解答例

STEP I 2004、第 5 問

純粋数学 • 5 を法とする剰余

> **STEP I 2004、問 5**
>
> 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/04-s1-q5

鍵となる考え方

5 つの等差数列（arithmetic progression）は、正の整数を 5 で割った余りによって分類している。各類の一般項（general term）が $5n-3$ のような形で書ければ、展開して 5 をくくり出すことで、和や平方がどの類に入るかを追跡できる。これにより平方数がどこに入りうるかの全体像が得られ、2 つの不可能性の証明はどちらもそこから従う。右辺は、左辺が決して入りえない類に属しているのである。

解答

一般項

各数列の公差（common difference）は 5 なので、$n = 1, 2, 3, \ldots$ に対して第 n 項は

$$A:\ 5n-4, \qquad B:\ 5n-3, \qquad C:\ 5n-2, \qquad D:\ 5n-1, \qquad E:\ 5n.$$

である（$n = 1$ を代入すると、それぞれ最初に挙げられた項になることが確かめられる）。よって、正の整数が A、B、C、D、E に属するのは、それぞれ余りが 1、2、3、4、0 となるとき、そしてそのときに限る（5 で割ったときの余りである）。

B の項と C の項の和

B の任意の項 $5m-3$ と C の任意の項 $5n-2$ をとる。ただし $m, n \geq 1$ とする。このとき

$$(5m-3)+(5n-2) = 5m+5n-5 = 5(m+n-1).$$

$m+n-1 \geq 1$ は正の整数なので、これは E の第 $(m+n-1)$ 項であり、題意が示された。

B と C の項の平方

B の項 $5m-3$ に対して

$$\begin{aligned}(5m-3)^2 &= 25m^2-30m+9\\ &= 5(5m^2-6m+2)-1.\end{aligned}$$

ここで $k=5m^2-6m+2$ は整数であり、すべての $m \geq 1$ に対して $k=5m^2-6m+2=m(5m-6)+2 \geq 1$ である（$m=1$ のとき値は 1 であり、$m \geq 2$ のときは m と $5m-6$ がともに正である）。よって $(5m-3)^2=5k-1$ は D の第 k 項である。B の項の平方はすべて D に属する。

C についての同様の主張は、**C のすべての項の平方もまた D の項である**、というものである。実際、C の項 $5m-2$ に対して

$$\begin{aligned}(5m-2)^2 &= 25m^2-20m+4\\ &= 5(5m^2-4m+1)-1,\end{aligned}$$

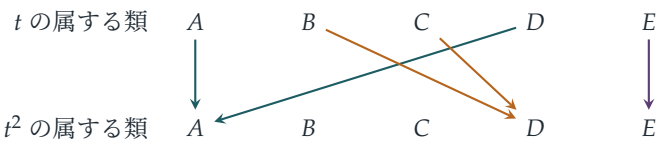
であり、$m \geq 1$ のとき $k=5m^2-4m+1=m(5m-4)+1 \geq 2$ である。よって $(5m-2)^2$ は D の第 k 項である。

考えてみよう A、D、E の項の平方はどこに属するか？

小問 (i) と (ii) でこれが必要になるので、残りの 3 つの類も同じように調べておく価値がある：

$$\begin{aligned}(5m-4)^2 &= 25m^2-40m+16 = 5(5m^2-8m+4)-4 && (A \text{ に属する}),\\ (5m-1)^2 &= 25m^2-10m+1 = 5(5m^2-2m+1)-4 && (A \text{ に属する}),\\ (5m)^2 &= 5(5m^2) && (E \text{ に属する}).\end{aligned}$$

括弧内は $m \geq 1$ のとき正の整数である（たとえば $5m^2-8m+4=m(5m-8)+4 \geq 1$、また $5m^2-2m+1 \geq 4$）。よって平方をとると、各類は次のように移る：



特に、**B や C に属する完全平方数（*perfect square*）は存在しない**。正の平方数はすべて A、D、E のいずれかに属する。

小問 (i)

