$u_{n+1} = 4u_n(1-u_n)$

$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$

$\pi^e < e^\pi$

$F_n = 2^{2^n} + 1$

$e^{i\tau} + 1 = 0$

STEP 대비 · 대학 수학

Beyond STEP

제1장

정수론과 증명

$R(3,3) = 6$

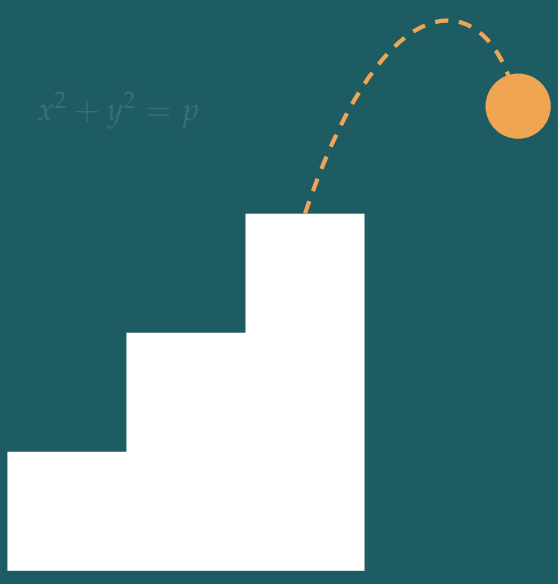
$\frac{22}{7} - \pi = \int_0^1 \frac{x^4(1-x)^4}{1+x^2}\,dx$

$x^2 + y^2 = p$

$P(A \mid B)$

$\ddot{x} = -\omega^2 x$

$\sin^2(2^n\theta)$



KEITH McNULTY

Beyond STEP

STEP 기출문제로 여는
대학 수학의 세계

제1장

정수론과 증명

Keith McNulty

Beyond STEP: STEP 기출문제로 여는 대학 수학의 세계

제1장: 정수론과 증명

이 PDF는 *Beyond STEP*의 전체 13개 장 가운데 제1장이다. 책 전체, 각 장의 개별 PDF, 모든 절의 인쇄용 연습지, 모든 STEP 문제의 자세한 풀이를 `beyondstep.keithmcnulty.org`에서 무료로 읽고 내려받을 수 있다.

2026년 11월 온라인 초판 발행.

이 PDF에서 지은이가 직접 만든 모든 것, 곧 본문, 풀이, 그림, 연습문제와 해답은 크리에이티브 커먼즈 CC0 1.0 Universal 라이선스에 따라 퍼블릭 도메인(public domain)으로 공개한다. 누구든 허락을 구하지 않고 어떤 목적으로든 복사하고, 고쳐 쓰고, 공유할 수 있다. 자세한 내용은 `creativecommons.org/publicdomain/zero/1.0`을 보라.

여기에서 다루는 STEP 문제의 저작권은 Cambridge University Press & Assessment에 있다. 문제는 이 책에 싣지 않았으며, 각 문제마다 공식 출처인 STEP Support Programme의 문제 데이터베이스나 OCR의 기출 시험지로 가는 링크를 달았다.

오류 제보는 `github.com/keithmcnulty/step_book_mcnulty`에 이슈로 남겨 주기 바란다.

장

1

정수론과 증명

정수는 수학에서 가장 오래된 대상이며, 지금도 수학의 가장 깊은 비밀 가운데 일부를 품고 있다.

이 장의 내용

1.1 소수 공장 STEP II 2002

1.2 소수는 얼마나 드문드문 흩어져 있는가? STEP III 2016

1.3 가장 작은 반례 STEP III 2015

1.4 e는 무리수이고, e^2도 그렇다 STEP III 2024

1.5 무한 강하법 STEP III 2022

1.6 두 제곱수의 합 STEP II 2023

1.7 인수분해가 무너질 때 STEP I 2016

1.8 유리수 세기 STEP III 2020

1.9 삼차곡선의 접선 STEP I 2009

A 연습문제 해답 71쪽

왜 정수인가?

