详细解答

STEP I 2006，第 1 题

纯数学 · 平方差

> **STEP I 2006，第 1 题**
>
> 继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：
>
> step.maths.org/questions/06-s1-q1

关键思路

若 $(n+m)^2 - 33\,127 = k^2$，则 $33\,127 = (n+m)^2 - k^2$ 是一个平方差（difference of two squares），因此可分解为 $(n+m-k)(n+m+k)$。这正是费马（Fermat）用来做因式分解（factorisation）的古老技巧：由刚好大于 $\sqrt{N}$ 的整数开始，逐步向上试，直至 $a^2 - N$ 是一个平方数为止。把这个论证倒过来看，33 127 的每一个分解都给出一个 m 的值，所以要数算 m 有多少个值，归根究底就是数算有多少个分解。

解答

求 n

由于 $180^2 = 32\,400$，33 127 的平方根略大于 180。我们求得

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

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

一个较小的 m 值

我们依次试 $m = 1, 2, \ldots$：

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

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

分解 $33\,127$

移项后运用平方差公式，

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

所以我们可取 $p = 157$ 和 $q = 211$，两者均大于 1。

恰好有两个 m 值

两个因数都是质数（prime）。对于 157：由于 $13^2 = 169 > 157$，我们只需测试质数 $2, 3, 5, 7, 11$，而当中没有一个能整除 157。对于 211：由于 $15^2 = 225 > 211$，我们测试 $2, 3, 5, 7, 11, 13$，而当中没有一个能整除 211。所以 $33\,127 = 157 \times 211$ 就是质因数分解（prime factorisation），而把 $33\,127$ 写成正整数之积 uv（其中 $u \le v$）的方法只有

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

现在假设 $(n+m)^2 - 33\,127 = k^2$，其中 $k \ge 0$。我们取 $a = n + m > 0$，这正是题目所设想的情况（由 n 开始向上走）。于是

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

这里 $a + k > 0$，所以 $a - k > 0$ 亦成立，而且 $a - k \le a + k$。因此 $(a-k,\, a+k)$ 必定是上面两对 (u, v) 的其中之一，于是

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

由于 u 和 v 都是奇数，这两个数都是整数。

想一想 为甚么每一个分解恰好给出一个 m，又为甚么不会有其他 m 混进来？

这个对应是双向的。给定 a 和 k，数对 $(a-k, a+k)$ 就是一个分解；给定一个分解 (u, v)，上面的公式可唯一地还原出 a 和 k。所以 a 的值（因而 $m = a - 182$ 的值）与因数对一一对应（one-to-one correspondence），而因数对恰好有两个。

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

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

因此恰好有两个 m 值，即 $m = 2$ 和 $m = 16\,382$。验算第二个值：$16\,564^2 - 16\,563^2 = 16\,564 + 16\,563 = 33\,127$。

（假如我们也容许 $n + m$ 为负数，则 a 可以是 -184 或 $-16\,564$，给出镜像的值 $m = -366$ 和 $m = -16\,746$。题目的原意显然是 $n + m$ 为正数。）

验算

用电脑直接搜索由 0 至 16 564 的每一个 m，结果发现只有当 $m = 2$ 和 $m = 16\,382$ 时，$(182 + m)^2 - 33\,127$ 才是完全平方数，而且 33 127 的因数恰好是 $1, 157, 211, 33\,127$。用手计算，$157 \times 211 = 157 \times 200 + 157 \times 11 = 31\,400 + 1\,727 = 33\,127$。

常见错误

- 忘记了平凡的分解 $1 \times 33\,127$，因而只找到一个 m 值。
- 未经检查就声称 157 和 211 是质数：“恰好有两个值”这个论证正是建基于此。
- 没有检查 u 和 v 的奇偶性（parity）是否相同。这里两者都是奇数，所以 a 和 k 都是整数；但若换成一个不是 4 的倍数的偶数，就没有任何分解可行。

STEP 之外

这就是费马因式分解法（Fermat's factorisation method），当 N 有两个接近 $\sqrt{N}$ 的因数时（正如本题），这方法很快见效。同一个想法，即改为寻找 $a^2 \equiv k^2 \pmod{N}$，而非要求 $a^2 - N = k^2$ 严格成立，正是二次筛法（quadratic sieve）的基础，而二次筛法是最快的通用因数分解算法之一。分解与平方差表示法之间的联系，正好让你初尝 Davenport 所著 *The Higher Arithmetic*（一本初等数论入门书）中的初等数论（elementary number theory）。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。