详细解答

STEP II 2005，第 2 题

纯数学 · 欧拉 φ 函数

> **STEP II 2005，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/05-s2-q2

关键思路

一切都源于把 N 写成质因数分解（prime factorisation）的形式。每个因子 $(1-\frac{1}{p})=\frac{p-1}{p}$ 的分母都有一个 p，而 N 必定含有至少一个 p 可以把它约去。一旦把 $\mathrm{f}(N)$ 写成各质数幂（prime power）的乘积，便能清楚看出 $\mathrm{f}(m)\mathrm{f}(n)$ 与 $\mathrm{f}(mn)$ 何时相等：关键在于 m 与 n 有没有公共的质因数。

解答

第 (i) 部分

(a) 整除 $12=2^2\cdot 3$ 的质数是 2 和 3，所以

$$\mathrm{f}(12)=12\Big(1-\frac{1}{2}\Big)\Big(1-\frac{1}{3}\Big)=12\cdot\frac{1}{2}\cdot\frac{2}{3}=4.$$

整除 $180=2^2\cdot 3^2\cdot 5$ 的质数是 2、3 和 5，所以

$$\mathrm{f}(180)=180\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=48.$$

(b) 当 $N=1$ 时没有质因数，乘积是空积（empty product），故 $\mathrm{f}(1)=1$。当 $N\geq 2$ 时，写

$$N=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},$$

其中 p_i 是整除 N 的相异质数，而每个 $a_i\geq 1$。于是

$$\begin{aligned}\mathrm{f}(N)&=p_1^{a_1}\cdots p_k^{a_k}\cdot\frac{p_1-1}{p_1}\cdots\frac{p_k-1}{p_k}\\&=p_1^{a_1-1}(p_1-1)\,p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1).\end{aligned}$$

由于每个 $a_i \geq 1$，每个指数 $a_i - 1$ 都是非负整数，所以每个因子 $p_i^{a_i-1}(p_i - 1)$ 都是正整数。因此对所有 N，$\mathrm{f}(N)$ 都是整数。本题余下部分都会用到这条公式：

$$\mathrm{f}(N) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1), \qquad (*)$$

第 (ii) 部分

(a) 这是错的。取 $m = n = 2$，则 $\mathrm{f}(2) = 2 \cdot \frac{1}{2} = 1$，所以 $\mathrm{f}(2)\mathrm{f}(2) = 1$，但 $\mathrm{f}(4) = 4 \cdot \frac{1}{2} = 2$。问题在于因子 $(1 - \frac{1}{2})$ 在左边出现了两次，在右边却只出现一次，因为 2 作为 4 的质因数只计算一次。

(b) 这是对的。若 p 和 q 是相异质数，则 $\mathrm{f}(p) = p(1 - \frac{1}{p}) = p - 1$，同理 $\mathrm{f}(q) = q - 1$。整除 pq 的质数恰好是 p 和 q，而且两者不同，所以

$$\mathrm{f}(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1) = \mathrm{f}(p)\mathrm{f}(q).$$

(c) 这个命题是说：$\mathrm{f}(p)\mathrm{f}(q) = \mathrm{f}(pq)$ 只有在 p 和 q 是相异质数时才可能成立；换言之，这条等式迫使 p 和 q 必须是相异质数。这是错的。取 $p = 3$ 和 $q = 4$；等式要有意义，两者都不必是质数。于是

$$\mathrm{f}(3)\mathrm{f}(4) = 2 \cdot 2 = 4 = \mathrm{f}(12),$$

这里用了第 (i)(a) 部分的结果，但 4 不是质数。（更简单的例子是 $p = 1$，因为对任何 q 都有 $\mathrm{f}(1)\mathrm{f}(q) = \mathrm{f}(q)$。）

> ? **想一想** 如果不是质数这个性质，那么真正令等式成立的是甚么？

真正重要的是 p 和 q 没有公共的质因数。若 $\gcd(m, n) = 1$，则 m 与 n 各自所含的质数幂互不相同，所以 mn 的分解式不过是把两个分解式并排写在一起，而由 $(*)$ 可得 $\mathrm{f}(mn) = \mathrm{f}(m)\mathrm{f}(n)$。若有某个质数 r 同时整除两者，则因子 $(1 - \frac{1}{r})$ 在 $\mathrm{f}(m)\mathrm{f}(n)$ 中出现两次，在 $\mathrm{f}(mn)$ 中却只出现一次，所以 $\mathrm{f}(m)\mathrm{f}(n) < \mathrm{f}(mn)$。因此等式恰好在 $\gcd(m, n) = 1$ 时成立，而 3、4 只是其中一对互质（coprime）但并非两个都是质数的数。

