1.7 인수분해가 무너질 때

학습지

문제

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

힌트

먼저 혼자 힘으로 문제를 풀어 보자. 막히면 힌트를 **하나씩** 읽고, 힌트를 하나 읽을 때마다 다시 문제로 돌아가자. **잠깐, 직접 해 보기**라고 표시된 힌트가 핵심 단계이다. 각 힌트 뒤에는 풀이를 적을 공간이 있다.

생각해 보기 S와 T의 처음 몇 원소를 나열해 보자. 소문항 (iv)의 정의에 따르면 S의 원소 중 어느 것이 S-소수인가?

1단계 합집합, 교집합과 곱

다루는 내용: 소문항 (i), (ii)

생각해 보기 S와 T의 원소를 4로 나눈 나머지는 각각 무엇인가? 어떤 양의 정수가 그런 나머지를 가질 수 있는가?

생각해 보기 $(4a+1)(4b+1)$을 전개하여 그 결과를 $4\times(\text{어떤 수})+1$의 꼴로 나타내 보자.

잠깐, 직접 해 보기 T에 대해서는 3×3과 같은 작은 예를 시도해 보자. 뒤의 소문항에서 쓰이므로 $(4a+3)(4b+3)$과 $(4a+1)(4b+3)$도 미리 계산해 두는 것이 좋다.

2단계 T에 속하는 소인수

다루는 내용: 소문항 (iii)

생각해 보기 T에 속하는 수의 소인수(prime factor)는 모두 홀수이므로, 각 소인수는 S 또는 T에 속한다.

잠깐, 직접 해 보기 모든 소인수가 S에 속한다면 어떻게 되는가? 소문항 (ii)를 반복해서 사용해 보자.

3단계 홀수 개의 인수

다루는 내용: 소문항 (iv)(a)

생각해 보기 T의 모든 원소는 3 이상이다. 강한 귀납법(strong induction)을 사용하여 각 $n \in T$가 T-소수이거나 T-소수들의 곱임을 보여라.

잠깐, 직접 해 보기 곱에 나타나는 T-소수의 개수는 왜 홀수여야 하는가? T의 원소를 짝수 개 곱한 수를 4로 나눈 나머지가 무엇인지 생각해 보자.

4단계 두 가지 인수분해

다루는 내용: 소문항 (iv)(b)

생각해 보기 15는 T-소수인가? 소수인가? S에서도 같은 일이 일어날 수 있다. S의 원소 중 T에 속하는 보통의 소수 두 개의 곱인 것은 무엇인가?

잠깐, 직접 해 보기 T에 속하는 소수 두 개, 예를 들어 3과 7을 택하자. 각각을 두 개씩 가지고 있을 때, 이들을 둘씩 짝지어 S의 원소를 만드는 방법은 몇 가지인가?

숨은 수학

정수는 무엇이 특별한가

보통의 정수에서는 왜 인수분해가 잘 되는 것일까? 핵심이 되는 사실은 **유클리드의 보조정리**(Euclid's lemma)이다. 소수 p가 곱 ab를 나누면, p는 a를 나누거나 p는 b를 나눈다. 이 보조정리는 유클리드 호제법(Euclidean algorithm)을 이용하여 증명하며, 바로 이것이 S에서 성립하지 않는다. 거기서는 S-소수 9가 $21 \times 21 = 441$을 나누지만($441 = 9 \times 49$이므로), 9는 21을 S 안에서 나누지 않는다. 대학 1학년 때 유클리드의 보조정리를 엄밀하게 증명하고, 유일 인수분해가 그로부터 따라 나온다는 것을 보게 될 것이다.

