omega)^n + (1+\omega^2)^n + (1+\omega^3)^n = \sum_{j=0}^{n} \binom{n}{j} \left(\omega^j + \omega^{2j} + \omega^{3j}\right).$$

> **想一想** 對一般的整數 $j$，$\omega^j + \omega^{2j} + \omega^{3j}$ 等於甚麼？

由於 $\omega^{3j} = 1$，括號內的式子就是 $1 + \omega^j + \omega^{2j}$；又因為 $\omega^3 = 1$，它只取決於 $j$ 模 3 的值。

- 若 $j$ 是 3 的倍數，則 $\omega^j = 1$，括號內的值是 $1 + 1 + 1 = 3$。
- 若 $j \equiv 1 \pmod 3$，則 $\omega^j = \omega$ 及 $\omega^{2j} = \omega^2$，所以括號內的值是 $1 + \omega + \omega^2 = 0$。
- 若 $j \equiv 2 \pmod 3$，則 $\omega^j = \omega^2$ 及 $\omega^{2j} = \omega^4 = \omega$，所以括號內的值同樣是 0。

因此只有 $3 \mid j$ 的項留下來，而

$$(1+\omega)^n + (1+\omega^2)^n + (1+\omega^3)^n = 3\left[\binom{n}{0} + \binom{n}{3} + \cdots + \binom{n}{k}\right],$$

其中 $k$ 是不超過 $n$ 的最大的 3 的倍數。

*方法二：模與輻角。*由第一部分，$1 + \omega = \mathrm{e}^{\mathrm{i}\pi/3}$ 及 $1 + \omega^2 = \mathrm{e}^{-\mathrm{i}\pi/3}$，而 $1 + \omega^3 = 2$。根據棣美弗定理，

$$\begin{aligned}(1+\omega)^n + (1+\omega^2)^n + (1+\omega^3)^n &= \mathrm{e}^{\mathrm{i}n\pi/3} + \mathrm{e}^{-\mathrm{i}n\pi/3} + 2^n \\ &= 2^n + 2\cos\left(\frac{n\pi}{3}\right).\end{aligned}$$

比較兩種算法的結果，再除以 3，

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots + \binom{n}{k} = \frac{1}{3}\left(2^n + 2\cos\left(\frac{n\pi}{3}\right)\right),$$

這就是所要證明的結果。

### $n = 25$ 的情況

不超過 25 的最大的 3 的倍數是 24，所以第一個和正正就是恆等式取 $n = 25$ 的情況。現在 $\frac{25\pi}{3} = 8\pi + \frac{\pi}{3}$，所以 $\cos\frac{25\pi}{3} = \cos\frac{\pi}{3} = \frac{1}{2}$，而

$$\binom{25}{0} + \binom{25}{3} + \cdots + \binom{25}{24} = \frac{1}{3}\left(2^{25} + 1\right) = \frac{33554433}{3} = 11184811.$$

### 第二個和

這裏 $n = 24$，而我們要的是 $j \equiv 2 \pmod 3$ 的係數 $\binom{24}{j}$。把所有係數 $\binom{24}{j}$ 按 $j$ 除以 3 的餘數分組：

$$S_0 + S_1 + S_2 = \sum_{j=0}^{24} \binom{24}{j} = 2^{24},$$

其中 $S_m$ 是所有 $j \equiv m \pmod 3$ 的 $\binom{24}{j}$ 之和。

對稱性 $\binom{24}{j} = \binom{24}{24-j}$ 把這些項配成對：若 $j \equiv 2$，則 $24 - j \equiv -2 \equiv 1 \pmod 3$，因為 24 是 3 的倍數。所以 $j \mapsto 24 - j$ 把 $S_2$ 的各項與 $S_1$ 的各項一一對應，於是 $S_1 = S_2$。

取 $n = 24$ 的恆等式可給出 $S_0$：由於 $\cos 8\pi = 1$，

$$S_0 = \frac{1}{3}\left(2^{24} + 2\right).$$

因此

$$S_2 = \frac{1}{2}\left(2^{24} - S_0\right) = \frac{1}{2} \cdot \frac{2 \cdot 2^{24} - 2}{3} = \frac{2^{24} - 1}{3}.$$

把題目給出的數值減半，得 $2^{24} = 16777216$，所以

$$\binom{24}{2} + \binom{24}{5} + \cdots + \binom{24}{23} = \frac{16777215}{3} = 5592405.$$

## 驗算

- 小數值的情況：當 $n = 3$ 時，左邊是 $1 + 1 = 2$，右邊是 $\frac{1}{3}(8 + 2\cos\pi) = 2$；當 $n = 4$ 時，左邊是 $1 + 4 = 5$，右邊是 $\frac{1}{3}\left(16 + 2\cos\frac{4\pi}{3}\right) = \frac{1}{3}(16 - 1) = 5$。
- 整除性：$2^{25} + 1$ 和 $2^{24} - 1$ 都必須是 3 的倍數；事實確是如此，因為 $2 \equiv -1 \pmod 3$。
- 我們用電腦直接把二項式係數相加：恆等式對 199 或以下的每個 $n$ 都成立，第一個和是 11184811，第二個和是 5592405。

## 常見錯誤

- 把 $1 + \omega^2$ 的輻角寫成 $\frac{\pi}{3}$：它位於第四象限，所以輻角主值（principal argument）是 $-\frac{\pi}{3}$（等價地，$\frac{5\pi}{3}$）。
- 忘記了 $r = 3$ 的情況，而 $2^n$ 正是由它而來。
- 在第二個和中，試圖直接套用公式：公式只給出 3 的倍數的項，所以要處理餘數為 2 的項，還需要另一個想法（這裏是對稱性）。

## STEP 之外

這個技巧稱為單位根篩選法（roots of unity filter），它是離散傅立葉變換（discrete Fourier transform）的第一個例子：把 $f(\omega^r)$ 在所有 $m$ 次單位根上取平均，就能抽出多項式 $f$ 中屬於模 $m$ 某個指定剩餘類（residue class）的係數。同樣這種在一個對稱羣上取平均的做法，會在有限羣的特徵標理論（character theory）以及伯恩賽德引理（Burnside's lemma）等計數論證中再次出現。想進一步了解為何複數令這類計算變得如此自然，可參閱 Needham 的 *Visual Complex Analysis*（《複分析：可視化方法》）。

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。