1.1 素数を生み出す工場

ワークシート

問題

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

ヒント

まずは自力で問題に取り組んでみよう。行き詰まったら、ヒントを**一つずつ**読み、そのたびに問題に戻ること。**手を止めて、やってみよう**と記したヒントが重要な段階である。各ヒントの後には計算用の余白がある。

> **考えてみよう**　最後の行は**無限に多くの素数**について問うている。中ほどでは**公約数**について問うている。「どの二つのフェルマー数も共通の約数をもたない」ことと「素数は無限に存在する」こととは、いったいどうつながりうるのだろうか。

段階 1　数の感触をつかむ

扱う内容：最初の 4 つのフェルマー数（Fermat numbers）

> **考えてみよう**　指数の積み重ねに注意すること。2^{2^n} は $2^{(2^n)}$ を意味する。まず $n = 0, 1, 2, 3$ に対して 2^n を計算し、そのあとで 2 をその値で累乗せよ。

段階 2 恒等式（identity）を確かめる

扱う内容：$k = 1, 2, 3$ に対する $(*)$

考えてみよう $k = 1, 2, 3$ のとき、$(*)$ の左辺はそれぞれ 1 個、2 個、3 個のフェルマー数の積である。各積を計算し、$F_k - 2$ と比べよ。

段階 3　恒等式を証明する

扱う内容：すべての $k \geq 1$ に対する $(*)$

考えてみよう　数学的帰納法（induction）を使うのが自然である。$(*)$ が k で成り立つとき、$k+1$ の場合の左辺を得るには両辺に何を掛ければよいか。

考えてみよう　その段階のあとで必要になるのは $(F_k - 2)\,F_k = F_{k+1} - 2$ である。$F_k - 2$ と F_k を、2 の累乗から 1 を引いたもの、または 1 を足したものとして表せ。

手を止めて、やってみよう　$(a-1)(a+1) = a^2 - 1$ である。$a = 2^{2^k}$ とおくと、a^2 は 2 の何乗か。

段階 4 公約数（common factor）をもたない

考えてみよう $m < n$ として、d が F_m と F_n の両方を割り切ると仮定する。$k = n$ として $(*)$ を用いよ。F_m はその左辺の因数の 1 つになっているか。

手を止めて、やってみよう したがって d は F_n だけでなく $F_n - 2$ も割り切る。すると d は何を割り切らなければならないか。その候補のうちどれを除外できるか、またそれはなぜか。

段階 5　素数は無限に存在する

考えてみよう　どのフェルマー数も少なくとも 1 つの素因数（prime factor）をもつ。各フェルマー数から素因数を 1 つずつ選べ。

手を止めて、やってみよう　F_m に対して選んだ素数が、F_n に対して選んだ素数と同じになることはありうるか。前の小問の結果を用いよ。

背後にある数学

フェルマーは正しかったか

正しくなかった。1732 年、レオンハルト・オイラー（Leonhard Euler）は

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

であることを示した。オイラーは偶然 641 を見つけたのではない。彼は F_n の素因数はきわめて特殊な形をしていなければならないこと（$n = 5$ のときは、64 の倍数に 1 を加えた数でなければならないこと）を証明し、それによって候補を大幅に絞り込んだのである。このことは演習 4 で自分で証明できる。

それ以来、これまでに調べることができた F_5 から F_{32} までのすべてのフェルマー数

は、合成数（composite）であることが判明している。知られている限りでは、F_0 から F_4 までが**唯一の**フェルマー素数かもしれないが、それを証明できた者はいない。これは正真正銘の未解決問題である。

愉快なひねりは、私たちの証明はそのことをまったく気にしないという点である。素数であれ合成数であれ、フェルマー数はやはり無限に多くの素数を生み出すのである。

フェルマー素数と多角形の作図

フェルマー素数は、まったく思いがけない場所に現れる。古代ギリシャ人は定規とコンパスで正三角形と正五角形を作図する方法を知っていたが、$3 = F_0$ かつ $5 = F_1$ であることに注目しよう。二千年もの間、辺の数が素数であるそれ以外の正多角形を作図できた者はいなかった。そして 1796 年、19 歳のカール・フリードリヒ・ガウス（Carl Friedrich Gauss）が正 17 **角形**の作図法を示した。そして $17 = F_2$ である。