페르마의 마지막 정리의 실패한 증명

1847년 3월 1일, 가브리엘 라메(Gabriel Lamé)는 파리 과학 아카데미(Paris Academy)에서 페르마의 마지막 정리를 증명했다고 발표했다. 그의 아이디어는 복소수 단위근(roots of unity)을 이용하여 $x^n + y^n$을

$$x^n + y^n = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y), \qquad \zeta = e^{2\pi i/n}$$

(단, n은 홀수)과 같이 인수분해한 다음, 각 괄호의 소인수에 대해 논증하는 것이었다. 조제프 리우빌(Joseph Liouville)은 곧바로 이의를 제기했다. ζ로 만들어진 수들이 왜 유일하게 인수분해되어야 하는가? 몇 주 뒤, 에른스트 쿠머(Ernst Kummer)가 그런 수들이 유일하게 인수분해되지 않는 경우가 많다는 것을 이미 보였다는 사실이 밝혀졌다. 처음으로 실패하는 경우는 $n = 23$이다.

쿠머는 유일 인수분해를 회복시켜 주는 새로운 대상인 "아이디얼 수(ideal numbers)"를 고안하여 살릴 수 있는 것을 살려 냈고, 매우 많은 지수에 대해 페르마의 마지막 정리를 증명했다. 리하르트 데데킨트(Richard Dedekind)는 쿠머의 아이디얼 수를 현대 대수학의 핵심 개념 중 하나인 **아이디얼**(ideal)로 발전시켰다.

기억해 둘 만한 더 작은 예

수 체계 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$에서는

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

이고, 네 인수는 모두 그 체계에서 "소수"이다(연습문제 3). 이를 인수분해가 **실제로** 유일한 Section 1.6의 가우스 정수(Gaussian integers)와 비교해 보자. 이런 종류의 체계 중 어떤 것에서 유일 인수분해가 성립하는지는 깊은 문제이다. 가우스(Gauss)는 $\mathbb{Z}[\sqrt{-d}]$ 꼴의 체계와 그와 가까운 체계들 가운데 이 성질을 가지는 것은 아홉 개뿐이라고 추측했다. 이 추측은 1952년부터 1967년 사이에 Heegner, Baker, Stark에 의해 마침내 증명되었다.

더 도전하기

---

1 **또 다른 예.** 693이 S-소수로의 인수분해를 서로 다른 두 가지로 가짐을 보여라. 이런 예를 만들어 내는 일반적인 방법을 찾을 수 있는가?

2 **짝수.** $E = \{2, 4, 6, 8, \ldots\}$라 하자. 어떤 수가 E-소수인가? 60이 E-소수로의 인수분해를 두 가지 이상 가짐을 보여라.

3 $\mathbb{Z}[\sqrt{-5}]$. **노름**(norm)을 $N(a + b\sqrt{-5}) = a^2 + 5b^2$으로 정의하자. $N(zw) = N(z)N(w)$임을 보여라. 노름이 2 또는 3인 원소가 없음을 보여서, 2, 3, $1 \pm \sqrt{-5}$가

$\mathbb{Z}[\sqrt{-5}]$에서 더 이상 인수분해되지 않음을 유도하라.

4 **유클리드의 보조정리 활용.** 심화 유클리드의 보조정리(소수가 ab를 나누면 그 소수는 a 또는 b를 나눈다)를 가정하고, 1보다 큰 모든 정수는 인수의 순서를 무시하면 소수로의 인수분해를 단 하나만 가짐을 증명하라.

더 읽을거리

- **Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem*** (CRC Press). 앞부분의 장들에서 라메, 쿠머, 아이디얼의 이야기를 의욕 있는 대학 1학년 학생이 따라갈 수 있는 수준으로 들려준다.
- **John Stillwell, *Elements of Number Theory***. 정수와 가우스 정수에서의 유일 인수분해를 나란히 비교한다.
- **Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction*** (Springer). 야심 있는 독자를 위한 책으로, 쿠머의 업적을 그 역사를 통해 설명한다.

안내에 따른 전체 풀이는 제 1.7절에 있다:

https://beyondstep.keithmcnulty.org/ko/ch01/factorisation-fails.html

매주 STEP 문제 하나를 끝까지 풀어 본다. The STEP Up은 이메일로 무료로 받아 볼 수 있다: keithmcnulty.substack.com