# 1.7 因数分解が破綻するとき

## ワークシート

### 問題

**STEP I 2016、問 7**

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/16-s1-q7

## 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**　$S$ と $T$ の最初のいくつかの要素を書き出せ。小問 (iv) の定義によれば、$S$ のどの要素が*S*-**素数**（*S*-prime）か。

### 段階 1 和集合（union）、共通部分（intersection）と積

扱う内容：小問 (i), (ii)

**考えてみよう** $S$ と $T$ の要素を 4 で割った余り（remainder）はそれぞれいくつか。また、そのような余りになる正の整数はどれか。

**考えてみよう** $(4a+1)(4b+1)$ を展開し、その結果を $4\times(\text{何か})+1$ の形に表せ。

**手を止めて、やってみよう** $T$ については、$3\times 3$ のような小さな例を試してみよ。後の小問で使うので、$(4a+3)(4b+3)$ と $(4a+1)(4b+3)$ も計算しておくとよい。

### 段階 2　$T$ に属する素因数

扱う内容：小問 (iii)

**考えてみよう**　$T$ の要素の素因数（prime factor）はすべて奇数であるから、それぞれ $S$ または $T$ のどちらかに属する。

**手を止めて、やってみよう**　すべての素因数が $S$ に属するとしたら、どうなるか。小問 (ii) を繰り返し用いよ。

### 段階 3 奇数個の因数

扱う内容：小問 (iv)(a)

**考えてみよう** $T$ の要素はすべて 3 以上である。強い帰納法（strong induction）を用いて、各 $n \in T$ が $T$-素数（$T$-prime）であるか、$T$-素数の積であることを示せ。

**手を止めて、やってみよう** 積に現れる $T$-素数の個数が奇数でなければならないのはなぜか。$T$ の要素を偶数個掛けた積を 4 で割った余りがどうなるかを考えよ。

### 段階 4　2 通りの因数分解（factorisation）

扱う内容：小問 (iv)(b)

**考えてみよう**　15 は $T$-素数か。また、素数か。同じことは $S$ でも起こりうる。$S$ の要素のうち、$T$ に属する通常の素数 2 つの積になっているものはどれか。

**手を止めて、やってみよう**　$T$ に属する素数を 2 つ、たとえば 3 と 7 をとる。それぞれを 2 個ずつ用意したとき、それらを 2 つずつ組にして $S$ の要素を作る方法は何通りあるか。

## 背後にある数学

### 整数を特別なものにしているもの

通常の整数では、なぜ因数分解がうまくいくのか。鍵となる事実は**ユークリッドの補題**（Euclid's lemma）である。すなわち、素数 $p$ が積 $ab$ を割り切るならば、$p$ は $a$ を割り切るか、または $p$ は $b$ を割り切る。これはユークリッドの互除法（Euclidean algorithm）を用いて証明され、まさに $S$ で成り立たない性質である。そこでは、$S$-素数 9 は $21 \times 21 = 441$ を割り切る（$441 = 9 \times 49$ だから）が、9 は $S$ において 21 を割り切らない。大学 1 年で、ユークリッドの補題を注意深く証明し、そこから素因数分

解の一意性が導かれることを学ぶだろう。

### フェルマーの最終定理の誤った証明

1847 年 3 月 1 日、ガブリエル・ラメ（Gabriel Lamé）はパリ科学アカデミーで、フェルマーの最終定理を証明したと発表した。彼のアイデアは、1 の複素冪根（complex roots of unity）を用いて $x^n + y^n$ を

$$x^n + y^n = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y), \qquad \zeta = e^{2\pi \mathrm{i}/n}$$

（$n$ が奇数のとき）と因数分解し、各括弧の素因数について議論するというものであった。ジョゼフ・リウヴィル（Joseph Liouville）はすぐに異議を唱えた。$\zeta$ から作られる数が一意に因数分解されると言えるのはなぜか、と。数週間後、エルンスト・クンマー（Ernst Kummer）が、それらがしばしば一意に因数分解されないことをすでに示していたことが明らかになった。最初に破綻するのは $n = 23$ のときである。

クンマーは、素因数分解の一意性を回復させる追加の対象である「理想数」（ideal numbers）を考案して救えるものを救い、広い範囲の指数に対してフェルマーの最終定理を証明した。リヒャルト・デデキント（Richard Dedekind）はクンマーの理想数を**イデアル**（ideals）へと発展させた。これは現代代数学の中心的な概念の 1 つである。

---

### 覚えておきたい小さな例

数の体系 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ において

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

であり、4 つの因数はいずれもこの体系で「素数」である（演習 3）。これを、因数分解が一意である Section 1.6 のガウス整数（Gaussian integers）と比べてみよ。この種の体系のうちどれが素因数分解の一意性をもつかは、深い問題である。ガウス（Gauss）は、$\mathbb{Z}[\sqrt{-d}]$ の形の体系とその近い仲間のうち、それをもつのは 9 つだけであると予想した。これは最終的に、1952 年から 1967 年にかけて Heegner、Baker、Stark によって証明された。

## 次の一歩

---

1 **別の例。** 693 が $S$-素数への 2 通りの異なる因数分解をもつことを示せ。このような例を作る一般的な方法を見つけられるか。

**2** **偶数。** $E = \{2, 4, 6, 8, \ldots\}$ とする。どの数が $E$-素数か。60 が $E$-素数への因数分解を 2 通り以上もつことを示せ。

**3** $\mathbb{Z}[\sqrt{-5}]$。**ノルム** (norm) $N(a + b\sqrt{-5}) = a^2 + 5b^2$ を定義する。$N(zw) = N(z)N(w)$ を示せ。ノルムが 2 または 3 となる元が存在しないことを示すことにより、2、3、$1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ においてこれ以上因数分解できないことを導け。

**4** **ユークリッドの補題の応用。** やや難 ユークリッドの補題（素数が $ab$ を割り切るならば、それは $a$ または $b$ を割り切る）を仮定して、1 より大きいすべての整数は、因数の順序を除いて、ただ 1 通りの素因数分解しかもたないことを証明せよ。

## さらに学ぶために

- **Ian Stewart & David Tall,** ***Algebraic Number Theory and Fermat's Last Theorem*** （CRC Press）。『代数的整数論とフェルマーの最終定理』。冒頭の数章では、ラメ、クンマー、イデアルの物語が、意欲的な大学 1 年生がついていける水準で語られている。
- **John Stillwell,** ***Elements of Number Theory***。『数論の基礎』。整数とガウス整数における素因数分解の一意性を、並べて比較している。
- **Harold Edwards,** ***Fermat's Last Theorem: A Genetic Introduction*** （Springer）。『フェルマーの最終定理：発生的入門』。意欲的な読者向けで、クンマーの仕事をその歴史を通して解説している。

詳しい解説付きの解答は第 1.7 節にある：

https://beyondstep.keithmcnulty.org/ja/ch01/factorisation-fails.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