7.8 네 제곱수

학습지

> 문제
>
> **STEP III 1994, 8번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/94-s3-q8

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** 두 제곱수 버전을 떠올려 보자. 복소수 $z = a + bi$, $w = p + qi$에 대하여 $|z|^2|w|^2 = |zw|^2$이므로 $(a^2 + b^2)(p^2 + q^2)$은 두 제곱수의 합이다. 행렬을 이용하면 이것을 어떻게 네 제곱수로 확장할 수 있을까?

1단계 행렬식은 네 제곱수의 합이다

다루는 내용: 각 행렬의 행렬식

? **생각해 보기** $\begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix}$의 행렬식(determinant)을 계산해 보아라. 복소수 z에 대하여 zz^*는 무엇인가?

2단계 곱도 같은 꼴이다

다루는 내용: 두 행렬의 곱

> **잠깐, 직접 해 보기** 두 행렬을 곱하여라. 곱의 윗줄을 (w_1, w_2)라 하자. 아랫줄은 $(-w_2^*, w_1^*)$인가? 그다음 양변의 행렬식을 구하여라.

3단계 네 제곱수 읽어 내기

다루는 내용: L_1, L_2, L_3, L_4 구하기

> **생각해 보기** w_1과 w_2를 a, b, c, d, p, q, r, s로 전개하고, 각각을 실수부(real part)와 허수부(imaginary part)로 나누어라. 이 네 부분이 바로 구하는 L들이다.

숨은 수학

라그랑주의 네 제곱수 정리

라그랑주의 증명의 개요는 다음과 같다. 오일러의 항등식에 의해 모든 소수 p가 네 제곱수의 합임을 보이면 충분하다. 개수 세기 논법으로 $m < p$인 어떤 배수 mp가 네 제곱수의 합임을 보인다. 그다음 교묘한 "강하법(descent)"으로, $1 < m < p$인 mp가 네 제곱수의 합

이면 더 작은 어떤 m'에 대하여 $m'p$도 네 제곱수의 합임을 보인다. 이를 반복하면 $m = 1$에 도달한다. (Section 1.5의 페르마의 강하법과 비교해 보아라.) 1834년 야코비(Jacobi)는 훨씬 더 나아가 n을 네 제곱수의 합으로 나타내는 방법의 정확한 개수를 구하였다. 그 개수는 n의 약수(divisor) 중 4의 배수가 아닌 것들의 합의 8배이다. 예를 들어 1은 8가지 방법으로 나타낼 수 있다(네 자리 중 어느 한 곳에 ± 1).

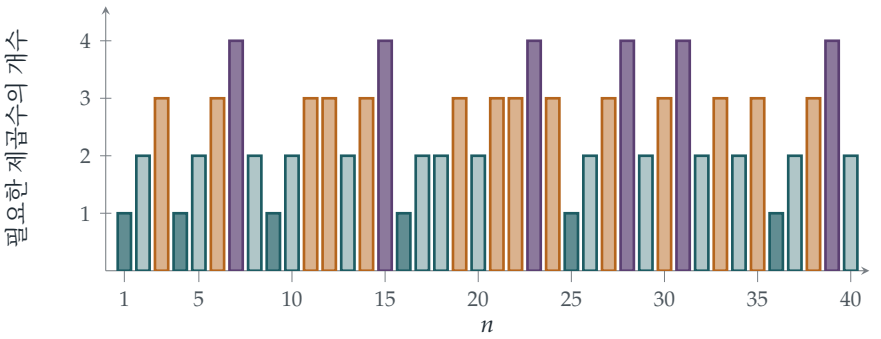

그림 7.8.1 1부터 40까지의 각 n을 만드는 데 필요한 제곱수의 최소 개수. 라그랑주의 정리에 의해 모든 수는 많아야 네 개면 된다. 네 개가 필요한 수(자주색)는 $7, 15, 23, 28, 31, 39, \ldots$이며, 르장드르(Legendre)와 가우스(Gauss)의 정리에 의해 정확히 $4^k(8m+7)$ 꼴의 수들이다.

둘, 셋, 넷

차원에 따른 양상은 미묘하다. 두 제곱수의 합은 복소수에서 나오며, 어떤 수가 두 제곱수의 합일 필요충분조건은 그 수의 $4k+3$ 꼴인 소인수가 모두 짝수 거듭제곱으로 나타나는 것이다(Section 1.6). 네 제곱수의 합은 사원수에서 나오며, 모든 수가 네 제곱수의 합이다. 그러나 세 제곱수의 합에는 곱셈 항등식이 전혀 없으며(크기가 곱셈적인 3차원 수 체계는 존재하지 않는다. 해밀턴(Hamilton)이 세 쌍으로 실패한 이유가 이것이다. Section 6.7 참고), 정리도 더 어렵다. 르장드르와 가우스는 $n = 4^k(8m+7)$이 아닌 한 n이 세 제곱수의 합임을 보였다(그림 7.8.1). 넷을 넘어서면 8차원의 팔원수(octonion)가 여덟 제곱수 항등식을 주는데, 이는 Degen과 Graves가 발견하였다. 후르비츠(Hurwitz)는 1898년에 이런 종류의 항등식이 1, 2, 4, 8개의 제곱수에 대해서만 존재함을 증명하였다.

워링의 문제

라그랑주의 정리는 1770년 워링(Edward Waring)이 제기한 질문의 첫 번째 경우이다. 각 k에 대하여, 모든 양의 정수가 많아야 $g(k)$개의 k제곱수의 합이 되는 수 $g(k)$가 존재하는가? 힐베르트(David Hilbert)는 1909년에 그러한 수가 존재함을 증명하였다. 오늘날 우리는 $g(2) = 4$, $g(3) = 9$(예를 들어 $23 = 2 \cdot 2^3 + 7 \cdot 1^3$은 세제곱수 아홉 개가 필요하다),

$g(4) = 19$임을 알고 있다.

더 도전하기

1 **계산 예제.** $(a,b,c,d) = (p,q,r,s) = (2,1,1,1)$로 두고 $L_1,\dots,L_4$의 공식을 이용하여 $49 = 7\times 7$을 네 제곱수의 합으로 나타내고, 답을 확인하여라. 이것은 자명한 $49 = 7^2+0^2+0^2+0^2$과 같은가?

2 **넷 속의 둘.** $c = d = r = s = 0$이면 이 항등식이 Section 1.6의 두 제곱수 항등식으로 줄어듦을 보여라.

3 **네 제곱수가 필요한 수.** 제곱수를 8로 나눈 나머지를 생각하여, $8m+7$ 꼴의 수는 세 제곱수의 합이 될 수 없음을 보여라.

4 **야코비의 공식.** 2를 네 제곱수의 합으로 나타내는 방법(순서와 부호를 구별한다)의 수를 세고, 그 답이 $8\times(1+2) = 24$임을 확인하여라.

더 읽을거리

- **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press). 제 V장에서 라그랑주의 네 제곱수 정리를 증명한다.
- **John Conway & Derek Smith, *On Quaternions and Octonions*** (A. K. Peters). 사원수의 산술을 다루며, 사원수 정수를 이용한 네 제곱수 정리의 증명도 담고 있다.
- **Aigner & Ziegler, *Proofs from THE BOOK*,** "Representing numbers as sums of two squares" 장(수를 두 제곱수의 합으로 나타내기). 이 절과 짝을 이루는 두 제곱수 이야기이다.

안내에 따른 전체 풀이는 제 7.8절에 있다:

https://beyondstep.keithmcnulty.org/ko/ch07/four-squares.html

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