1.1 质数工厂

工作纸

题目

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

提示

请先自行尝试解题。如果遇到困难，请逐一阅读提示，每读完一个便回到题目再试。标有“停一停，试一试”的提示是关键步骤。每个提示之后均留有空位供你演算。

> **想一想**　最后一行问的是“无穷多个质数”，中间问的是“公因数”。“任何两个费马数（Fermat number）都没有公因数”和“质数有无穷多个”之间，究竟有甚么关系？

阶段 1　感受一下这些数

涵盖：首四个费马数（Fermat numbers）

> **想一想**　留意这个指数塔（power tower）：2^{2^n} 的意思是 $2^{(2^n)}$。先就 $n = 0, 1, 2, 3$ 算出 2^n，然后才把 2 自乘至该次幂（power）。

阶段 2 验证恒等式（identity）

涵盖：$(*)$ 在 $k = 1, 2, 3$ 时的情况

想一想 当 $k = 1, 2, 3$ 时，$(*)$ 的左方分别是一个、两个和三个费马数的乘积。逐一计算这些乘积，再与 $F_k - 2$ 比较。

阶段 3　证明恒等式

涵盖：$(*)$ 对所有 $k \geq 1$ 成立

想一想　归纳法（induction）是最自然的工具。若 $(*)$ 对 k 成立，你要把两边同时乘以甚么，才能得到 $k+1$ 时的左方？

想一想　完成这一步之后，你需要证明 $(F_k - 2)\,F_k = F_{k+1} - 2$。把 $F_k - 2$ 和 F_k 分别写成 2 的幂减去或加上 1 的形式。

停一停，试一试　$(a-1)(a+1) = a^2 - 1$。取 $a = 2^{2^k}$：把 a^2 写成 2 的幂，会是甚么？

阶段 4 没有公因数（common factor）

想一想 假设 d 同时整除 F_m 和 F_n，其中 $m < n$。在 $(*)$ 中取 $k = n$。F_m 是否左方的其中一个因数?

停一停，试一试 因此 d 既整除 F_n，也整除 $F_n - 2$。那么 d 必定整除甚么？在各个可能之中，哪些可以排除？为甚么?

阶段 5　无穷多个质数（prime）

想一想　每个费马数都至少有一个质因数（prime factor）。从每个费马数中各选一个质因数。

停一停，试一试　你为 F_m 选的质数，会否与你为 F_n 选的质数相同？运用上一部分的结果。

背后的数学

费马猜对了吗？

没有。1732 年，莱昂哈德．欧拉证明了

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

欧拉并不是靠运气找到 641 的。他证明了 F_n 的任何质因数都必定具有一种非常特殊的形式（当 $n = 5$ 时，它必定是 64 的倍数加一），从而大幅减少了需要考虑的可能。你可以在练习 4 中亲自证明这一点。

自此以后，凡是有人成功检验过的费马数，由 F_5 到 F_{32}，结果全都是合成数（composite）。

就目前所知，F_0 至 F_4 可能是仅有的费马质数，但没有人能够证明这一点。这是一个货真价实的未解难题。

妙就妙在我们的证明完全不受影响。不论是质数还是合成数，费马数依然能产生无穷多个质数。

费马质数与正多边形作图

费马质数会在一个相当意想不到的地方出现。古希腊人懂得用直尺和圆规作出等边三角形和正五边形，而请留意 $3 = F_0$ 和 $5 = F_1$。其后两千年间，没有人能作出其他边数为质数的正多边形（regular polygon）。到了 1796 年，年仅 19 岁的卡尔．弗里德里希．高斯（Gauss）示范了怎样作出*正十七边形*，而 $17 = F_2$。

高斯更进一步：正 N 边形可以用直尺和圆规作出，当且仅当 N 是 2 的幂乘以若干个*互不相同的费马质数*。（Pierre Wantzel 在 1837 年补全了这个证明。）所以哪些正多边形可以作图，取决于费马质数有多少个。你会在 Section 6.2（STEP II 1991，第 4 题）遇到高斯正十七边形背后的关键计算，而完整的来龙去脉则属于*伽罗瓦理论*（Galois theory），那是大学本科数学课程的精华之一。

