解答例

STEP I 2006、第 1 問

純粋数学 • 平方の差

> **STEP I 2006、問 1**
>
> 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/06-s1-q1

鍵となる考え方

$(n+m)^2 - 33\,127 = k^2$ ならば、$33\,127 = (n+m)^2 - k^2$ は 2 つの平方数の差（difference of two squares）であるから、$(n+m-k)(n+m+k)$ と因数分解（factorise）できる。これはフェルマー（Fermat）による古くからの因数分解の技法である：$\sqrt{N}$ のすぐ上から始めて、$a^2 - N$ が平方数になるまで 1 つずつ上へ進んでいく。議論を逆にたどると、33 127 のどの因数分解からも m の値が 1 つ得られるので、m の値の個数を数えることは因数分解の個数を数えることに帰着する。

解答

n を求める

$180^2 = 32\,400$ であるから、33 127 の平方根は 180 より少し大きい。計算すると

$$182^2 = 33\,124 < 33\,127 < 33\,489 = 183^2,$$

となるので、$n = 182$ である。$33\,127 = 182^2 + 3$ であるから、これ自身は完全平方数（perfect square）ではないことに注意する。

小さな m の値

$m = 1, 2, \ldots$ を順に試す：

$$183^2 - 33\,127 = 33\,489 - 33\,127 = 362, \quad \text{平方数ではない} (19^2 = 361),$$
$$184^2 - 33\,127 = 33\,856 - 33\,127 = 729 = 27^2.$$

したがって $m = 2$ が条件を満たし、このとき $(n+m)^2 - 33\,127 = 27^2$ である。

33 127 を因数分解する

移項して平方の差を用いると、

$$33\,127 = 184^2 - 27^2 = (184-27)(184+27) = 157 \times 211,$$

となるので、$p = 157$、$q = 211$ ととることができ、どちらも 1 より大きい。

m の値がちょうど 2 つであること

どちらの因数も素数（prime）である。157 については、$13^2 = 169 > 157$ であるから素数 $2, 3, 5, 7, 11$ だけを調べればよく、いずれも 157 を割り切らない。211 については、$15^2 = 225 > 211$ であるから $2, 3, 5, 7, 11, 13$ を調べればよく、いずれも 211 を割り切らない。よって $33\,127 = 157 \times 211$ が素因数分解（prime factorisation）であり、$u \le v$ を満たす正の整数の積 uv として 33 127 を表す方法は

$$1 \times 33\,127 \qquad \text{および} \qquad 157 \times 211.$$

に限られる。

次に、$k \ge 0$ として $(n+m)^2 - 33\,127 = k^2$ が成り立つと仮定する。$a = n + m > 0$ とおく。これは問題が想定している状況である（n から出発して上へ進む）。すると

$$(a-k)(a+k) = 33\,127.$$

となる。ここで $a + k > 0$ であるから $a - k > 0$ でもあり、また $a - k \le a + k$ である。したがって $(a-k, a+k)$ は上の 2 組 (u, v) のいずれかでなければならず、このとき

$$a = \frac{u+v}{2}, \qquad k = \frac{v-u}{2}.$$

である。u と v はどちらも奇数であるから、これらは整数である。

> **考えてみよう** なぜ各因数分解からちょうど 1 つの m が得られるのか。また、なぜそれ以外の m が紛れ込むことはないのか。

この対応は双方向である。a と k が与えられれば、組 $(a-k, a+k)$ は 1 つの因数分解である。逆に因数分解 (u, v) が与えられれば、上の式から a と k がただ 1 通りに復元される。よって a の値（したがって $m = a - 182$ の値）は因数の組と一対一に対応（one-to-one correspondence）し、因数の組はちょうど 2 つである。

- $(u, v) = (157, 211)$ からは $a = 184$、$k = 27$ が得られ、$m = 184 - 182 = 2$ となる。これは先に求めた値である。
- $(u, v) = (1, 33\,127)$ からは $a = 16\,564$、$k = 16\,563$ が得られ、

$$m = 16\,564 - 182 = 16\,382.$$

となる。

以上より、m の値はちょうど 2 つであり、それは $m = 2$ と $m = 16\,382$ である。2 つ目の値の検算として、$16\,564^2 - 16\,563^2 = 16\,564 + 16\,563 = 33\,127$ である。

（$n + m$ が負になることも許すならば、a は -184 または $-16\,564$ でもよく、鏡像となる値 $m = -366$ と $m = -16\,746$ が得られる。問題は明らかに $n + m$ が正であることを意図している。）

検算

0 から 16 564 までのすべての m についてコンピュータで直接探索すると、$(182 + m)^2 - 33\,127$ が完全平方数となるのは $m = 2$ と $m = 16\,382$ のときだけであり、33 127 の約数はちょうど $1, 157, 211, 33\,127$ であることがわかる。手計算では、$157 \times 211 = 157 \times 200 + 157 \times 11 = 31\,400 + 1\,727 = 33\,127$ である。

よくある間違い

- 自明な因数分解 $1 \times 33\,127$ を見落とし、m の値を 1 つしか見つけられない。
- 157 と 211 が素数であることを確かめずに主張してしまう。値がちょうど 2 つであるという議論はこの事実に依存している。
- u と v の偶奇（parity）が一致することを確かめない。ここではどちらも奇数なので a と k は整数になるが、4 の倍数でない偶数に対しては、どの因数分解もうまくいかない。

STEP のその先へ

これはフェルマーの因数分解法であり、今回のように N が $\sqrt{N}$ に近い 2 つの因数をもつときにはすばやく機能する。$a^2 - N = k^2$ をちょうど満たすものではなく $a^2 \equiv k^2 \pmod{N}$ を満たすものを見つけるという同じ考え方は、汎用の因数分解アルゴリズムとして最速のものの一つである二次ふるい法（quadratic sieve）の基礎となっている。因数分解と平方の差としての表示との結びつきは、Davenport の *The Higher Arithmetic* で扱われる初等整数論（elementary number theory）への格好の入門となる。

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。