풀이

STEP I 2016, 문제 7

순수수학 • 4를 법으로 하는 인수분해

> **STEP I 2016, 7번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/16-s1-q7

이 문제는 *Beyond STEP*의 1.7 절 **인수분해가 무너질 때**에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch01/factorisation-fails.html

핵심 아이디어

모든 것은 법(modulo) 4로 계산하는 데서 나온다. 홀수는 $\equiv 1$이거나 $\equiv 3 \equiv -1 \pmod 4$이므로, 홀수들의 곱은 T에서 온 인수가 짝수 개인지 홀수 개인지에 따라 S 또는 T에 속한다. 이 홀짝성(parity) 규칙 하나로 (ii), (iii), (iv)(a)가 해결된다. (iv)(b)에서는 S-소수가 소수일 필요가 없다는 것을 알아차려야 하며, 그 결과 소인수분해의 유일성(unique factorisation)이 깨진다.

풀이

소문항 (i)

모든 양의 홀수는 4로 나눈 나머지가 1 또는 3이고, 짝수는 그렇지 않다. 따라서 $S \cup T$는 모든 양의 홀수의 집합이다. 어떤 정수도 서로 다른 두 나머지를 가질 수 없으므로 $S \cap T$는 공집합(*empty set*)이다.

소문항 (ii)

$a, b \geq 0$인 정수에 대하여 S의 원소 $4a+1$과 $4b+1$을 잡자. 그러면

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1,$$

이고, 이는 나머지가 1인 양의 정수이므로 S에 속한다.

T에 대해서는 답이 **아니다**이다. 예를 들어 $3 \in T$이지만 $3 \times 3 = 9 = 4 \times 2 + 1 \in S$이고, $S \cap T$는 공집합이다. 사실 이는 항상 일어난다.

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1 \in S.$$

섞인 곱도 필요하다.

$$(4a+1)(4b+3) = 16ab + 12a + 4b + 3 = 4(4ab + 3a + b) + 3 \in T.$$

요컨대 T의 수를 $\equiv -1 \pmod 4$로 쓰면, 홀수들의 곱은 $\equiv (-1)^k \pmod 4$이다. 여기서 k는 T에서 온 인수의 개수이다. 따라서 k가 짝수이면 곱은 S에, k가 홀수이면 T에 속한다.

소문항 (iii)

$n \in T$를 합성수(composite)라 하고, $n = p_1 p_2 \cdots p_r$를 소수(prime)들의 곱으로 나타내자. n이 홀수이므로 모든 p_i는 홀수이고, 따라서 (i)에 의해 각 p_i는 S 또는 T에 속한다.

귀류법(proof by contradiction)으로, 모든 p_i가 S에 속한다고 가정하자. (ii)를 반복해서 적용하면 $p_1 p_2 \in S$, 그다음 $(p_1 p_2)p_3 \in S$, 이런 식으로 계속하여 $n \in S$이다. 그런데 $n \in T$이고 $S \cap T = \varnothing$이므로 모순이다. 따라서 n의 소인수 중 적어도 하나는 T에 속한다. (홀짝성으로 말하면, $n \equiv -1$이 되려면 $\equiv -1$인 인수가 홀수 개, 따라서 적어도 하나 있어야 한다.)

소문항 (iv)(a)

먼저 $1 \notin T$이므로 T의 모든 원소는 3 이상임에 주목하자.

모든 $n \in T$는 T-소수이거나 T-소수들의 곱이다. n에 대한 강한 귀납법(strong induction)을 쓴다. n이 T-소수이면 끝이다. 그렇지 않으면 $k \geq 2$이고 각 $t_i \in T$인 $n = t_1 t_2 \cdots t_k$로 쓸 수 있다. 각 $t_i \geq 3$이므로 각 $t_i \leq n/3 < n$이고, 귀납 가정(induction hypothesis)에 의해 각 t_i는 T-소수이거나 T-소수들의 곱이다. 이것들을 $n = t_1 \cdots t_k$에 대입하면 n이 T-소수들의 곱으로 표현된다.

> **생각해 보기** T-소수들의 곱을 얻었는데, 왜 그 개수가 반드시 **홀수**여야 할까?

모든 T-소수는 T에 속하므로 $\equiv -1 \pmod 4$이다. 따라서 (ii)의 끝에서 얻은 규칙에 의해 이런 수 m개의 곱은 $\equiv (-1)^m \pmod 4$이다. 만약 m이 짝수라면 곱은 $\equiv 1$이 되어 T가 아니라 S에 속할 것이다. 곱이 $n \in T$이므로 m은 홀수이다. 따라서 모든 $n \in T$는 T-소수이거나 홀수 개의 T-소수의 곱이며, 이것이 보이려던 것이다.