假如你把第 (ii) 部分中的 p 和 q 一律理解为质数，那么 (c) 问的只是 $p = q$ 的情况会否出现，而答案是不会：$\mathrm{f}(p)^2 = (p-1)^2$，而 $\mathrm{f}(p^2) = p(p-1)$，由于 $p - 1 \neq p$，两者永不相等。在这种理解下，(c) 是对的。不过，配合上面反例（counterexample）的一般理解，才是较自然的读法。

第 (iii) 部分

由 $(*)$，质数幂满足

$$\mathrm{f}(p^m) = p^{m-1}(p - 1).$$

把目标数值分解，得 $146410 = 10 \times 14641 = 2 \cdot 5 \cdot 11^4$，因为 $14641 = 121^2 = 11^4$。这已经是 $p^{m-1}(p-1)$ 的形式，其中 $p = 11$：$11^4 \cdot 10 = 11^4(11-1)$，所以 $m - 1 = 4$。因此

$$p = 11, \quad m = 5: \qquad \mathrm{f}(11^5) = 11^4 \cdot 10 = 146410.$$

事实上这是唯一的答案。若 $m \geq 2$，则 p 整除 146410，所以 $p \in \{2, 5, 11\}$。取 $p = 2$ 会得到 $2^{m-1} = 146410$，这不可能，因为 146410 有奇质因数。取 $p = 5$ 会得到 $4 \cdot 5^{m-1} = 146410$，这也不可能，因为 146410 不能被 4 整除。余下只有 $p = 11$，由此得 $m = 5$。若 $m = 1$，则需要 $p = 146411$ 是质数，但 $146411 = 41 \times 3571$。

验算

- 这个函数就是欧拉函数（Euler's totient）：$\mathrm{f}(N)$ 计算 $\{1, \ldots, N\}$ 中与 N 互质的整数的个数。例如当 $N = 12$ 时，这样的数有四个，就是 $1, 5, 7, 11$。经电脑验证，对每个 $N < 2000$，乘积公式都与这个个数吻合，而且结果是整数。
- 题目中的示例给出 $\mathrm{f}(80) = 80 \cdot \frac{1}{2} \cdot \frac{4}{5} = 32 = 2^3(2-1) \cdot 5^0(5-1)$，与 $(*)$ 吻合。
- 电脑测试了 20 000 对随机选取的 $m, n \leq 400$，发现 $\mathrm{f}(m)\mathrm{f}(n) = \mathrm{f}(mn)$ 恰好在 $\gcd(m, n) = 1$ 时成立。另外，搜索所有质数 $p \leq 146411$ 后，发现 $(p, m) = (11, 5)$ 是 (iii) 的唯一解。

常见错误

- 在乘积中把同一个质数计算多于一次：对 $180 = 2^2 \cdot 3^2 \cdot 5$ 而言，因子有三个，不是五个。
- 把“仅当”（only if）当作“若”（if）。(b) 部分是“若”的方向，而 (c) 部分是它的逆命题（converse），两者是不同的命题。
- 在 (iii) 中看不出 $14641 = 11^4$。留意到 $11^2 = 121$ 和 $121^2 = 14641$，或者认出帕斯卡三角形（Pascal's triangle）中 $1, 4, 6, 4, 1$ 这一行，便能很快找到。

STEP 之外

这个函数就是欧拉函数 φ，而第 (ii) 部分的结果说明它是积性（multiplicative）的：只要 $\gcd(m, n) = 1$，便有 $\varphi(mn) = \varphi(m)\varphi(n)$，但一般情况下则不然。它出现在欧拉定理（Euler's theorem）之中：若 a 与 n 互质，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$；这条定理推广了费马小定理（Fermat's little theorem），也是 RSA 加密法（RSA encryption）的基础。在群论

（group theory）中，$\varphi(n)$ 是模 n 单位群（group of units）的阶（order）。Davenport 的 *The Higher Arithmetic*（一本经典的数论入门书）把这一切阐述得十分精彩。

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。