詳細解答

STEP I 2006，第 1 題

純數學 • 平方差

> **STEP I 2006，第 1 題**
>
> 繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：
>
> step.maths.org/questions/06-s1-q1

關鍵思路

若 $(n+m)^2 - 33\,127 = k^2$，則 $33\,127 = (n+m)^2 - k^2$ 是一個平方差（difference of two squares），因此可分解為 $(n+m-k)(n+m+k)$。這正是費馬（Fermat）用來做因式分解（factorisation）的古老技巧：由剛好大於 $\sqrt{N}$ 的整數開始，逐步向上試，直至 $a^2 - N$ 是一個平方數為止。把這個論證倒過來看，33 127 的每一個分解都給出一個 m 的值，所以要數算 m 有多少個值，歸根究底就是數算有多少個分解。

解答

求 n

由於 $180^2 = 32\,400$，33 127 的平方根略大於 180。我們求得

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

所以 $n = 182$。留意 $33\,127 = 182^2 + 3$，所以它本身並不是完全平方數（perfect square）。

一個較小的 m 值

我們依次試 $m = 1, 2, \ldots$：

$$183^2 - 33\,127 = 33\,489 - 33\,127 = 362, \quad \text{不是平方數}(19^2 = 361),$$
$$184^2 - 33\,127 = 33\,856 - 33\,127 = 729 = 27^2.$$

所以 $m = 2$ 可行，此時 $(n+m)^2 - 33\,127 = 27^2$。

分解 33 127

移項後運用平方差公式，

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

所以我們可取 $p = 157$ 和 $q = 211$，兩者均大於 1。

恰好有兩個 m 值

兩個因數都是質數（prime）。對於 157：由於 $13^2 = 169 > 157$，我們只需測試質數 $2, 3, 5, 7, 11$，而當中沒有一個能整除 157。對於 211：由於 $15^2 = 225 > 211$，我們測試 $2, 3, 5, 7, 11, 13$，而當中沒有一個能整除 211。所以 $33\,127 = 157 \times 211$ 就是質因數分解（prime factorisation），而把 33 127 寫成正整數之積 uv（其中 $u \le v$）的方法只有

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

現在假設 $(n+m)^2 - 33\,127 = k^2$，其中 $k \ge 0$。我們取 $a = n + m > 0$，這正是題目所設想的情況（由 n 開始向上走）。於是

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

這裏 $a + k > 0$，所以 $a - k > 0$ 亦成立，而且 $a - k \le a + k$。因此 $(a-k,\, a+k)$ 必定是上面兩對 (u, v) 的其中之一，於是

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

由於 u 和 v 都是奇數，這兩個數都是整數。

想一想 為甚麼每一個分解恰好給出一個 m，又為甚麼不會有其他 m 混進來？

這個對應是雙向的。給定 a 和 k，數對 $(a-k, a+k)$ 就是一個分解；給定一個分解 (u, v)，上面的公式可唯一地還原出 a 和 k。所以 a 的值（因而 $m = a - 182$ 的值）與因數對一一對應（one-to-one correspondence），而因數對恰好有兩個。

- $(u, v) = (157, 211)$ 給出 $a = 184$，$k = 27$，所以 $m = 184 - 182 = 2$，即我們之前找到的值。
- $(u, v) = (1, 33\,127)$ 給出 $a = 16\,564$，$k = 16\,563$，所以

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

因此恰好有兩個 m 值，即 $m = 2$ 和 $m = 16\,382$。驗算第二個值：$16\,564^2 - 16\,563^2 = 16\,564 + 16\,563 = 33\,127$。

（假如我們也容許 $n + m$ 為負數，則 a 可以是 -184 或 $-16\,564$，給出鏡像的值 $m = -366$ 和 $m = -16\,746$。題目的原意顯然是 $n + m$ 為正數。）

驗算

用電腦直接搜尋由 0 至 16 564 的每一個 m，結果發現只有當 $m = 2$ 和 $m = 16\,382$ 時，$(182 + m)^2 - 33\,127$ 才是完全平方數，而且 33 127 的因數恰好是 $1, 157, 211, 33\,127$。用手計算，$157 \times 211 = 157 \times 200 + 157 \times 11 = 31\,400 + 1\,727 = 33\,127$。

常見錯誤

- 忘記了平凡的分解 $1 \times 33\,127$，因而只找到一個 m 值。
- 未經檢查就聲稱 157 和 211 是質數：「恰好有兩個值」這個論證正是建基於此。
- 沒有檢查 u 和 v 的奇偶性（parity）是否相同。這裏兩者都是奇數，所以 a 和 k 都是整數；但若換成一個不是 4 的倍數的偶數，就沒有任何分解可行。

STEP 之外

這就是費馬因式分解法（Fermat's factorisation method），當 N 有兩個接近 $\sqrt{N}$ 的因數時（正如本題），這方法很快見效。同一個想法，即改為尋找 $a^2 \equiv k^2 \pmod{N}$，而非要求 $a^2 - N = k^2$ 嚴格成立，正是二次篩法（quadratic sieve）的基礎，而二次篩法是最快的通用因數分解演算法之一。分解與平方差表示法之間的聯繫，正好讓你初嘗 Davenport 所著 *The Higher Arithmetic*（一本初等數論入門書）中的初等數論（elementary number theory）。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。