풀이

# STEP III 견본 문제지, 문제 10

순수수학 • 모듈러 산술

> **STEP III 견본 문제지, 10번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/spec-s3-q10

## 핵심 아이디어

두 소문항 모두 나머지에 관한 문제이므로, 잘 고른 수를 법(modulo)으로 하여 생각한다. (i)에서는 제곱수가 8을 법으로 할 때 가질 수 있는 값이 몇 개뿐이고, 그 값 세 개를 더해서는 결코 7이 될 수 없다. (ii)에서는 거듭제곱을 다시 써서 두 항이 17을 법으로 같은 밑을 갖도록 만든다. 그러면 두 계수의 합이 17의 배수가 된다.

## 풀이

### 소문항 (i)

**홀수의 제곱.** 홀수를 $2k+1$로 쓴다. 여기서 $k$는 정수이다. 그러면

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

연속한 두 정수 $k$와 $k+1$ 중 하나는 짝수이므로 $k(k+1)$은 짝수이고, 따라서 $4k(k+1)$은 8의 배수이다. 그러므로 모든 홀수의 제곱은 8로 나눈 나머지가 1이다.

**짝수의 제곱.** 짝수를 $2k$로 쓴다. 그러면 $(2k)^2 = 4k^2$이다.

- $k$가 짝수이면, 즉 $k = 2j$이면 $4k^2 = 16j^2$은 8의 배수이다: 나머지는 0이다.
- $k$가 홀수이면 $k^2$도 홀수이므로 $k^2 = 2j+1$이라 하면 $4k^2 = 8j + 4$이다: 나머지는 4이다.

따라서 모든 짝수의 제곱은 8로 나눈 나머지가 0 또는 4이다.

**결론 이끌어 내기.** 모든 제곱수는 8을 법으로 0, 1, 4 중 하나와 합동(congruent)이다. (여기에는 $0^2 = 0$도 포함되므로, 세 제곱수 중 일부가 0인 경우도 허용하고 있는 것이다.) $N = a^2 + b^2 + c^2$이라 하자. 그러면 $N$ mod 8은 각각 $\{0, 1, 4\}$에서 고른 세 수의 합을 8로

나눈 나머지이다. 그중 4인 것이 몇 개인지에 따라 분류하면 다음과 같다.

| 4의 개수 | 나머지 수들의 가능한 합, 그리고 전체 합의 mod 8 값 |
|---|---|
| 0 | $0, 1, 2, 3$ |
| 1 | $4 + \{0, 1, 2\} = 4, 5, 6$ |
| 2 | $8 + \{0, 1\} \equiv 0, 1$ |
| 3 | $12 \equiv 4$ |

가능한 나머지는 $0, 1, 2, 3, 4, 5, 6$이고, 7은 결코 나타나지 않는다. $8n + 7$ 꼴의 수는 8로 나눈 나머지가 7이므로, 세 제곱수의 합이 될 수 없다.

> **생각해 보기** 그냥 7 자체가 세 제곱수의 합이 아님을 확인하면 안 되는 이유는 무엇인가?

주장이 $7, 15, 23, \ldots$처럼 무한히 많은 수에 관한 것이어서, 하나씩 확인해서는 결코 끝나지 않기 때문이다. 8을 법으로 생각하면 이들을 한꺼번에 다룰 수 있다. $a$, $b$, $c$가 무엇이든 그 나머지만 중요하며, 위의 표가 모든 경우를 다 포함한다.

**소문항 (ii)**

각 항이 상수와 $n$제곱의 곱이 되도록 거듭제곱을 떼어 낸다.

$$2^{3n+1} = 2 \cdot 8^n, \qquad 3\left(5^{2n+1}\right) = 15 \cdot 25^n.$$

이제 $25 = 17 + 8$이므로 $25 \equiv 8 \pmod{17}$이고, 따라서 모든 $n \geq 0$에 대하여 $25^n \equiv 8^n \pmod{17}$이다(합동식은 서로 곱할 수 있다). 그러므로

$$\begin{aligned} 2^{3n+1} + 3\left(5^{2n+1}\right) &= 2 \cdot 8^n + 15 \cdot 25^n \\ &\equiv 2 \cdot 8^n + 15 \cdot 8^n \\ &= 17 \cdot 8^n \equiv 0 \pmod{17}. \end{aligned}$$

따라서 요구한 대로, 모든 정수 $n \geq 0$에 대하여 17은 $2^{3n+1} + 3(5^{2n+1})$을 나눈다.

> **생각해 보기** 합동식을 배운 적이 없다면 어떻게 하는가?

같은 아이디어를 수학적 귀납법(induction)으로도 쓸 수 있다. $f(n) = 2 \cdot 8^n + 15 \cdot 25^n$이라 하자. 그러면 $f(0) = 17$이고,

$$f(n+1) - 8f(n) = 15 \cdot 25^{n+1} - 15 \cdot 8 \cdot 25^n = 15 \cdot 25^n(25 - 8) = 17 \cdot 15 \cdot 25^n,$$

이므로 $f(n+1) = 8f(n) + 17 \cdot 15 \cdot 25^n$이다. $17 \mid f(n)$이면 $17 \mid f(n+1)$이므로, 수학적 귀납법에 의해 결과가 성립한다.

## 검산

작은 경우를 확인해 본다. $7 = 4+1+1+1$은 제곱수가 네 개 필요하고, $15 = 9+4+1+1$도 네 개가 필요하다. 반면 $6 = 4+1+1$과 $14 = 9+4+1$은 세 개로 충분하다. 컴퓨터로 탐색해 보면 5000 이하의 $8n+7$ 꼴의 수 중 세 제곱수의 합인 것은 하나도 없음을 확인할 수 있다. (ii)의 경우: $n = 0$이면 $2+15 = 17$이고, $n = 1$이면 $16+375 = 391 = 17\times 23$이다. 0부터 299까지의 모든 $n$에 대하여 이 식이 17로 나누어떨어짐을 확인하였다.

## 흔한 실수

- 0도 제곱수라는 사실을 잊는 것. 따라서 "세 제곱수의 합"이 실제로는 0이 아닌 제곱수를 한두 개만 쓸 수도 있다. 위의 논증은 0이 나머지(residue) 중 하나이므로 이 경우를 자동으로 포함한다.
- "$4k^2+4k$가 4로 나누어떨어지므로" 홀수의 제곱이 1 mod 8이라고 말하는 것. 이것으로는 1 mod 4밖에 얻지 못한다. $k(k+1)$에서 나오는 인수 2가 필요하다.

## STEP 너머

소문항 (i)은 르장드르(Legendre)의 세 제곱수 정리(three-square theorem)의 쉬운 절반이다. 이 정리는 양의 정수가 $4^a(8n+7)$ 꼴이 아닐 **때, 그리고 그때에만** 세 제곱수의 합이 된다는 것이다. 역방향은 훨씬 어려우며 이차 형식(quadratic form) 이론이 필요하다. 이와 대조적으로 라그랑주(Lagrange)는 **모든** 양의 정수가 네 제곱수의 합임을 증명하였다. 소문항 (ii)는 $\mathbb{Z}/17\mathbb{Z}$에서의 일상적인 산술이며, 대학 1학년 과정에서는 이를 군(group)과 환(ring)의 연구로 발전시킨다. Davenport의 *The Higher Arithmetic*(고등 산술)은 합동식과 제곱수의 합을 훌륭하게 다룬다.

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.