详细解答

STEP I 1990，第 2 题

纯数学 · 单位根筛选法

> **STEP I 1990，第 2 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/90-s1-q2

本题在 *Beyond STEP* 第 5.2 节单位根筛选法中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch05/roots-filter.html

关键思路

单位立方根（cube roots of unity）在这里起着筛选器的作用。当我们用二项式定理（binomial theorem）展开 $(1+\omega^r)^n$，再把 $r=1,2,3$ 的结果相加时，每个二项式系数 $\binom{n}{j}$ 都会乘上 $1+\omega^j+\omega^{2j}$；当 3 整除 j 时这个数是 3，否则是 0。因此这个和刚好只保留我们想要的系数。计算每个 $(1+\omega^r)^n$ 的另一个方法，是把 $1+\omega^r$ 写成模—辐角形式（modulus–argument form），再用棣美弗定理（de Moivre's theorem）。

解答

单位立方根

由于 $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$，我们有 $\omega^3=\mathrm{e}^{2\pi\mathrm{i}}=1$，但 $\omega\neq 1$。于是

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

而因为 $\omega-1\neq 0$，可以把它约去，得到 $1+\omega+\omega^2=0$。

由此可知 $1+\omega^2=-\omega$。乘以 $-1=\mathrm{e}^{-\mathrm{i}\pi}$ 相当于旋转 $-\pi$，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，辐角是 $-\frac{\pi}{3}$。（验算一下：$1+\omega^2=1+\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}\right)=\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$。）同理，$1+\omega=-\omega^2=\mathrm{e}^{\mathrm{i}\pi/3}$，即它的共轭复数（complex conjugate）。

恒等式

*方法一：二项式定理。*对 $r = 1, 2, 3$，

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

把三种情况相加，

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

> **想一想** 对一般的整数 j，$\omega^j + \omega^{2j} + \omega^{3j}$ 等于甚么？

由于 $\omega^{3j} = 1$，括号内的式子就是 $1 + \omega^j + \omega^{2j}$；又因为 $\omega^3 = 1$，它只取决于 j 模 3 的值。

- 若 j 是 3 的倍数，则 $\omega^j = 1$，括号内的值是 $1 + 1 + 1 = 3$。
- 若 $j \equiv 1 \pmod 3$，则 $\omega^j = \omega$ 及 $\omega^{2j} = \omega^2$，所以括号内的值是 $1 + \omega + \omega^2 = 0$。
- 若 $j \equiv 2 \pmod 3$，则 $\omega^j = \omega^2$ 及 $\omega^{2j} = \omega^4 = \omega$，所以括号内的值同样是 0。

因此只有 $3 \mid j$ 的项留下来，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 是不超过 n 的最大的 3 的倍数。

*方法二：模与辐角。*由第一部分，$1 + \omega = \mathrm{e}^{\mathrm{i}\pi/3}$ 及 $1 + \omega^2 = \mathrm{e}^{-\mathrm{i}\pi/3}$，而 $1 + \omega^3 = 2$。根据棣美弗定理，

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

比较两种算法的结果，再除以 3，

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

这就是所要证明的结果。

$n = 25$ 的情况

不超过 25 的最大的 3 的倍数是 24，所以第一个和正正就是恒等式取 $n = 25$ 的情况。现在 $\frac{25\pi}{3} = 8\pi + \frac{\pi}{3}$，所以 $\cos\frac{25\pi}{3} = \cos\frac{\pi}{3} = \frac{1}{2}$，而

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

第二个和

这里 $n=24$，而我们要的是 $j\equiv 2 \pmod 3$ 的系数 $\binom{24}{j}$。把所有系数 $\binom{24}{j}$ 按 j 除以 3 的余数分组：

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

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

对称性 $\binom{24}{j}=\binom{24}{24-j}$ 把这些项配成对：若 $j\equiv 2$，则 $24-j\equiv -2\equiv 1 \pmod 3$，因为 24 是 3 的倍数。所以 $j\mapsto 24-j$ 把 S_2 的各项与 S_1 的各项一一对应，于是 $S_1=S_2$。

取 $n=24$ 的恒等式可给出 S_0：由于 $\cos 8\pi=1$，

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

因此

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

把题目给出的数值减半，得 $2^{24}=16777216$，所以

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

验算

- 小数值的情况：当 $n=3$ 时，左边是 $1+1=2$，右边是 $\frac{1}{3}(8+2\cos\pi)=2$；当 $n=4$ 时，左边是 $1+4=5$，右边是 $\frac{1}{3}\left(16+2\cos\frac{4\pi}{3}\right)=\frac{1}{3}(16-1)=5$。
- 整除性：$2^{25}+1$ 和 $2^{24}-1$ 都必须是 3 的倍数；事实确是如此，因为 $2\equiv -1 \pmod 3$。
- 我们用电脑直接把二项式系数相加：恒等式对 199 或以下的每个 n 都成立，第一个和是 11184811，第二个和是 5592405。

常见错误

- 把 $1+\omega^2$ 的辐角写成 $\frac{\pi}{3}$：它位于第四象限，所以辐角主值（principal argument）是 $-\frac{\pi}{3}$（等价地，$\frac{5\pi}{3}$）。
- 忘记了 $r=3$ 的情况，而 2^n 正是由它而来。
- 在第二个和中，试图直接套用公式：公式只给出 3 的倍数的项，所以要处理余数为 2 的项，还需要另一个想法（这里是对称性）。

STEP 之外

这个技巧称为单位根筛选法（roots of unity filter），它是离散傅里叶变换（discrete Fourier transform）的第一个例子：把 $f(\omega^r)$ 在所有 m 次单位根上取平均，就能抽出多项式 f 中属于模 m 某个指定剩余类（residue class）的系数。同样这种在一个对称群上取平均的做法，会在有限群的特征标理论（character theory）以及伯恩赛德引理（Burnside's lemma）等计数论证中再次出现。想进一步了解为何复数令这类计算变得如此自然，可参阅 Needham 的 *Visual Complex Analysis*（《复分析：可视化方法》）。

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。