7.8 四つの平方数

ワークシート

問題

STEP III 1994、問 8

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/94-s3-q8

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　2 つの平方数の場合を思い出そう。複素数（complex number）$z = a + b\mathrm{i}$, $w = p + q\mathrm{i}$ に対して $|z|^2|w|^2 = |zw|^2$ が成り立つので、$(a^2 + b^2)(p^2 + q^2)$ は 2 つの平方数の和になる。行列を使って、これを 4 つの平方数に拡張するにはどうすればよいだろうか？

段階 1　行列式は 4 つの平方の和である

扱う内容：各行列の行列式

考えてみよう　$\begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix}$ の行列式（determinant）を計算せよ。複素数 z に対して zz^* は何になるか。

段階 2 積も同じ形をしている

扱う内容：2 つの行列の積

> **手を止めて、やってみよう** 2 つの行列を掛け合わせよ。積の 1 行目を (w_1, w_2) とおく。2 行目は $(-w_2^*, w_1^*)$ になっているか。そのうえで両辺の行列式をとれ。

段階 3　4 つの平方を読み取る

扱う内容：L_1, L_2, L_3, L_4 を求める

> **考えてみよう**　w_1 と w_2 を a, b, c, d, p, q, r, s で展開し、それぞれを実部（real part）と虚部（imaginary part）に分けよ。この 4 つの部分が求める L である。

背後にある数学

ラグランジュの四平方定理

ラグランジュの証明の概略は次のとおりである。オイラーの恒等式により、すべての素数 p が 4 つの平方数の和であることを示せば十分である。数え上げの議論により、$m < p$ を満たすある倍数 mp が 4 つの平方数の和であることがわかる。次に巧妙な「降下法（descent）」によって、$1 < m < p$ で mp が 4 つの平方数の和ならば、より小さいある m' についても $m'p$ が 4 つの平方数の和であることが示される。これを繰り返せば $m = 1$ に到達する（Section 1.5 のフェルマーの降下法と比べてみよ）。1834 年、ヤコビ（Jacobi）はさらに先へ進み、n を 4 つの平方数の和として表す方法の正確な個数を求めた。それは、n の約数（divisor）のうち 4 の倍数でないものの和の 8 倍である。たとえば、1 の表し方は 8 通りある（4 つの位置のどれかに ± 1 を置く）。

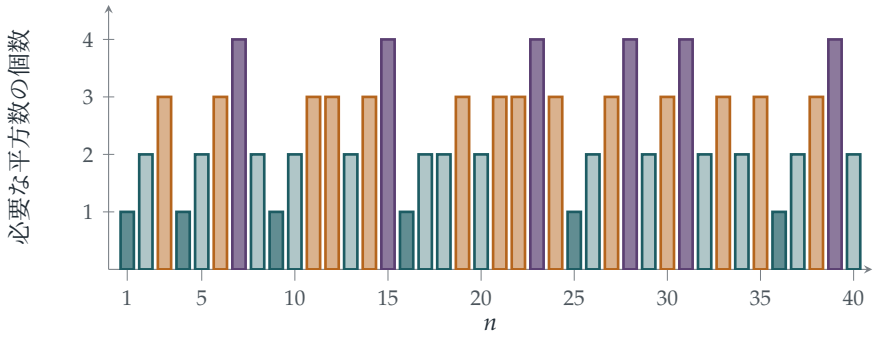

図 7.8.1　1 から 40 までの各 n をつくるのに必要な平方数の最小個数。ラグランジュの定理により、どの数も高々 4 個で足りる。4 個必要な数（紫）は $7, 15, 23, 28, 31, 39, \ldots$ であり、ルジャンドル（Legendre）とガウス（Gauss）の定理により、これはちょうど $4^k(8m+7)$ の形の数である。

2 つ、3 つ、4 つ

次元ごとの様子は微妙である。2 つの平方数の和は複素数から生じ、ある数が 2 つの平方数の和となるのは、$4k+3$ の形の素因数がすべて偶数乗で現れるときであり、かつそのときに限る（Section 1.6）。4 つの平方数の和は四元数から生じ、すべての数がそう表せる。ところが 3 つの平方数の和には積の恒等式がまったくない（乗法的な大きさをもつ 3 次元の数の体系は存在しない。ハミルトン（Hamilton）が 3 つ組で失敗したのはそのためである。Section 6.7 を参照）。そして定理もより難しい。ルジャンドルとガウスは、$n = 4^k(8m+7)$ でない限り n は 3 つの平方数の和であることを示した（図 7.8.1）。4 より先では、8 次元の八元数（octonions）が 8 つの平方数の恒等式を与える。これは Degen と Graves によって発見された。そしてフルヴィッツ（Hurwitz）は 1898 年に、この種の恒等式が存在するのは 1, 2, 4, 8 個の平方数の場合に限ることを証明した。

ウェアリングの問題

ラグランジュの定理は、1770 年にエドワード・ウェアリング（Edward Waring）が提起した問題の最初の場合である。その問題とは、各 k に対して、すべての正の整数が高々 $g(k)$ 個の k 乗数の和として表せるような数 $g(k)$ が存在するか、というものである。ダフィット・ヒルベルト（David Hilbert）は 1909 年に、そのような数が存在することを証明した。現在では $g(2) = 4, g(3) = 9$（たとえば $23 = 2 \cdot 2^3 + 7 \cdot 1^3$ には 9 個の立方数が必要である）、$g(4) = 19$ であることがわかっている。

次の一歩

1. **具体例。** $(a,b,c,d) = (p,q,r,s) = (2,1,1,1)$ として $L_1, \ldots, L_4$ の式を用い、$49 = 7 \times 7$ を 4 つの平方数の和として表し、答えを確かめよ。それは自明な $49 = 7^2 + 0^2 + 0^2 + 0^2$ と同じだろうか？

2. **4 つの中の 2 つ。** $c = d = r = s = 0$ のとき、この恒等式が Section 1.6 の 2 つの平方数の恒等式に帰着することを示せ。

3. **4 つの平方数が必要な数。** 平方数を 8 を法として（modulo）考えることにより、$8m + 7$ の形の数は 3 つの平方数の和として表せないことを示せ。

4. **ヤコビの公式。** 2 を 4 つの平方数の和として表す方法（順序と符号を区別する）を数え上げ、その答えが $8 \times (1 + 2) = 24$ であることを確かめよ。

さらに学ぶために

- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）。第 V 章でラグランジュの四平方定理を証明している。
- **John Conway & Derek Smith, *On Quaternions and Octonions***（A. K. Peters）。四元数の算術を扱い、四元数の整数を用いた四平方定理の証明も含む。
- **Aigner & Ziegler, *Proofs from THE BOOK***、「Representing numbers as sums of two squares」の章（数を 2 つの平方数の和として表す）。本節と対をなす、2 つの平方数の話である。

詳しい解説付きの解答は第 7.8 節にある：

https://beyondstep.keithmcnulty.org/ja/ch07/four-squares.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