解答例

STEP I 2019、第 7 問

純粋数学 ・ 無理性と合同式

> **STEP I 2019、問 7**
>
> 先に進む前に、まず問題を読んでおこう。問題は、OCR が配布している 2019 年の STEP 過去問一式（zip ファイル）のうち、STEP I の問題用紙にある：
>
> www.ocr.org.uk/Images/696590-2019-past-papers.zip

鍵となる考え方

$\sqrt{2}+\sqrt{3}=a/b$ が既約分数（lowest terms）で表されているとすると、2 回平方することで根号（surd）が消え、整数 a, b に関する多項式（polynomial）の方程式が残る。次に、その方程式を小さな素数（prime）を法（modulo）として考える。この方程式から、その素数は a と b の両方を割り切るか、どちらも割り切らないかのいずれかであることが従う。「両方」は既約であることに矛盾し、「どちらも割り切らない」は余りによって否定される。この解法の要は、余りが本当に食い違うような素数を選ぶことに尽きる。

解答

小問 (i)

ステップ 1. すべての整数は、ある整数 k を用いて $3k, 3k+1, 3k-1$ のいずれかの形に表せる。よって $3 \nmid a$ ならば $a = 3k \pm 1$ である。どちらの場合も

$$a^2 = 9k^2 \pm 6k + 1 = 3(3k^2 \pm 2k) + 1,$$

となり、これは 3 の倍数に 1 を加えたものである。

ステップ 3. $\dfrac{a}{b} = \sqrt{2}+\sqrt{3}$ の両辺を平方すると

$$\frac{a^2}{b^2} = 2 + 2\sqrt{6} + 3, \qquad \text{よって} \qquad a^2 - 5b^2 = 2\sqrt{6}\,b^2.$$

これで根号が一方の辺に孤立したので、もう一度平方すれば根号は消える：

$$a^4 - 10a^2b^2 + 25b^4 = 24b^4,$$
$$a^4 + b^4 = 10a^2b^2,$$

となり、示すべき式が得られた。（必要なのはこの向きの含意だけである。すなわち、ステップ 2 の a, b はどれもこの方程式を満たさなければならない。）

ステップ 4. $3 \mid a$ と仮定する。ステップ 3 の式を変形すると

$$b^4 = 10a^2b^2 - a^4 = a^2\,(10b^2 - a^2),$$

となり、右辺は 3 で（さらには 9 で）割り切れる。もし $3 \nmid b$ ならば、ステップ 1 より $b^2 = 3m + 1$ であるから、$b^4 = (b^2)^2 = 9m^2 + 6m + 1$ は 3 の倍数では**ない**。これは矛盾である。したがって $3 \mid b$ である。

> **考えてみよう** ステップ 4 は $3 \mid a$ の場合を扱っている。では、3 が a も b も割り切らない場合はどうか？

ステップ 5. ステップ 3 の方程式は a と b について対称（symmetric）であるから、ステップ 4 は役割を入れ替えても成り立つ。すなわち、$3 \mid b$ ならば $3 \mid a$ である。a と b は 1 より大きい公約数をもたないので、両方が 3 の倍数であることはなく、したがってステップ 4 よりどちらも 3 の倍数ではない。この場合はステップ 2–4 では扱われておらず、ここでステップ 1 が役に立つ。$a^2 = 3r + 1, b^2 = 3s + 1$ とおく。すると a^4, b^4, a^2b^2 はいずれも 3 の倍数に 1 を加えたものになる（そのような 2 数の積もまた同じ形である）。ステップ 3 の式を 3 を法として考えると、$10 \equiv 1$ であるから

$$a^4 + b^4 \equiv 1 + 1 = 2, \qquad 10a^2b^2 \equiv 1 \cdot 1 \cdot 1 = 1 \pmod 3,$$

となる。ステップ 3 の両辺を 3 で割った余りが異なるが、これはありえない。よって、そのような a, b は存在しない。また $\sqrt{2} + \sqrt{3} > 0$ であるから、もしこれが有理数ならば、互いに素（coprime）な正の整数 a, b を用いて表せるはずである。以上より、$\sqrt{2} + \sqrt{3}$ は無理数（irrational）である。

小問 (ii)

$\sqrt{6} + \sqrt{7} = a/b$ で、a, b は 1 より大きい公約数をもたない正の整数であると仮定する。先ほどと同様に

$$\frac{a^2}{b^2} = 13 + 2\sqrt{42} \quad \Longrightarrow \quad (a^2 - 13b^2)^2 = 168\,b^4,$$