一个定理，多种证明

数学家为甚么要不厌其烦地把同一个定理证明多于一次？因为不同的证明会揭示不同的东西。这个证明一般归功于克里斯蒂安．哥德巴赫（Goldbach）在 1730 年写给欧拉的一封信，它表明：*任何一个由大于 1 的整数组成、各项两两互质的无穷数列，都必然带来无穷多个质数*。费马数只是其中一个方便的例子。（练习 3 给出另一个例子。）

它给出的结论也比欧几里得的证明更多。质数 $p_0, p_1, \ldots, p_{n-1}$ 是 n *个不同*的质数，每个都不超过 F_{n-1}。所以不大于 $2^{2^{n-1}} + 1$ 的质数至少有 n 个。这是一个关于质数如何分布的*定量*陈述。它非常弱（实际情况要好得多），但它是迈向十九世纪数学其中一项伟大成果的第一步，那就是*质数定理*（Prime Number Theorem），它精确地描述了质数怎样变得越来越稀疏。Section 1.2 会踏出下一步。

延伸练习

1 **欧几里得的版本。**写出欧几里得对“质数有无穷多个”的证明。它在甚么意义上是“反证法”（by contradiction），而费马数的证明又在甚么意义上是“构造性”（constructive）的？

2 **末位数字。**证明当 $n \geq 2$ 时，费马数 F_n 的末位数字是 7。

3 **西尔维斯特（Sylvester）数列。**定义 $a_1 = 2$ 及 $a_{n+1} = a_n^2 - a_n + 1$，于是数列的开头几项是 $2, 3, 7, 43, 1807, \ldots$

(a) 证明 $a_{n+1} - 1 = a_1 a_2 \cdots a_n$。

(b) 由此推导出各项两两互质，从而给出“质数有无穷多个”的另一个证明。

(c) 较难 证明 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$。

4 **欧拉的妙着。**本题需要用到费马小定理（*Fermat's Little Theorem*）：若 p 是质数且 $p \nmid a$，则 $a^{p-1} \equiv 1 \pmod{p}$。假设质数 p 整除 F_n。

(a) 证明 $2^{2^n} \equiv -1 \pmod{p}$，从而证明 $2^{2^{n+1}} \equiv 1 \pmod{p}$。

(b) 设 d 为满足 $2^d \equiv 1 \pmod{p}$ 的最小正整数。证明 d 整除 2^{n+1} 但不整除 2^n，并由此得出 $d = 2^{n+1}$。

(c) 利用费马小定理，证明 d 整除 $p - 1$。由此推导出 $p \equiv 1 \pmod{2^{n+1}}$。

(d) 当 $n = 5$ 时，这表示 F_5 的任何质因数都具有 $64k + 1$ 的形式。验证 641 确实如此。小于 641 而又具有这种形式的质数有多少个？

5 **质数的一个上界。**利用一个定理，多种证明中的论证，证明第 n 个质数不超过 $2^{2^{n-1}} + 1$。当 $n = 5$ 时，这个上界有多准确？

延伸阅读

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK***（Springer），第 1 章“Six proofs of the infinity of primes”（质数无穷性的六个证明）。书中除了这个证明外，还收录了欧几里得的证明和另外四个证明，其中一个用上了拓扑学（topology）。这是入读大学前最值得一读的书之一。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press），第 1–2 章。一本文笔优美的入门书，介绍质数与因数分解，最适合在入读大学前的暑假阅读。
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers***（Springer，2001）。关于费马数的一切，由欧拉的分解到高斯的正多边形，应有尽有。不妨翻翻开首几章。
- **Ian Stewart, *Why Beauty Is Truth***（Basic Books），关于高斯的一章。以一般读者为对象，讲述正十七边形的故事。

完整的引导式解答见第 1.1 节：

https://beyondstep.keithmcnulty.org/zh-hans/ch01/fermat-numbers.html

每星期一道 STEP 题目，完整讲解：The STEP Up，以电子邮件免费发送，订阅网址：keithmcnulty.substack.com