详细解答

STEP II 2002，第 3 题

纯数学 · 费马数与质数

> **STEP II 2002，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/02-s2-q3

本题在 *Beyond STEP* 第 1.1 节质数工厂中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch01/fermat-numbers.html

关键思路

写出 $F_k - 2 = 2^{2^k} - 1$。把它乘以 $F_k = 2^{2^k} + 1$，便得到一个平方差（difference of two squares），而这正是归纳法（induction）所需要的那一步。乘积公式一旦成立，任何两个费马数（Fermat number）的公因数（common factor）都必须整除 2。由于每个费马数都是奇数，这个因数只可能是 1。

解答

首四个费马数

由于 $2^0 = 1$、$2^1 = 2$、$2^2 = 4$ 及 $2^3 = 8$，

$$F_0 = 2^1 + 1 = 3, \qquad F_1 = 2^2 + 1 = 5, \qquad F_2 = 2^4 + 1 = 17, \qquad F_3 = 2^8 + 1 = 257.$$

现在就 k 的首三个值验证 $(*)$：

$$\begin{aligned} k = 1: &\quad F_0 = 3 = 5 - 2 = F_1 - 2, \\ k = 2: &\quad F_0 F_1 = 15 = 17 - 2 = F_2 - 2, \\ k = 3: &\quad F_0 F_1 F_2 = 15 \times 17 = 255 = 257 - 2 = F_3 - 2. \end{aligned}$$

证明 $(*)$ 对所有 $k \geq 1$ 成立

我们对 k 使用归纳法。$k = 1$ 的情况已在上面完成。

假设 $(*)$ 对某个 $k \geq 1$ 成立，即 $F_0 F_1 \cdots F_{k-1} = F_k - 2$。那么

$$\begin{aligned} F_0 F_1 \cdots F_{k-1} F_k &= (F_k - 2)\, F_k \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) \\ &= \left(2^{2^k}\right)^2 - 1 \\ &= 2^{2 \cdot 2^k} - 1 = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2. \end{aligned}$$

所以 $(*)$ 对 $k+1$ 同样成立，根据归纳法，它对每个 $k \geq 1$ 都成立。

? **想一想** 为甚么 $\left(2^{2^k}\right)^2$ 等于 $2^{2^{k+1}}$，而不是 $2^{2^{2k}}$ 或其他式子?

把一个幂平方，指数（exponent）便会加倍：$\left(2^a\right)^2 = 2^{2a}$。这里 $a = 2^k$，而 $2a = 2 \cdot 2^k = 2^{k+1}$。归纳步骤的大部分工夫，就在于小心处理这类层层叠起的指数。

任何两个费马数都没有公因数

取两个不同的费马数 F_m 和 F_n，其中 $m < n$。那么 $n \geq 1$，而在 $k = n$ 时的 $(*)$ 中，F_m 是因数 $F_0, \ldots, F_{n-1}$ 的其中一个。所以

$$F_n - 2 = F_m \times (\text{某个整数}),$$

这表示 F_m 整除 $F_n - 2$。

现在假设正整数 d 同时整除 F_m 和 F_n。由于 $d \mid F_m$ 及 $F_m \mid F_n - 2$，我们有 $d \mid F_n - 2$。又由于 d 也整除 F_n，它便整除两者之差：

$$d \mid F_n - (F_n - 2) = 2,$$

所以 $d = 1$ 或 $d = 2$。但 $F_m = 2^{2^m} + 1$ 是一个偶数加 1，所以是奇数（注意 $2^m \geq 1$）。因此 $d \neq 2$，从而 $d = 1$。由此可见，任何两个费马数都没有大于 1 的公因数。

质数有无限多个

每个 F_n 都至少是 3，所以它至少有一个质因数（prime factor）。选取其中一个，称它为 p_n。这样，每个 $n = 0, 1, 2, \ldots$ 都对应一个质数。

? **想一想** 两个不同的费马数会不会给出同一个质数?

不会。假如 $p_m = p_n$ 而 $m \neq n$，这个质数便会同时整除 F_m 和 F_n。它就成了一个大于 1 的公因数，而上一部分已排除了这个可能。所以质数 $p_0, p_1, p_2, \ldots$ 全部互不相同。由于费马数有无限多个，互不相同的质数也有无限多个。

留意我们从来不需要 F_n 本身是质数，只需要每个费马数都有某个质因数，是其他费马数所没有的。

验算

- $k = 4$ 时的 $(*)$：$255 \times 257 = 65535 = 65537 - 2 = F_4 - 2$。我们亦用电脑以精确运算验证了 $(*)$ 对直至 12 的所有 k 都成立。
- $F_0, \ldots, F_5$ 的最小质因数分别是 $3, 5, 17, 257, 65537, 641$，全部不同，正如论证所预测。$F_5 = 4294967297 = 641 \times 6700417$ 是第一个不是质数的费马数。
- 我们以数值计算确认了对所有 $0 \leq m < n \leq 10$，都有 $\gcd(F_m, F_n) = 1$。

常见错误

- 把 2^{2^n} 读成 $(2^2)^n = 4^n$。指数是 2^n，所以 $F_3 = 2^8 + 1$，而不是 $4^3 + 1$。
- 得出 $d \mid 2$ 之后，忘记排除 $d = 2$。正是“费马数是奇数”这个事实，才令论证得以完成。
- 假设每个费马数都是质数。最后一部分不需要这个假设，而且它根本是错的（$641 \mid F_5$）。

STEP 之外

这个证明出自波利亚（Pólya）。它属于“质数有无限多个”的一系列证明之一。这类证明都是构造一个两两互质（pairwise coprime）的无穷整数数列，于是每一项都贡献一个属于自己的新质数。欧几里得（Euclid）的证明也可以这样理解。费马数在数论课程中还会再次出现：高斯（Gauss）证明了正 n 边形可以用尺规作图（ruler and compass construction），当且仅当 n 是 2 的幂乘以若干个互不相同的费马质数（Fermat prime）之积，而至今仍未发现 F_4 之后的费马质数。想了解更多，可阅读 Davenport 的 *The Higher Arithmetic*（一本经典的数论入门书）。

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。