详细解答

STEP I 1996，第 3 题

纯数学 · 整数的整除性

> **STEP I 1996，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/96-s1-q3

关键思路

要处理被合成数（composite number）如 24 整除（divisibility）的问题，最简单的做法是逐个质数幂（prime power）处理：$24 = 3 \times 8$，而 3 与 8 互质（coprime），所以我们分别证明可被 3 整除和可被 8 整除。因式分解（factorise）之后会得到连续整数之积，而任意 k 个连续整数之中，必有一个是 k 的倍数。其余两部分也可用同一习惯解决：因式分解，或者把 n 写成能显示其余数的形式。

解答

第 (i) 部分

抽出公因式，再运用平方差公式（difference of two squares），

$$n^5 - n^3 = n^3(n^2 - 1) = n^3(n-1)(n+1) = n^2\,(n-1)\,n\,(n+1).$$

可被 3 整除。$n-1$、n、$n+1$ 是三个连续整数，所以其中恰好有一个是 3 的倍数。因此 $3 \mid (n-1)n(n+1)$，从而 $3 \mid n^5 - n^3$。

可被 8 整除。我们按 n 的奇偶性（parity）分情况讨论。

- 若 n 是偶数，设 $n = 2m$，则 $n^3 = 8m^3$，是 8 的倍数。
- 若 n 是奇数，则 $n-1$ 和 $n+1$ 是连续偶数。任意两个连续偶数之中，一个是 4 的倍数，另一个是 2 的倍数，所以 $8 \mid (n-1)(n+1)$。

无论哪种情况，都有 $8 \mid n^3(n-1)(n+1) = n^5 - n^3$。

想一想 为甚么知道 $3 \mid N$ 和 $8 \mid N$ 就可以推出 $24 \mid N$？换成 $4 \mid N$ 和 $6 \mid N$，结论还成立吗？

由于 3 和 8 没有公因数，$8 \mid N$ 表示 $N = 8a$，于是 $3 \mid 8a$ 迫使 $3 \mid a$（因为 3 是质数，而且不整除 8）。所以 $N = 24b$。这个论证对 4 和 6 并不成立，因为两者有公因数 2：12 可同时被两者整除，却不能被 24 整除。

因此，对每个正整数 n，$n^5 - n^3$ 都可被 24 整除，证毕。

第 (ii) 部分

写成 $2^{2n} = 4^n$。运用因式分解 $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$，取 $x = 4$，

$$2^{2n} - 1 = 4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right) = 3\left(4^{n-1} + \cdots + 1\right).$$

括号内是整数，所以 $2^{2n} - 1$ 可被 3 整除。

用模算术（modular arithmetic）来说，这等价于：$4 \equiv 1 \pmod 3$，所以 $4^n \equiv 1^n = 1 \pmod 3$。用归纳法(induction)证明也可以：若 $4^k - 1 = 3a$，则 $4^{k+1} - 1 = 4(4^k - 1) + 3 = 3(4a + 1)$。

第 (iii) 部分

由于 $3 \mid n - 1$，可写 $n = 3k + 1$，其中 $k \geq 0$ 为某个整数。因式分解得

$$n^3 - 1 = (n-1)(n^2 + n + 1).$$

第一个因式是 $n - 1 = 3k$。至于第二个，

$$\begin{aligned} n^2 + n + 1 &= (9k^2 + 6k + 1) + (3k + 1) + 1 \\ &= 9k^2 + 9k + 3 \\ &= 3(3k^2 + 3k + 1). \end{aligned}$$

所以每个因式各提供一个 3：

$$n^3 - 1 = 3k \cdot 3(3k^2 + 3k + 1) = 9k(3k^2 + 3k + 1),$$

它可被 9 整除，证毕。（当 $n = 1$ 时，$k = 0$，$n^3 - 1 = 0$，同样可被 9 整除。）

重点在于 $n - 1$ 只提供一个因数 3；第二个来自 $n^2 + n + 1$。要看出这第二个因数，有一个巧妙的方法：$n^2 + n + 1 = (n-1)^2 + 3n$，只要 $3 \mid n - 1$，这就是两个 3 的倍数之和。

验算

- 第 (i) 部分：$n = 2$ 给出 $32 - 8 = 24$，$n = 3$ 给出 $243 - 27 = 216 = 9 \times 24$。由于 $n = 2$ 时刚好得到 24，没有更大的数能整除每一个 $n^5 - n^3$，所以 24 已是最佳结果。
- 第 (ii) 部分：$n = 1, 2, 3$ 分别给出 3、15、63。
- 第 (iii) 部分：$n = 4$ 给出 $63 = 7 \times 9$，$n = 7$ 给出 $342 = 38 \times 9$，与 $9k(3k^2 + 3k + 1)$ 在 $k = 1$ 和 $k = 2$ 时的值吻合。

我们用电脑对所有小于 5000 的 n 验证了全部三个结果（第 (ii) 部分则验证了 $n < 2000$），并确认 $n^5 - n^3$ 各个值的最大公因数（highest common factor）恰好是 24。

常见错误

- 论证时写“$(n-1)n(n+1)$ 可被 6 整除，而 n^2 是 ...”，结果弄不清因数 8 从何而来。偶数的情况需要用到 n^3，而不只是 n。
- 由可被 4 整除和可被 6 整除推断可被 24 整除；两个因数必须互质。
- 在第 (iii) 部分，写到“$n - 1$ 可被 3 整除，所以 $n^3 - 1 = (n-1)(\dots)$ 可被 3 整除”便停下来，这样只得到一个因数 3。

STEP 之外

这三部分其实都是模算术中的命题：模 m 的整数构成一个环（ring），而第 (iii) 部分说的是：若 $n \equiv 1 \pmod 3$，则 $n^3 \equiv 1 \pmod 9$。这是一个称为指数提升（*lifting the exponent*）的一般现象的第一步：若 $p \mid n - 1$，则 $p^{j+1} \mid n^{p^j} - 1$。费马小定理（Fermat's little theorem, $n^p \equiv n \pmod p$）也能解释第 (i) 部分，因为它直接给出 $3 \mid n^3 - n$。Davenport 的 *The Higher Arithmetic*（一本讲高等算术的数论入门书）是这些思想的一本优美入门读物。

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。