詳細解答

STEP II 2005，第 2 題

純數學 • 歐拉 φ 函數

STEP II 2005，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/05-s2-q2

關鍵思路

一切都源於把 N 寫成質因數分解（prime factorisation）的形式。每個因子 $(1-\frac{1}{p})=\frac{p-1}{p}$ 的分母都有一個 p，而 N 必定含有至少一個 p 可以把它約去。一旦把 $\mathrm{f}(N)$ 寫成各質數冪（prime power）的乘積，便能清楚看出 $\mathrm{f}(m)\mathrm{f}(n)$ 與 $\mathrm{f}(mn)$ 何時相等：關鍵在於 m 與 n 有沒有公共的質因數。

解答

第 (i) 部分

(a) 整除 $12=2^2\cdot 3$ 的質數是 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 $180=2^2\cdot 3^2\cdot 5$ 的質數是 2、3 和 5，所以

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

(b) 當 $N=1$ 時沒有質因數，乘積是空積（empty product），故 $\mathrm{f}(1)=1$。當 $N\geq 2$ 時，寫

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

其中 p_i 是整除 N 的相異質數，而每個 $a_i\geq 1$。於是

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

由於每個 $a_i \geq 1$，每個指數 $a_i - 1$ 都是非負整數，所以每個因子 $p_i^{a_i-1}(p_i - 1)$ 都是正整數。因此對所有 N，$\mathrm{f}(N)$ 都是整數。本題餘下部分都會用到這條公式：

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

第 (ii) 部分

(a) 這是錯的。取 $m = n = 2$，則 $\mathrm{f}(2) = 2 \cdot \frac{1}{2} = 1$，所以 $\mathrm{f}(2)\mathrm{f}(2) = 1$，但 $\mathrm{f}(4) = 4 \cdot \frac{1}{2} = 2$。

問題在於因子 $(1 - \frac{1}{2})$ 在左邊出現了兩次，在右邊卻只出現一次，因為 2 作為 4 的質因數只計算一次。

(b) 這是對的。若 p 和 q 是相異質數，則 $\mathrm{f}(p) = p(1 - \frac{1}{p}) = p - 1$，同理 $\mathrm{f}(q) = q - 1$。整除 pq 的質數恰好是 p 和 q，而且兩者不同，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) 這個命題是說：$\mathrm{f}(p)\mathrm{f}(q) = \mathrm{f}(pq)$ 只有在 p 和 q 是相異質數時才可能成立；換言之，這條等式迫使 p 和 q 必須是相異質數。這是錯的。取 $p = 3$ 和 $q = 4$；等式要有意義，兩者都不必是質數。於是

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

這裏用了第 (i)(a) 部分的結果，但 4 不是質數。（更簡單的例子是 $p = 1$，因為對任何 q 都有 $\mathrm{f}(1)\mathrm{f}(q) = \mathrm{f}(q)$。）

> ? **想一想** 如果不是質數這個性質，那麼真正令等式成立的是甚麼？

真正重要的是 p 和 q 沒有公共的質因數。若 $\gcd(m, n) = 1$，則 m 與 n 各自所含的質數冪互不相同，所以 mn 的分解式不過是把兩個分解式並排寫在一起，而由 $(*)$ 可得 $\mathrm{f}(mn) = \mathrm{f}(m)\mathrm{f}(n)$。若有某個質數 r 同時整除兩者，則因子 $(1 - \frac{1}{r})$ 在 $\mathrm{f}(m)\mathrm{f}(n)$ 中出現兩次，在 $\mathrm{f}(mn)$ 中卻只出現一次，所以 $\mathrm{f}(m)\mathrm{f}(n) < \mathrm{f}(mn)$。因此等式恰好在 $\gcd(m, n) = 1$ 時成立，而 3、4 只是其中一對互質（coprime）但並非兩個都是質數的數。

假如你把第 (ii) 部分中的 p 和 q 一律理解為質數，那麼 (c) 問的只是 $p = q$ 的情況會否出現，而答案是不會：$\mathrm{f}(p)^2 = (p-1)^2$，而 $\mathrm{f}(p^2) = p(p-1)$，由於 $p - 1 \neq p$，兩者永不相等。在這種理解下，(c) 是對的。不過，配合上面反例（counterexample）的一般理解，才是較自然的讀法。

第 (iii) 部分

由 $(*)$，質數冪滿足

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

把目標數值分解，得 $146410 = 10 \times 14641 = 2 \cdot 5 \cdot 11^4$，因為 $14641 = 121^2 = 11^4$。這已經是 $p^{m-1}(p-1)$ 的形式，其中 $p = 11$：$11^4 \cdot 10 = 11^4(11-1)$，所以 $m - 1 = 4$。因此

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

事實上這是唯一的答案。若 $m \geq 2$，則 p 整除 146410，所以 $p \in \{2, 5, 11\}$。取 $p = 2$ 會得到 $2^{m-1} = 146410$，這不可能，因為 146410 有奇質因數。取 $p = 5$ 會得到 $4 \cdot 5^{m-1} = 146410$，這也不可能，因為 146410 不能被 4 整除。餘下只有 $p = 11$，由此得 $m = 5$。若 $m = 1$，則需要 $p = 146411$ 是質數，但 $146411 = 41 \times 3571$。

驗算

- 這個函數就是歐拉函數（Euler's totient）：$\mathrm{f}(N)$ 計算 $\{1, \ldots, N\}$ 中與 N 互質的整數的個數。例如當 $N = 12$ 時，這樣的數有四個，就是 $1, 5, 7, 11$。經電腦驗證，對每個 $N < 2000$，乘積公式都與這個個數吻合，而且結果是整數。
- 題目中的示例給出 $\mathrm{f}(80) = 80 \cdot \frac{1}{2} \cdot \frac{4}{5} = 32 = 2^3(2-1) \cdot 5^0(5-1)$，與 $(*)$ 吻合。
- 電腦測試了 20 000 對隨機選取的 $m, n \leq 400$，發現 $\mathrm{f}(m)\mathrm{f}(n) = \mathrm{f}(mn)$ 恰好在 $\gcd(m, n) = 1$ 時成立。另外，搜尋所有質數 $p \leq 146411$ 後，發現 $(p, m) = (11, 5)$ 是 (iii) 的唯一解。

常見錯誤

- 在乘積中把同一個質數計算多於一次：對 $180 = 2^2 \cdot 3^2 \cdot 5$ 而言，因子有三個，不是五個。
- 把「僅當」（only if）當作「若」（if）。(b) 部分是「若」的方向，而 (c) 部分是它的逆命題（converse），兩者是不同的命題。
- 在 (iii) 中看不出 $14641 = 11^4$。留意到 $11^2 = 121$ 和 $121^2 = 14641$，或者認出帕斯卡三角形（Pascal's triangle）中 $1, 4, 6, 4, 1$ 這一行，便能很快找到。

STEP 之外

這個函數就是歐拉函數 φ，而第 (ii) 部分的結果說明它是積性（multiplicative）的：只要 $\gcd(m,n)=1$，便有 $\varphi(mn)=\varphi(m)\varphi(n)$，但一般情況下則不然。它出現在歐拉定理（Euler's theorem）之中：若 a 與 n 互質，則 $a^{\varphi(n)}\equiv 1 \pmod{n}$；這條定理推廣了費馬小定理（Fermat's little theorem），也是 RSA 加密法（RSA encryption）的基礎。在羣論（group theory）中，$\varphi(n)$ 是模 n 單位羣（group of units）的階（order）。Davenport 的 *The Higher Arithmetic*（一本經典的數論入門書）把這一切闡述得十分精彩。

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。