解答例

STEP III 見本問題、第 10 問

純粋数学 ・ 合同算術

> **STEP III 見本問題、問 10**
>
> 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/spec-s3-q10

鍵となる考え方

どちらの小問も剰余（remainder）に関する問題なので、うまく選んだ数を法（modulo）として考えるとよい。(i) では、平方数（square）は 8 を法としてごく限られた値しかとらず、そのうちの 3 つを足しても決して 7 にはならない。(ii) では、2 つの項が 17 を法として同じ底を含むように累乗を書き直す。すると 2 つの係数の和が 17 の倍数になる。

解答

小問 (i)

奇数の平方。奇数を $2k+1$（k は整数）と表す。すると

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

連続する 2 つの整数 k と $k+1$ のうち一方は偶数であるから、$k(k+1)$ は偶数であり、$4k(k+1)$ は 8 の倍数である。したがって、奇数の平方を 8 で割った余りはつねに 1 である。

偶数の平方。偶数を $2k$ と表す。すると $(2k)^2 = 4k^2$ である。

- k が偶数で $k = 2j$ のとき、$4k^2 = 16j^2$ は 8 の倍数であり、余りは 0 である。
- k が奇数のとき、k^2 は奇数であるから $k^2 = 2j+1$ とおくと、$4k^2 = 8j+4$ となり、余りは 4 である。

よって、偶数の平方を 8 で割った余りは 0 または 4 である。

結論を導く。どの平方数も 8 を法として 0、1、4 のいずれかと合同である（ここには $0^2 = 0$ も含まれるので、3 つの平方数のうちいくつかが 0 であってもよいことになる）。$N = a^2 + b^2 + c^2$ とする。すると $N \bmod 8$ は、それぞれ $\{0, 1, 4\}$ から選んだ 3 つの数の和の余りである。そのうち 4 に等しいものの個数で場合分けすると、次のようになる。

4 の個数	残りの和として可能な値と、合計の 8 を法とした値
0	$0, 1, 2, 3$
1	$4 + \{0, 1, 2\} = 4, 5, 6$
2	$8 + \{0, 1\} \equiv 0, 1$
3	$12 \equiv 4$

とりうる余りは $0, 1, 2, 3, 4, 5, 6$ であり、7 は決して現れない。$8n + 7$ の形の数は 8 で割ると余りが 7 になるので、3 つの平方数の和にはなりえない。

考えてみよう 7 そのものが 3 つの平方数の和でないことを確かめるだけではいけないのはなぜか？

主張は $7, 15, 23, \ldots$ という無限個の数についてのものであり、1 つずつ確かめていてはいつまでも終わらないからである。8 を法として考えれば、これらすべてを一度に扱える。a、b、c が何であっても重要なのはその余りだけであり、上の表がすべての場合を尽くしている。

小問 (ii)

各項が定数と n 乗の積になるように累乗を分ける。

$$2^{3n+1} = 2 \cdot 8^n, \qquad 3\left(5^{2n+1}\right) = 15 \cdot 25^n.$$

ここで $25 = 17 + 8$ であるから $25 \equiv 8 \pmod{17}$ であり、したがってすべての $n \geq 0$ に対して $25^n \equiv 8^n \pmod{17}$ が成り立つ（合同式（congruence）は辺々掛けてよい）。よって

$$\begin{aligned} 2^{3n+1} + 3\left(5^{2n+1}\right) &= 2 \cdot 8^n + 15 \cdot 25^n \\ &\equiv 2 \cdot 8^n + 15 \cdot 8^n \\ &= 17 \cdot 8^n \equiv 0 \pmod{17}. \end{aligned}$$

ゆえに、すべての整数 $n \geq 0$ に対して 17 は $2^{3n+1} + 3(5^{2n+1})$ を割り切る。これが示すべきことであった。

考えてみよう 合同式をまだ習っていない場合はどうすればよいか？

同じ考え方は数学的帰納法（induction）でも使える。$f(n) = 2 \cdot 8^n + 15 \cdot 25^n$ とおく。すると $f(0) = 17$ であり、

$$f(n+1) - 8f(n) = 15 \cdot 25^{n+1} - 15 \cdot 8 \cdot 25^n = 15 \cdot 25^n(25 - 8) = 17 \cdot 15 \cdot 25^n,$$

であるから、$f(n+1) = 8f(n) + 17 \cdot 15 \cdot 25^n$ となる。$17 \mid f(n)$ ならば $17 \mid f(n+1)$ であり、数学的帰納法により結果が従う。

検算

小さな場合を試してみる。$7 = 4+1+1+1$ は 4 つの平方数を必要とし、$15 = 9+4+1+1$ も 4 つを必要とする。一方、$6 = 4+1+1$ や $14 = 9+4+1$ は問題ない。コンピュータで探索すると、5000 以下の $8n+7$ の形の数で 3 つの平方数の和になるものは 1 つもないことが確かめられる。(ii) については、$n = 0$ のとき $2 + 15 = 17$、$n = 1$ のとき $16 + 375 = 391 = 17 \times 23$ である。0 から 299 までのすべての n について、この式が 17 で割り切れることを確認した。

よくある間違い

- 0 も平方数であることを忘れること。「3 つの平方数の和」は、実際には 0 でない平方数を 1 つか 2 つしか使わないこともある。上の議論では 0 が剰余の 1 つとして含まれているので、この場合も自動的に扱われている。
- 「$4k^2 + 4k$ は 4 で割り切れる」という理由で奇数の平方が $1 \bmod 8$ であると述べること。これでは $1 \bmod 4$ しか得られない。$k(k+1)$ から出てくる因数 2 が必要である。

STEP のその先へ

小問 (i) は、ルジャンドル（Legendre）の三平方定理（three-square theorem）のやさしいほうの半分である。この定理は、正の整数が 3 つの平方数の和で表せるのは、それが $4^a(8n+7)$ の形でないとき、そして**そのときに限る**、と主張する。逆向きの証明ははるかに難しく、二次形式（quadratic form）の理論を必要とする。これに対して、ラグランジュ（Lagrange）は**すべての**正の整数が 4 つの平方数の和で表せることを証明した。小問 (ii) は $\mathbb{Z}/17\mathbb{Z}$ における日常的な計算であり、大学 1 年次の講義ではこれが群（group）や環（ring）の研究へと発展していく。ダヴェンポート（Davenport）の *The Higher Arithmetic*（高等整数論）は、合同式と平方数の和を見事に解説している。

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。