ガウスはさらに進んだ。正 N 角形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**の積であるときであり、かつそのときに限る。（Pierre Wantzel が 1837 年に証明を完成させた。）つまり、どの多角形が作図できるかは、フェルマー素数がいくつあるかに依存するのである。ガウスの 17 角形の背後にある鍵となる計算には Section 6.2（STEP II 1991, Question 4）で出会うことになる。そして物語の全貌は、大学の学部課程の白眉の一つである**ガロア理論**（Galois theory）に属している。

一つの定理、多くの証明

数学者はなぜ同じ定理を何度も証明しようとするのだろうか。それは、異なる証明が異なることを明らかにするからである。この証明は通常、クリスティアン・ゴールドバッハ（Christian Goldbach）が 1730 年にオイラーに宛てた手紙によるものとされるが、これは、1 より大きい整数からなり、どの二つも互いに素であるような**任意の**無限数列が、無限に多くの素数の存在を導くことを示している。フェルマー数はその便利な一例にすぎない。（演習 3 で別の例を扱う。）

この証明はまた、ユークリッドの証明よりも多くのことを教えてくれる。素数 $p_0, p_1, \ldots, p_{n-1}$ は n 個の**相異なる**素数であり、それぞれ F_{n-1} 以下である。したがって、$2^{2^{n-1}} + 1$ 以下の素数は少なくとも n 個ある。これは素数がどのように分布しているかについての**定量的**（quantitative）な主張である。非常に弱い主張ではある（実際にはずっと良いことが成り立つ）が、素数がどのようにまばらになっていくかを正確に記述する、19 世紀数学の偉大な成果の一つである**素数定理**（Prime Number Theorem）への第一歩なのである。Section 1.2 でその次の一歩を踏み出す。

次の一歩

1 **ユークリッドの証明。**素数が無限に存在することのユークリッドによる証明を書き出せ。それはどのような意味で「背理法（contradiction）による」証明であり、フェルマー数による証明はどのような意味で「構成的（constructive）」な証明であるか。

2 **一の位の数字。**$n \geq 2$ のとき、フェルマー数 F_n の一の位は 7 であることを示せ。

3 **シルベスター（Sylvester）の数列。**$a_1 = 2$、$a_{n+1} = a_n^2 - a_n + 1$ と定める。この数列は $2, 3, 7, 43, 1807, \ldots$ と始まる。

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

   (b) 各項はどの二つも互いに素であることを導き、それにより素数が無限に存在することの別証明を与えよ。

   (c) やや難 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$ を示せ。

4 **オイラーの技法。**この問題ではフェルマーの小定理（*Fermat's Little Theorem*）を用いる。すなわち、p が素数で $p \nmid a$ ならば $a^{p-1} \equiv 1 \pmod{p}$ である。素数 p が F_n を割り切るとする。

   (a) $2^{2^n} \equiv -1 \pmod{p}$ を示し、それにより $2^{2^{n+1}} \equiv 1 \pmod{p}$ を示せ。

   (b) d を $2^d \equiv 1 \pmod{p}$ を満たす最小の正の整数とする。d は 2^{n+1} を割り切るが 2^n は割り切らないことを示し、$d = 2^{n+1}$ であると結論せよ。

   (c) フェルマーの小定理を用いて、d が $p - 1$ を割り切ることを示せ。それにより $p \equiv 1 \pmod{2^{n+1}}$ を導け。

   (d) $n = 5$ のとき、これは F_5 の任意の素因数が $64k + 1$ の形をしていることを意味する。641 がこの形であることを確かめよ。641 より小さいこの形の素数はいくつあるか。

5 **素数の上界。**一つの定理、多くの証明の議論を用いて、n 番目の素数は $2^{2^{n-1}} + 1$ 以下であることを示せ。$n = 5$ のとき、この上界はどの程度良いか。

さらに学ぶために

► **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK*（Springer）**、第 1 章「Six proofs of the infinity of primes」（素数が無限に存在することの六つの証明）。この証明が、ユークリッドの証明や、位相空間論を用いるものを含む他の四つの証明とともに収められている。大学入学前に読める最良の本の一つである。

- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）、第 1–2 章。素数と素因数分解への見事な筆致の入門書であり、大学入学前の夏に読むのに理想的である。
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers***（Springer, 2001）。オイラーによる因数分解からガウスの多角形まで、フェルマー数のすべてが書かれている。最初のほうの章を拾い読みするとよい。
- **Ian Stewart, *Why Beauty Is Truth***（Basic Books）、ガウスについての章。17 角形の物語が一般読者向けに語られている。

詳しい解説付きの解答は第 1.1 節にある：

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

毎週 1 問の STEP の問題を丁寧に解き明かす The STEP Up。メールで無料配信中：keithmcnulty.substack.com