正の整数 x と y が $x^2+5y=243\,723$ を満たすと仮定する。$243\,723=5\times 48\,744+3$ なので、右辺は C の項 $5\times 48\,745-2$ である。すると

$$x^2=243\,723-5y=5(48\,745-y)-2.$$

これは正である（x^2 だからである）ので、$48\,745-y$ は正の整数であり、x^2 は C の項となる。しかし、C に属する平方数は存在しないことをすでに示した。この矛盾（contradiction）により、そのような正の整数 x と y は存在しない。

小問 (ii)

4 乗数（fourth power）は平方数の平方である。平方数 x^2 は A、D、E のいずれかに属し、A または D の項を平方すると A の項になり、E の項を平方すると E の項になる。よって任意の正の整数 x に対して

x^4 が属するのはA またはE, すなわち x^4 の余りは1 または0 である。ただし割る数は5.

y^4 についても同じことが成り立つので、$2y^4$ の余りは 2 または 0 である。足し合わせると、x^4+2y^4 を 5 で割った余りは、次のいずれかの余りに等しい。

$$1+2=3,\qquad 1+0=1,\qquad 0+2=2,\qquad 0+0=0,$$

よって x^4+2y^4 は C、A、B、E のいずれかに属し、D には**決して**属さない。

考えてみよう なぜ余りをそのまま足してよいのか？

$x^4=5a+r$、$2y^4=5b+s$ とすると $x^4+2y^4=5(a+b)+(r+s)$ なので、和と $r+s$ の差は 5 の倍数であり、和は $r+s$ と同じ類に属する。これはまさに、上で $B+C$ について行った計算を一般の形にしたものである。

さて、$26\,081\,974=5\times 5\,216\,395-1$ は一の位が 4 なので、D の項である。したがって、どのような正の整数 x と y に対しても、これが x^4+2y^4 に等しくなることはなく、題意が示された。

検算

- 小さな場合：$2^2=4$、$7^2=49$、$12^2=144$ はいずれも一の位が 4 または 9 なので D に属する。$3^2=9$、$8^2=64$、$13^2=169$ も同様である。
- 4 乗数：$1, 16, 81, 256, 625, 1296$ はいずれも一の位が 1、6、5 のいずれかなので、A または E に属する。

- $x \leq \sqrt{243\,723} \approx 493.7$ の範囲でコンピュータ探索を行っても、$243\,723 - x^2$ が 5 の正の倍数となる x は見つからない。また、$x^4 < 26\,081\,974$（したがって $x \leq 71$）を満たすすべての x について探索しても、$2y^4 = 26\,081\,974 - x^4$ となる y は見つからない。

よくある間違い

- E の一般項を $5n+5$、A の一般項を $5n+1$ と書くのは構わないが、その場合 n は 0 から始まる。2 つの流儀を混同すると、項が 1 つずれてしまう。
- 小問 (i) で、$x^2 > 0$ であることを使って $48\,745 - y$ が**正の**整数であると示すのを忘れる。数列には正の整数しか含まれないので、これがないと x^2 が C の項であるとは限らない。
- 小問 (ii) で x^4 だけを扱い、係数 2 によって y^4 の余りが 1 から 2 に移ることを忘れる。

STEP のその先へ

5 つの数列は 5 を法とする剰余類（residue classes modulo 5）であり、この問題全体は $\mathbb{Z}/5\mathbb{Z}$ における算術である。そこでの平方は $0, 1, 4$（**平方剰余**（quadratic residues））であり、4 乗は $0, 1$ である。これは、$5 \nmid a$ のとき $a^4 \equiv 1 \pmod 5$ が成り立つというフェルマーの小定理（Fermat's little theorem）の一例である。ディオファントス方程式（Diophantine equation）を、うまく選んだ数を法として考えることは、解が存在しないことを証明するための最初の道具である。ダヴェンポート（Davenport）の *The Higher Arithmetic* は、合同式（congruences）と平方剰余を見事に展開している。

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。