T-소수가 소수일 필요는 없다는 점에 주의하자. $15 = 3 \times 5$는 T-소수인데, $5 \notin T$이고 1보다 큰 수들로의 유일한 인수분해가 3×5이기 때문이다.

소문항 (iv)(b)

15에 대한 앞의 관찰과 같은 아이디어가 S에서도 통한다. T에 속하는 두 소수의 곱은 S에 속하지만 S 안에서는 인수분해되지 않는다. 다음을 보자.

$$9 = 3 \times 3, \qquad 21 = 3 \times 7, \qquad 49 = 7 \times 7.$$

각각은 S에 속한다. 또 각각은 S-소수이다. 1과 자기 자신 이외의 약수는 3 또는 7뿐인데, 이들은 S가 아니라 T에 속하기 때문이다. (21의 약수는 $1, 3, 7, 21$이다.) 이제

$$441 = 9 \times 49 = 21 \times 21,$$

이고 $441 = 4 \times 110 + 1 \in S$이다. 이 둘은 441을 S-소수들로 인수분해하는 진짜로 서로 다른 두 방법이다. 첫 번째는 9와 49를 쓰고, 두 번째는 21을 두 번 쓴다. 따라서 441이 구하는 예이다.

생각해 보기 이 예를 어떻게 찾을 수 있었을까?

보통의 정수에서 $441 = 3^2 \times 7^2$이고, 소수 $3, 7$은 T에 속한다. S 안에서는 3이나 7 하나만 따로 떼어 낼 수 없으므로, T에 속하는 소수들을 둘씩 짝지어야 한다. 3이 두 개, 7이 두 개 있으면 짝짓는 방법은 $(3 \cdot 3)(7 \cdot 7)$ 또는 $(3 \cdot 7)(3 \cdot 7)$의 두 가지이다. 서로 다른 소수 $p, q \in T$에 대한 임의의 p^2q^2도 같은 방식으로 통하며, 예를 들어 $9 \times 121 = 33 \times 33$이다.

검산

- 작은 경우를 확인해 보자. $5 \times 9 = 45 \in S, 3 \times 7 = 21 \in S, 5 \times 7 = 35 \in T$.
- (iii)에 대하여: $15 = 3 \times 5$와 $35 = 5 \times 7$은 T에 속하고, 각각 T에 속하는 소인수$(3, 7)$를 가진다.
- 컴퓨터로 확인하면, 3000 미만의 모든 $n \in T$에 대하여 T-소수들로의 모든 인수분해는 인수의 개수가 홀수이다. T-소수는 $3, 7, 11, 15, 19, 23, 31, 35, \ldots$로 시작한다. $27 = 3 \times 3 \times 3$은 T-소수가 아님에 주의하자. 인수가 세 개, 즉 홀수 개이다.

흔한 실수

- 한 가지 경우도 확인해 보지 않고 T의 두 원소의 곱이 T에 속한다고 주장하는 것. $3 \times 3 = 9$ 하나로 곧바로 결론이 난다.
- X-소수가 소수일 필요가 없다는 것을 잊는 것. 이것이 (iv)(b)의 요점 전부이다. 9와 21은 S-소수이다.

- (iv)(a)에서 인수의 개수가 홀수라는 것만 증명하고, T-소수들로의 인수분해가 애초에 존재한다는 것을 보이는 일을 잊는 것.

STEP 너머

집합 S는 곱셈에 대하여 닫혀 있고(closed under multiplication), 그 "소수"들은 유일하게 인수분해되지 않는다. 이것은 $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$가 성립하는 $\mathbb{Z}[\sqrt{-5}]$ 같은 환(ring)에서 무엇이 잘못되는지를 보여 주는 고전적인 장난감 모형(힐베르트(Hilbert) 수(Hilbert numbers)라고도 부른다)이다. 이런 환에서 소인수분해의 유일성을 되살리려는 시도가 아이디얼(ideal)과 대수적 정수론(algebraic number theory)으로 이어졌다. Davenport의 *The Higher Arithmetic*(고등 산술)은 $\mathbb{Z}$에서 소인수분해의 유일성이 왜 증명이 필요한 정리(theorem)인지 설명하고, Allenby의 *Rings, Fields and Groups*(환, 체, 군)는 그것이 성립하지 않는 환들을 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.