解答例

# STEP II 1993、第 7 問

純粋数学 • 5 を法とする無限降下法

> **STEP II 1993、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/93-s2-q7

## 鍵となる考え方

右辺は 5 の倍数なので、5 を法として（modulo 5）考えると、この方程式は有限個の場合を調べるだけの小さな問題に変わる。平方数は 5 を法として 0、1、4 $(\mathrm{mod}\ 5)$ のいずれかにしかならないからである。$a$ と $b$ が 5 の倍数であることが示されれば、方程式から $c$ も 5 の倍数となり、すべてを 5 で割ると**より小さい**解が得られる。0 でない整数を 5 で限りなく割り続けることはできない。これがフェルマー（Fermat）の無限降下法（method of infinite descent）である。

## 解答

### $a$ と $b$ が 5 で割り切れること

5 を法とする各剰余（residue）を 2 乗すると、次のようになる。

| $x\ (\mathrm{mod}\ 5)$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^2\ (\mathrm{mod}\ 5)$ | 0 | 1 | 4 | 4 | 1 |
| $2x^2\ (\mathrm{mod}\ 5)$ | 0 | 2 | 3 | 3 | 2 |

よって $b^2 \equiv 0, 1$ または 4 であり、$2a^2 \equiv 0, 2$ または 3 $(\mathrm{mod}\ 5)$ である。$5c^2 \equiv 0\ (\mathrm{mod}\ 5)$ であるから、

$$2a^2 + b^2 \equiv 0 \pmod 5.$$

が成り立たなければならない。そこで、すべての組合せを書き出す。

| $2a^2+b^2$ | $b^2\equiv 0$ | $b^2\equiv 1$ | $b^2\equiv 4$ |
|---|---|---|---|
| $2a^2\equiv 0$ | **0** | 1 | 4 |
| $2a^2\equiv 2$ | 2 | 3 | 1 |
| $2a^2\equiv 3$ | 3 | 4 | 2 |

値が 0 となるのは、$2a^2\equiv 0$ かつ $b^2\equiv 0$ の場合だけである。最初の表より、$x^2\equiv 0 \pmod 5$ となるのは $x\equiv 0$ のときに限る（同じことであるが、5 は素数（prime）なので、$5\mid x^2$ ならば $5\mid x$ である）。したがって $a\equiv 0$ かつ $b\equiv 0 \pmod 5$ であり、$a$ と $b$ はともに 5 で割り切れる。これが示すべきことであった。

### 解は $a=b=c=0$ のみであること

$p,q$ を整数として $a=5p$、$b=5q$ とおく。代入すると、

$$25(2p^2+q^2)=5c^2 \quad\Longrightarrow\quad c^2=5(2p^2+q^2).$$

よって $5\mid c^2$ であり、5 は素数なので $5\mid c$ である。$c=5r$ とおく。すると $25r^2=5(2p^2+q^2)$、すなわち

$$2p^2+q^2=5r^2.$$

となる。これは元の方程式そのものである。したがって、$(a,b,c)$ が解ならば、3 つとも 5 で割り切れ、$(a/5,\,b/5,\,c/5)$ もまた整数解である。

> **考えてみよう** 「5 で割り続けられる」ことから、なぜすべてが 0 でなければならないのか。

この操作を繰り返し適用する。解 $(a,b,c)$ から始めて $n$ 回操作すると整数解 $(a/5^n,\,b/5^n,\,c/5^n)$ が得られるので、**すべての** $n\geq 1$ に対して $5^n$ は $a$、$b$、$c$ のそれぞれを割り切る。

しかし、0 でない整数 $m$ は 5 で有限回しか割れない。実際、$5^n\mid m$ かつ $m\neq 0$ ならば $5^n\leq |m|$ であるが、$n$ が大きくなればこれは成り立たなくなる。よって $a$、$b$、$c$ のいずれも 0 でない値をとることはできない。

同じことを降下法の議論として述べることもできる。$c\neq 0$ である解が存在したと仮定し、そのうち $|c|$ が正で最小となるものを選ぶ。すると $(a/5,b/5,c/5)$ は $0<|c/5|<|c|$ を満たす解となり、矛盾する。よって $c=0$ であり、このとき $2a^2+b^2=0$ となるが、両方の項は非負なので $a=b=0$ でなければならない。

したがって、整数解は $a=b=c=0$ のみである。

## 検算

- 5 を法とする剰余の組 $(a, b) \bmod 5$ の 25 通りすべてを調べると、$2a^2 + b^2 \equiv 0$ となるのは $(0, 0)$ のみである。
- $|a|, |b| \leq 300$ の範囲をすべてコンピュータで探索しても、$2a^2 + b^2 = 5c^2$ の解は $a = b = c = 0$ 以外に見つからない。
- $a^2 + b^2 = 5c^2$ と比較してみよ。こちらは $(1, 2, 1)$ のような自明でない解を**実際にもつ**。この場合は $1 + 4 \equiv 0 \pmod 5$ となるので、前半の剰余による議論が成り立たなくなる。まさにそうなるべきなのである。

## よくある間違い

- $5 \mid a^2$ から理由を述べずに $5 \mid a$ と結論すること。これは 5 が素数であることから（あるいは表から）正しいが、そのことは書き添える必要がある。
- $c$ も 5 で割り切れることを示し忘れること。これがなければ $(a/5, b/5, c/5)$ が整数解であるとは限らず、降下法が始まらない。
- 「再び 5 で割れる」で止めてしまうこと。割り算を繰り返すとなぜ 0 になるのかを述べるまで、証明は完成しない。

## STEP のその先へ

これはフェルマーの**無限降下法**であり、$\sqrt{2}$ が無理数であることや、$x^4 + y^4 = z^2$ が自明でない解をもたないことを証明するのと同じ方法である。$2a^2 + b^2 = 5c^2$ のような方程式は、整数論（number theory）において体系的に研究されている。ルジャンドル（Legendre）の定理は、$Ax^2 + By^2 = Cz^2$ が自明でない整数解をもつための正確な条件を、平方剰余（quadratic residue）を用いて与える。今回の場合、解の存在を妨げているのは、$-2$ が 5 を法として平方数でないことである。Davenport の *The Higher Arithmetic*（『高等算術』）では、合同式、平方剰余、降下法が扱われている。

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。