1.6 두 제곱수의 합

학습지

문제

STEP II 2023, 7번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 OCR에서 내려받을 수 있는 2023년 STEP 시험지 묶음(zip 파일) 가운데 STEP II 시험지에 있다:

www.ocr.org.uk/Images/707102-2023-past-papers.zip

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 a와 b가 정수이고 $z = a + \mathrm{i}b$일 때, $|z|^2$은 무엇인가?

1단계 절댓값끼리 곱해진다

다루는 내용: 소문항 (i)

잠깐, 직접 해 보기 zw를 전개하여 $|zw|^2$을 적고, 이를 전개해 보자. 얻은 식을 인수분해(factorise)할 수 있는가?

2단계 활용하기

다루는 내용: 소문항 (ii)

생각해 보기 5와 221을 각각 두 제곱수의 합(sum of two squares)으로 나타내 보자. $|z|^2 = 5$, $|w|^2 = 221$을 만족하는 복소수(complex number)는 어떤 것인가?

잠깐, 직접 해 보기 소문항 (i)에 의해 $|zw|^2 = 5 \times 221$이다. zw를 전개하면 그 실수부분(real part)과 허수부분(imaginary part)이 h와 k이다. 두 번째 답을 얻으려면 두 인수 중 하나를 켤레복소수(conjugate)로 바꾸어 보자.

3단계 먼저 인수분해하기

다루는 내용: 소문항 (iii), (iv)

생각해 보기 8045는 일의 자리가 5이다. 이를 인수분해하자.

잠깐, 직접 해 보기 다른 인수는 어떤 완전제곱수(perfect square)보다 조금 크다. 얼마나 큰가? 그 차는 제곱수인가? 그다음 소문항 (ii)에서처럼 곱하자.

잠깐, 직접 해 보기 소문항 (iv): 36은 이미 제곱수이다. 절댓값의 제곱이 36인 복소수는 무엇이고, 그 수를 곱하면 어떤 효과가 있는가?

4단계 세 가지 방법

다루는 내용: 소문항 (v)

생각해 보기 소문항 (iii)에서처럼 큰 수가 어떤 완전제곱수에 가깝다. 먼저 이 수를 두 제곱수의 합으로 나타내자.

잠깐, 직접 해 보기 25는 여러 가지 방법으로 $|\alpha|^2$ 꼴로 나타낼 수 있다. 5가 그중 하나이다. $|\alpha|^2 = 25$를 만족하는 가우스 정수(Gaussian integer)는 몇 개인가? 그중 실제로 서로 다른 쌍을 주는 것은 어느 것인가?

5단계 나누기

다루는 내용: 소문항 (vi)

생각해 보기 1002037과 109를 각각 두 제곱수의 합으로 나타내자. 이번에도 가까운 완전제곱수를 찾아보자.

잠깐, 직접 해 보기 소문항 (ii)부터 (v)까지는 곱셈을 했다. 이 소문항은 그 아이디어를 거꾸로 적용한다. 한 가우스 정수를 다른 가우스 정수로 나누는 것이다. 나눗셈이 나누어떨어지지 않으면 켤레를 이용해 보자.

숨은 수학

페르마의 두 제곱수 정리

어떤 소수가 두 제곱수의 합일까? $2 = 1^2 + 1^2$, 5, 13, 17, 29, 37, 41은 그렇고, 3, 7, 11, 19, 23, 31은 그렇지 않다. 규칙은 이렇다. 2를 제외하면, 소수가 두 제곱수의 합인 것은 그 소수를 4로 나눈 나머지가 1일 때이고, 그때뿐이다. 페르마(Fermat)가 1640년에 이를 진술했고, 오일러(Euler)가 1749년에 증명했다. 가우스 정수의 언어로 말하면 다음과 같다. 소수 $p \equiv 1 \pmod 4$는 $p = (a+bi)(a-bi)$로 **분해되고**(*splits*), 소수 $p \equiv 3 \pmod 4$는 계

속 소수로 남는다. 예를 들어 $5 = (2+\mathrm{i})(2-\mathrm{i})$이지만, 3은 전혀 인수분해되지 않는다.

1990년에 돈 자기어(Don Zagier)는 단 한 문장으로 이루어진 것으로 유명한 두 제곱수 정리의 증명을 발표했다. 이 증명은 *Proofs from THE BOOK*에 설명과 함께 실려 있다.

고유한 소수를 가진 새로운 수 체계

가우스(Gauss)는 가우스 정수가 보통의 정수와 놀랄 만큼 비슷하게 행동한다는 것을 깨달았다. 나눗셈 알고리즘(division algorithm)과 유클리드 호제법(Euclidean algorithm)이 있고, 모든 가우스 정수는 (± 1 또는 $\pm\mathrm{i}$를 곱하는 차이를 무시하면) 가우스 소수(Gaussian prime)들의 곱으로 **유일하게** 인수분해된다. 이것을 ($\star$)와 결합하면, 어떤 수의 소인수분해(prime factorisation)만으로 그 수를 두 제곱수의 합으로 나타내는 방법이 정확히 몇 가지인지 셀 수 있다.

대학에서 이것은 **대수적 정수론**(*algebraic number theory*)으로 들어가는 관문이 된다. 대수적 정수론은 보통의 자연수를 이해하기 위해 $\mathbb{Z}[\mathrm{i}]$나 $\mathbb{Z}[\sqrt{-5}]$와 같은 수 체계를 연구한다. Section 1.7에서는 이 분야가 왜 만들어져야 했는지 보여 준다. 이런 수 체계가 모두 가우스 정수처럼 얌전하게 행동하지는 않기 때문이다.

네 제곱수와 그 너머

모든 양의 정수는 네 제곱수의 합이다(라그랑주(Lagrange), 1770년). 이 증명은 ($\star$)의 네 제곱수 버전에 기대는데, ($\star$)가 복소수에서 나오는 것과 같은 방식으로 이 식은 해밀턴(Hamilton)의 **사원수**(*quaternions*)에서 나온다. 이것은 Section 7.8에서 보게 될 것이다.

더 도전하기

1 **걸림돌.** $4k+3$ 꼴의 수는 두 제곱수의 합이 될 수 없음을 보여라. (제곱수를 4로 나눈 나머지는 무엇인가?)

2 **두 가지 방법.** 65와 85를 각각 두 가지 서로 다른 방법으로 두 제곱수의 합으로 나타내고, 그 답을 가우스 정수를 이용하여 설명하여라.

3 **네 가지 방법.** $1105 = 5 \times 13 \times 17$이다. 1105를 두 양의 제곱수의 합으로 나타내는 서로 다른 방법 네 가지를 찾아라. 왜 네 가지일까?

4 **가우스 소수.** 심화 a, b, c, d가 정수이고 $3 = (a+b\mathrm{i})(c+d\mathrm{i})$이면, 두 인수 중 하나의 절댓값이 1임을 보여라. (절댓값의 제곱을 취해 보아라.) 이로써 3이 가우스 소수임을 알 수 있다.

더 읽을거리

- **John Stillwell, *Elements of Number Theory*** (Springer). 역사와 함께 가우스 정수와 그 너머까지 차근차근 쌓아 올린다.
- **Aigner & Ziegler, *Proofs from THE BOOK***, 제 4장, “Representing numbers as sums of two squares”(수를 두 제곱수의 합으로 나타내기).
- **Joseph Silverman, *A Friendly Introduction to Number Theory***, 제곱수의 합과 가우스 정수를 다루는 장들.

안내에 따른 전체 풀이는 제 1.6절에 있다:
https://beyondstep.keithmcnulty.org/ko/ch01/two-squares.html

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