풀이

# STEP I 2006, 문제 1

순수수학 • 두 제곱의 차

> **STEP I 2006, 1번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/06-s1-q1

## 핵심 아이디어

$(n+m)^2 - 33\,127 = k^2$이면 $33\,127 = (n+m)^2 - k^2$은 두 제곱수의 차(difference of two squares)이므로 $(n+m-k)(n+m+k)$로 인수분해(factorisation)된다. 이것은 페르마(Fermat)의 오래된 인수분해 기법이다. $\sqrt{N}$보다 조금 큰 수에서 출발하여 $a^2 - N$이 제곱수가 될 때까지 하나씩 올라간다. 논증을 거꾸로 따라가면 33 127의 인수분해 하나하나가 $m$의 값 하나를 주므로, $m$의 값의 개수를 세는 일은 인수분해의 개수를 세는 일로 귀결된다.

## 풀이

### $n$ 구하기

$180^2 = 32\,400$이므로 33 127의 제곱근은 180보다 조금 크다. 계산하면

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

이므로 $n = 182$이다. $33\,127 = 182^2 + 3$이므로 이 수 자체는 완전제곱수(perfect square)가 아님에 주목하자.

### 작은 $m$의 값

$m = 1, 2, \ldots$을 차례로 대입해 본다.

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

따라서 $m = 2$가 조건을 만족하고, 이때 $(n+m)^2 - 33\,127 = 27^2$이다.

### 33 127의 인수분해

식을 정리하고 두 제곱수의 차를 이용하면

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

이므로 $p = 157, q = 211$로 잡을 수 있고, 둘 다 1보다 크다.

### 정확히 두 개의 $m$의 값

두 인수는 모두 소수(prime)이다. 157의 경우, $13^2 = 169 > 157$이므로 소수 $2, 3, 5, 7, 11$만 확인하면 되는데, 어느 것도 157을 나누지 않는다. 211의 경우, $15^2 = 225 > 211$이므로 $2, 3, 5, 7, 11, 13$을 확인하면 되는데, 어느 것도 211을 나누지 않는다. 따라서 $33\,127 = 157 \times 211$은 소인수분해(prime factorisation)이고, 33 127을 $u \le v$인 양의 정수의 곱 $uv$로 나타내는 방법은

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

뿐이다.

이제 $k \ge 0$에 대하여 $(n + m)^2 - 33\,127 = k^2$이라 하자. $a = n + m > 0$으로 두는데, 이것이 문제가 염두에 둔 상황이다(출발점 $n$에서 위로 올라간다). 그러면

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

이다. 여기서 $a + k > 0$이므로 $a - k > 0$이기도 하고, $a - k \le a + k$이다. 따라서 $(a - k, a + k)$는 위의 두 쌍 $(u, v)$ 중 하나여야 하고, 이때

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

이다. $u$와 $v$가 모두 홀수이므로 이 값들은 정수이다.

> **생각해 보기** 왜 각 인수분해는 정확히 하나의 $m$을 주며, 왜 다른 $m$이 끼어들 수 없을까?

이 대응은 양방향으로 성립한다. $a$와 $k$가 주어지면 쌍 $(a - k, a + k)$는 하나의 인수분해이고, 인수분해 $(u, v)$가 주어지면 위의 공식으로 $a$와 $k$를 유일하게 복원할 수 있다. 따라서 $a$의 값(따라서 $m = a - 182$의 값)은 인수 쌍과 일대일 대응(one-to-one correspondence)을 이루며, 인수 쌍은 정확히 두 개이다.

- $(u, v) = (157, 211)$이면 $a = 184, k = 27$이므로 $m = 184 - 182 = 2$이고, 이는 앞에서 찾은 값이다.
- $(u, v) = (1, 33\,127)$이면 $a = 16\,564, k = 16\,563$이므로

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

이다.

그러므로 $m$의 값은 정확히 두 개이며, 그 값은 $m = 2$와 $m = 16\,382$이다. 두 번째 값을 검산하면 $16\,564^2 - 16\,563^2 = 16\,564 + 16\,563 = 33\,127$이다.

($n + m$이 음수인 경우도 허용한다면 $a$는 $-184$ 또는 $-16\,564$일 수 있고, 이로부터 대칭적인 값 $m = -366$과 $m = -16\,746$을 얻는다. 문제는 분명히 $n + m$이 양수인 경우를 의도하고 있다.)

## 검산

0부터 16 564까지의 모든 $m$에 대해 컴퓨터로 직접 탐색하면 $(182 + m)^2 - 33\,127$이 완전제곱수가 되는 것은 $m = 2$와 $m = 16\,382$일 때뿐이고, 33 127의 약수는 정확히 $1, 157, 211, 33\,127$임을 확인할 수 있다. 손으로 계산하면 $157 \times 211 = 157 \times 200 + 157 \times 11 = 31\,400 + 1\,727 = 33\,127$이다.

## 흔한 실수

- 자명한 인수분해 $1 \times 33\,127$을 빠뜨려서 $m$의 값을 하나만 찾는 것.
- 157과 211이 소수임을 확인하지 않고 주장하는 것. 값이 **정확히** 두 개라는 논증은 이 사실에 의존한다.
- $u$와 $v$의 홀짝성(parity)이 같은지 확인하지 않는 것. 여기서는 둘 다 홀수이므로 $a$와 $k$가 정수이지만, 4의 배수가 아닌 짝수의 경우에는 어떤 인수분해도 성립하지 않는다.

## STEP 너머

이것은 페르마 인수분해법(Fermat's factorisation method)으로, 여기서처럼 $N$이 $\sqrt{N}$에 가까운 두 인수를 가질 때 빠르게 작동한다. $a^2 \equiv k^2 \pmod{N}$을 찾는다는 같은 아이디어(정확히 $a^2 - N = k^2$일 필요는 없다)는 가장 빠른 범용 인수분해 알고리즘 중 하나인 이차 체(quadratic sieve)의 기초이다. 인수분해와 두 제곱수의 차로 나타내는 표현 사이의 연결은 Davenport의 *The Higher Arithmetic*(고등 산술)에 나오는 초등 정수론(elementary number theory)을 처음 맛보기에 좋은 예이다.

Beyond STEP 풀이: https://beyondstep.keithmcnulty.org/ko/. 풀이 글은 CC0 1.0이다. 문제 자체의 저작권은 © Cambridge University Press & Assessment에 있으며 여기에 싣지 않는다. 영어 원문을 기계 번역하였으며 아직 검토되지 않았다.