であり、展開すると $a^4 - 26a^2b^2 + 169b^4 = 168b^4$、すなわち

$$a^4 + b^4 = 26a^2b^2.$$

5 を法とする平方数. $5 \nmid a$ ならば $a = 5k \pm 1$ または $a = 5k \pm 2$ であり、

$$a^2 = 5(5k^2 \pm 2k) + 1 \qquad \text{または} \qquad a^2 = 5(5k^2 \pm 4k) + 4.$$

となる。よって $a^2 \equiv \pm 1 \pmod 5$ であり、したがって $a^4 \equiv 1 \pmod 5$ である。

整除性. $5 \mid a$ ならば、$b^4 = a^2(26b^2 - a^2)$ は 5 の倍数である。しかし $5 \nmid b$ ならば $b^4 \equiv 1 \pmod 5$ であるから、$5 \mid b$ でなければならない。対称性より、$5 \mid b$ ならば $5 \mid a$ である。a と b は互いに素であるから、どちらも 5 で割り切れない。

矛盾. このとき $a^4 \equiv b^4 \equiv 1$ であり、$a^2b^2 \equiv (\pm 1)(\pm 1) = \pm 1 \pmod 5$ である。$26 \equiv 1$ であるから

$$a^4 + b^4 \equiv 2, \qquad 26a^2b^2 \equiv \pm 1 \pmod 5.$$

しかし $2 \not\equiv \pm 1 \pmod 5$ であるから、この方程式は成り立ちえない。したがって $\sqrt{6} + \sqrt{7}$ は無理数である。

考えてみよう ここで 5 の代わりに 3 を使おうとすると、どのステップが破綻するか？

3 がうまくいかない理由. 議論の前半は 3 を法としても成り立つ。すなわち、$3 \mid a$ ならば $3 \mid b^4$ なので $3 \mid b$ となり、よって a も b も 3 の倍数ではない。しかしこのとき $a^4 \equiv b^4 \equiv a^2b^2 \equiv 1 \pmod 3$ であり、$26 \equiv 2 \pmod 3$ であるから

$$a^4 + b^4 \equiv 2 \qquad \text{かつ} \qquad 26a^2b^2 \equiv 2 \pmod 3.$$

両辺が一致するので、矛盾は生じない。3 を法とすると、方程式 $a^4 + b^4 = 26a^2b^2$ は 3 の倍数でない**すべての**組で満たされるため、3 による整除性ではこれを否定できない。（小問 (i) では係数が $10 \equiv 1$ であり、$2 \neq 1$ から食い違いが生じた。ここでは係数が $26 \equiv 2$ なので、食い違いが消えてしまう。）

検算

- 数値的に、$x = \sqrt{2} + \sqrt{3} \approx 3.1463$ に対して $x^4 - 10x^2 + 1 \approx 0$（誤差はおよそ 10^{-14}）となる。同様に $y = \sqrt{6} + \sqrt{7} \approx 5.0952$ に対して $y^4 - 26y^2 + 1 \approx 0$ となる。よって 2 つの 4 次方程式（quartic equation）は正しい。
- 余りの組をすべて試してみると、$a^4 + b^4 \equiv 10a^2b^2 \pmod 3$ の解は $a \equiv b \equiv 0$ のみであり、$a^4 + b^4 \equiv 26a^2b^2 \pmod 5$ についても同じことが成り立つ。しかし $a^4 + b^4 \equiv 26a^2b^2 \pmod 3$ は $(1,1), (1,2), (2,1), (2,2)$ でも満たされる。これこそが、小問 (ii) で 3 がうまくいかない理由である。
- コンピュータで探索したところ、どちらの方程式についても、それを満たす互いに素な正の整数 $a, b \leq 400$ は見つからなかった。

よくある間違い

- ステップ 4 で止めてしまうこと。ステップ 4 は a と b が 3 の倍数になりえないことを示すにすぎない。どちらも 3 の倍数でない場合を扱うには、さらにステップ 1 が必要である。
- $3 \mid b^4 \Rightarrow 3 \mid b$ を理由なしに主張すること。その理由はステップ 1 が与える。すなわち、$3 \nmid b$ ならば b^4 を 3 で割った余りは 1 である。
- 小問 (ii) で、平方数を 5 で割った余りが 4（すなわち -1）にもなりうることを忘れること。そのため a^2b^2 は 1 だけでなく $\equiv \pm 1$ となりうる。

STEP のその先へ

数 $\sqrt{2}+\sqrt{3}$ は $x^4 - 10x^2 + 1$ の根であり、ここでの議論は実質的に、この多項式が有理数の根をもたないことの証明である。有理根定理（rational root theorem）を使えばより早く示せる。すなわち、有理数の根があるとすればそれは ± 1 でなければならないが、どちらも根ではない。多項式を素数を法として還元し、根や因数をもたないことを示すのは、大学 1 年の代数学における標準的な道具である（たとえば既約性（irreducibility）の判定法）。興味深いことに、$x^4 - 10x^2 + 1$ は有理数体上では既約であるにもかかわらず、すべての素数を法として因数分解できる。これは有名な例である。Allenby の *Rings, Fields and Groups*（環・体・群）はこうした考え方を展開しており、ダヴェンポート（Davenport）の *The Higher Arithmetic*（高等算術）は合同式（congruence）へのすばらしい入門書である。

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。