풀이

STEP I 2014, 문제 1

순수수학 • 제곱의 차

> **STEP I 2014, 1번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/14-s1-q1

핵심 아이디어

모든 것은 하나의 인수분해(factorisation) $a^2 - b^2 = (a-b)(a+b)$에 달려 있다. n을 두 제곱수의 차(difference of two squares)로 나타내는 것은 $d = a - b$, $e = a + b$로 두고 $n = de$로 나타내는 것과 같다. 그리고 d와 e는 짝수 $2b$만큼 차이가 나므로 홀짝성(parity)이 같아야 한다. 이것을 알아차리면 모든 소문항이 홀짝성이 같은 인수쌍(factor pair)에 대한 문제가 된다.

풀이

이 풀이 전체에서 a와 b는 음이 아닌 정수(non-negative integer)이다. $n \geq 1$이고 $n = a^2 - b^2$이면 $a > b$이므로, 한 가지 방법을 언제나 $a > b \geq 0$인 (a, b)로 나타낼 수 있다.

소문항 (i)

$$3 = 2^2 - 1^2, \quad 5 = 3^2 - 2^2, \quad 8 = 3^2 - 1^2, \quad 12 = 4^2 - 2^2, \quad 16 = 5^2 - 3^2.$$

(16의 경우 뻔한 $4^2 - 0^2$는 허용되지 않는다. 제곱수가 0이 아니어야 하기 때문이다.)

소문항 (ii)

연속한 두 제곱수의 차는 홀수이다: $(m+1)^2 - m^2 = 2m + 1$. 따라서 $m \geq 0$인 임의의 홀수 $2m + 1$은

$$2m + 1 = (m+1)^2 - m^2.$$

이다.

소문항 (iii)

2만큼 떨어진 두 수의 제곱의 차는 4의 배수이다: $(k+1)^2 - (k-1)^2 = 4k$. $k \geq 1$이면 $k+1$과 $k-1$이 모두 음이 아니므로

$$4k = (k+1)^2 - (k-1)^2.$$

이다. $k = 0$이면 간단히 $0 = 0^2 - 0^2$ (또는 $1^2 - 1^2$)이다.

소문항 (iv)

모든 제곱수는 4로 나눈 나머지(remainder)가 0 또는 1이다: $(2m)^2 = 4m^2$이고 $(2m+1)^2 = 4(m^2+m)+1$이다. 따라서 $a^2 - b^2$을 4로 나눈 나머지는

$$0-0=0, \quad 1-1=0, \quad 1-0=1 \quad \text{또는} \quad 0-1 \equiv 3 \pmod 4,$$

이고, 결코 2가 아니다. 그러므로 $4k+2$ 꼴의 수는 두 제곱수의 차가 될 수 없다.

(같은 내용을 다르게 말하면 다음과 같다. $(a-b)(a+b) = 4k+2$이면 $a-b$와 $a+b$는 홀짝성이 같다. 둘 다 홀수이면 곱이 홀수이고, 둘 다 짝수이면 곱이 4로 나누어떨어진다. 어느 경우도 $4k+2$가 아니다.)

소문항 (v)

$a > b \geq 0$이고 $pq = a^2 - b^2 = (a-b)(a+b)$라 하자. $d = a-b$, $e = a+b$로 두자. 그러면 d와 e는 $d \leq e$이고 $de = pq$인 양의 정수이다. 역으로, $d \leq e$이고 d, e의 홀짝성이 같은 인수분해 $pq = de$는 각각 정확히 한 가지 방법을 준다. 곧

$$a = \frac{e+d}{2}, \qquad b = \frac{e-d}{2},$$

이고, 이들은 음이 아닌 정수이다. 따라서 pq를 나타내는 방법들은 이러한 인수쌍 (d,e)와 일대일 대응(one-to-one correspondence)을 이룬다.

? **생각해 보기** 여기서 d와 e의 홀짝성은 왜 항상 같을까? 그리고 왜 인수쌍이 두 개뿐일까?

p와 q가 홀수 소수(odd prime)이므로 pq는 홀수이고, 따라서 pq의 모든 약수(divisor)가 홀수이므로 홀짝성 조건은 저절로 성립한다. $p \leq q$라 하자. 소인수분해의 유일성(unique factorisation)에 의해 $d \leq e$인 인수쌍은

$$(d,e) = (1, pq) \qquad \text{그리고} \qquad (d,e) = (p,q).$$

뿐이다. ($p = q$일 때에도 이는 여전히 참이다. p^2의 약수는 1, p, p^2이다.) 이들로부터

$$pq = \left(\frac{pq+1}{2}\right)^2 - \left(\frac{pq-1}{2}\right)^2 \qquad \text{그리고} \qquad pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{q-p}{2}\right)^2.$$

을 얻는다. 두 방법의 $d = a - b$ 값은 각각 1과 p이고 $p \geq 3$이므로, 두 방법은 서로 다르다. 따라서 pq를 두 제곱수의 차로 나타내는 방법은 정확히 두 가지이다. 예를 들어 $15 = 8^2 - 7^2 = 4^2 - 1^2$이다. $p = q$일 때 두 번째 방법은 $p^2 - 0^2$인데, 0이 아닌 제곱수를 요구하는 것은 소문항 (i)뿐이므로 여기서는 허용된다.

