解答例

STEP II 2002、第 3 問

純粋数学 ・ フェルマー数と素数

> **STEP II 2002、問 3**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/02-s2-q3

この問題は、*Beyond STEP* の第 1.1 節「素数を生み出す工場」で詳しく解説されている：
https://beyondstep.keithmcnulty.org/ja/ch01/fermat-numbers.html

鍵となる考え方

$F_k - 2 = 2^{2^k} - 1$ と書く。これに $F_k = 2^{2^k} + 1$ を掛けると平方の差（difference of two squares）が現れ、それこそが帰納法（induction）に必要な一歩である。積の公式が得られれば、2 つのフェルマー数（Fermat number）の公約数（common factor）は必ず 2 を割り切る。フェルマー数はすべて奇数であるから、その公約数は 1 しかありえない。

解答

最初の 4 つのフェルマー数

$2^0 = 1$、$2^1 = 2$、$2^2 = 4$、$2^3 = 8$ であるから、

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

次に、k の最初の 3 つの値について $(*)$ を確かめる。

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

すべての $k \geq 1$ に対する $(*)$ の証明

k に関する数学的帰納法を用いる。$k = 1$ の場合は上で示した。

ある $k \geq 1$ に対して $(*)$ が成り立つ、すなわち $F_0 F_1 \cdots F_{k-1} = F_k - 2$ であると仮定する。このとき

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

よって $(*)$ は $k+1$ に対しても成り立ち、数学的帰納法により、すべての $k \geq 1$ に対して成り立つ。

? **考えてみよう** なぜ $\left(2^{2^k}\right)^2$ は $2^{2^{k+1}}$ に等しく、$2^{2^{2k}}$ などにはならないのか？

累乗を2乗すると指数は2倍になる：$\left(2^a\right)^2 = 2^{2a}$。ここで $a = 2^k$ であり、$2a = 2 \cdot 2^k = 2^{k+1}$ である。帰納法の段階でやるべきことの大半は、このように積み重なった指数を注意深く扱うことである。

どの2つのフェルマー数も共通の因数をもたない

相異なる2つのフェルマー数 F_m と F_n（$m < n$）をとる。このとき $n \geq 1$ であり、F_m は $k = n$ とした $(*)$ における因数 $F_0, \ldots, F_{n-1}$ の1つである。よって

$$F_n - 2 = F_m \times (\text{整数}),$$

となり、F_m は $F_n - 2$ を割り切る。

ここで、正の整数 d が F_m と F_n の両方を割り切ると仮定する。$d \mid F_m$ かつ $F_m \mid F_n - 2$ であるから、$d \mid F_n - 2$ である。d は F_n も割り切るので、その差も割り切る：

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

したがって $d = 1$ または $d = 2$ である。しかし $F_m = 2^{2^m} + 1$ は偶数に1を加えたものなので奇数である（$2^m \geq 1$ に注意）。よって $d \neq 2$ であり、ゆえに $d = 1$ である。以上より、どの2つのフェルマー数も1より大きい公約数をもたない。

素数は無限に存在する

各 F_n は 3 以上であるから、少なくとも 1 つの素因数（prime factor）をもつ。そのうちの 1 つを選び、p_n とおく。これにより、各 $n = 0, 1, 2, \ldots$ に対して素数が 1 つずつ得られる。

> **考えてみよう** 相異なる 2 つのフェルマー数から同じ素数が得られることはないのか？

ない。もし $m \neq n$ で $p_m = p_n$ ならば、その素数は F_m と F_n の両方を割り切る。すると 1 より大きい公約数となるが、これは前の小問で否定されている。よって素数 $p_0, p_1, p_2, \ldots$ はすべて相異なる。フェルマー数は無限に存在するから、相異なる素数も無限に存在する。

F_n 自体が素数である必要はまったくなかったことに注意しよう。必要だったのは、各フェルマー数が、他のどのフェルマー数とも共有しない**何らかの**素因数をもつことだけである。

検算

- $k = 4$ のときの $(*)$：$255 \times 257 = 65535 = 65537 - 2 = F_4 - 2$。また、12 までのすべての k について、$(*)$ をコンピュータで厳密に確かめた。
- $F_0, \ldots, F_5$ の最小の素因数は $3, 5, 17, 257, 65537, 641$ であり、議論が予言するとおりすべて相異なる。$F_5 = 4294967297 = 641 \times 6700417$ は、素数でない最初のフェルマー数である。
- $0 \leq m < n \leq 10$ のすべてについて $\gcd(F_m, F_n) = 1$ であることを数値的に確認した。

よくある間違い

- 2^{2^n} を $(2^2)^n = 4^n$ と読んでしまう。指数は 2^n であるから、$F_3 = 2^8 + 1$ であり、$4^3 + 1$ ではない。
- $d \mid 2$ を導いたあと、$d = 2$ を除外し忘れる。議論を完結させるのは、フェルマー数が奇数であるという事実である。
- すべてのフェルマー数が素数であると思い込む。最後の小問はこの仮定なしで成り立つし、そもそもこれは誤りである（$641 \mid F_5$）。

STEP のその先へ

この証明はポリア（Pólya）によるものである。これは素数の無限性を示す一連の証明の仲間である。いずれの証明も、どの2つも互いに素（pairwise coprime）な整数からなる無限数列を構成し、各項がそれぞれ新しい素数をもたらす。ユークリッド（Euclid）の証明も同じように読むことができる。フェルマー数は整数論の講義で再び登場する。ガウス（Gauss）は、正 n 角形（regular n-gon）が定規とコンパスで作図できるのは、n が 2 の累乗と相異なるフェルマー素数（Fermat prime）の積との積であるときであり、かつそのときに限ることを示した。また、F_4 より先のフェルマー素数は1つも知られていない。さらに学ぶには、Davenport の *The Higher Arithmetic*（『高等算術』）を読むとよい。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。