$q = 2$일 때에는 이 결과가 성립하지 **않는다**. 이때 $pq = 2p$이고 p는 홀수이므로 $p = 2m + 1$로 두면 $2p = 4m + 2$이다. 소문항 (iv)에 의해 $2p$는 어떤 방법으로도 두 제곱수의 차로 나타낼 수 없다. (인수쌍 $(1, 2p)$와 $(2, p)$는 각각 하나는 홀수, 하나는 짝수이다.)

소문항 (vi)

소문항 (v)에서처럼 675를 나타내는 방법들은 $d \leq e$이고 d, e의 홀짝성이 같은 인수쌍 $675 = de$와 대응한다. 675는 홀수이므로 모든 약수가 홀수이고, 따라서 모든 인수쌍이 해당된다.

이제 $675 = 27 \times 25 = 3^3 \times 5^2$이므로 약수는 $(3+1)(2+1) = 12$개이다. 이들은 $d \leftrightarrow 675/d$로 짝지어지며, 675는 완전제곱수(perfect square)가 아니므로($26^2 = 676$) 자기 자신과 짝지어지는 약수는 없다. 따라서 인수쌍은 $12/2 = 6$개이다:

(d, e)	$(1, 675)$	$(3, 225)$	$(5, 135)$	$(9, 75)$	$(15, 45)$	$(25, 27)$
(a, b)	$(338, 337)$	$(114, 111)$	$(70, 65)$	$(42, 33)$	$(30, 15)$	$(26, 1)$

그러므로 675를 두 제곱수의 차로 나타내는 서로 다른 방법은 정확히 **6**가지이다.

> ? **생각해 보기** (a, b)와 $(-a, b)$, 또는 $a^2 - b^2$과 $-(b^2 - a^2)$을 서로 다른 방법으로 세어야 할까?

그렇지 않다. 문제에서 모든 수를 음이 아닌 정수로 제한했고, $a^2 - b^2 = 675 > 0$이므로 $a > b$일 수밖에 없다. 따라서 각 방법은 $a > b \geq 0$인 하나의 순서쌍 (a, b)이며, 우리가 센 것이 바로 이것이다.

검산

- 표의 일부를 확인해 보자: $26^2 - 1^2 = 676 - 1 = 675$이고 $30^2 - 15^2 = 900 - 225 = 675$이다.
- 소문항 (ii)–(iv)를 종합하면, $n \geq 1$이 두 제곱수의 차가 될 필요충분조건은 $n \not\equiv 2 \pmod 4$이다. 2000 이하의 모든 n에 대해 컴퓨터로 확인한 결과도 이와 일치하며, $p \leq q < 200$인 모든 홀수 소수에 대해 pq의 표현이 정확히 두 가지이고 $2p$의 표현은 하나도 없음을 확인한 결과도 마찬가지이다.
- 모든 b에 대해 탐색하면 675의 표현은 정확히 여섯 가지, 곧 표에 있는 여섯 가지가 나온

다.

흔한 실수

- 홀짝성 조건을 잊는 것: $2p$에 대해 $(2, p)$와 같은 쌍을 세면 정수가 아닌 $a = \frac{p+2}{2}$가 나온다.
- 소문항 (v)에서 $p = q$인 경우를 빠뜨리거나, 그 경우의 $p^2 - 0^2$을 제외하는 것. 소문항 (i) 밖에서는 0이 허용된다.
- 소문항 (vi)에서 인수쌍의 개수(6) 대신 약수의 개수(12)를 세는 것.

STEP 너머

표현의 개수가 n의 약수에 의해 결정된다는 이 패턴은 초등 정수론(elementary number theory)의 전형적인 모습이다. 이와 관련된 유명한 결과로 두 제곱수의 합에 관한 페르마(Fermat)의 정리가 있다. 홀수 소수가 $x^2 + y^2$ 꼴이 될 필요충분조건은 그 수가 $1 \bmod 4$인 것이며, 이 명제는 가우스 정수(Gaussian integer) $a + bi$를 이용하여 깔끔하게 증명된다. 더 알고 싶다면 Davenport의 *The Higher Arithmetic*(고등 산술)을 읽어 보라.

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.