> 수학은 과학의 여왕이고, 정수론은 수학의 여왕이다.
>
> — 카를 프리드리히 가우스(Carl Friedrich Gauss)

정수(whole numbers)는 누구나 처음 만나는 수학적 대상이다. 우리는 글을 읽기도 전에 수 세는 법을 배웠다. 그런데도 정수에 관한 가장 단순한 질문이 지독하게 어려울 수 있다. 2보다 큰 모든 짝수는 두 소수(prime)의 합일까? 아무도 모른다. 골드바흐(Christian Goldbach)가 1742년에 이 질문을 던졌고, 컴퓨터로 4×10^{18} 너머까지 확인했지만, 여전히 증명된 적은 없다. 11과 13, 또는 101과 103처럼 차가 2인 소수의 쌍은 무한히 많을까? 이 역시 아무도 모른다. 다만 2013년에 거의 알려지지 않았던 수학자 장이탕(Yitang Zhang)이 차가 많아야 70백만인 소수의 쌍이 무한히 많음을 증명하여 세상을 놀라게 했고, 그 수는 이후 246까지 줄어들었다. 페르마(Pierre de Fermat)는 1637년에 책의 여백에 $n \geq 3$일 때 $x^n + y^n = z^n$은 양의 정수 해를 갖지 않는다고 적어 두었다. 와일스(Andrew Wiles)가 1994년에 페르마가 옳았음을 증명하기까지는 350년이 넘는 시간과, 지금까지 만들어진 것 가운데 가장 정교한 수학 일부가 필요했다.

어린아이도 이해할 수 있는 질문과 수백 년이 걸릴 수도 있는 답이 이렇게 섞여 있다는 점이 정수론(number theory)을 중독성 있게 만든다. 정수론이 언제나 **증명**(proof)의 훈련장이었던 이유도 여기에 있다. 정수는 무한히 많으므로 모든 경우를 확인할 수 없을 때에는, 모든 경우를 한꺼번에 다루는 논증을 찾아야 한다. 여러분이 앞으로 수학을 하면서 평생 쓰게 될 증명 기법 대부분은 처음에 정수에 관한 질문을 통해 다듬어졌다.

순수하고, 쓸모없고, 인터넷을 움직이는

1940년에 케임브리지의 수학자 하디(G. H. Hardy)는 다소 자랑스럽게, 정수론은 모든 수학 가운데 가장 순수하여 일상생활과 너무 동떨어져 있으므로 실용적으로 쓰일 수 없고, 따라서 **해로운** 용도로 쓰일 수도 없다고 썼다. 이보다 더 틀릴 수는 없었을 것이다. 온라인에서 물건을 사거나, 보안 메시지를 보내거나, 휴대전화의 잠금을 풀 때마다 여러분은 정수론에 기대고 있다. RSA 암호 체계(1977)는 두 큰 소수를 곱하기는 쉽지만 그 곱으로부터 두 소수를 되찾기는 불가능할 만큼 어려워 보인다는 사실에 바탕을 둔다. 현대의 암호 체계는 이 장의 끝에서 만나게 될 바로 그 곡선들의 산술을 이용한다. 18세기와 19세기의 "쓸모없는" 수학이 21세기의 보안이 된 것이다.

대학에서 만나게 될 것

대학에서 수학을 공부한다면, 정수론은 가장 먼저 만나는 분야이자 가장 마지막에 이르는 분야 가운데 하나가 될 것이다.

- **첫 학기에는** 거의 틀림없이 **수와 집합**(Numbers and Sets)이나 **기초**(Foundations) 같은 이름의 강좌를 듣게 된다. 이 강좌는 증명을 제대로 쓰는 법을 가르치며, 그 재료의 상당 부분이 정수론이다. 귀납법(induction), 유클리드 호제법(Euclidean algorithm), 모듈러 산술(modular arithmetic), 페르마의 소정리(Fermat's Little Theorem), 중국인의 나머지 정리(Chinese Remainder Theorem), 그리고 어떤 무한집합은 다른 무한집합보다 크다는 놀라운 사실이 그것이다.
- **군론(group theory)에서는**, 보통 1학년에, 정수론의 많은 사실이 대칭에 관한 하나의 정리, 곧 라그랑주(Lagrange) 정리의 그림자임을 발견하게 된다.
- **2학년에는** 정수론 강좌에서 보통 이차 상호 법칙(quadratic reciprocity, 가우스의 "황금 정리"), 연분수(continued fractions), 펠 방정식(Pell's equation)을 다룬다.
- **그 뒤에는** 더 나아갈 수 있다. 가우스 정수(Gaussian integers) 같은 새로운 수 체계가 소인수분해의 유일성(unique factorisation)을 되살려 내는 **대수적 정수론**(algebraic number theory), 미적분과 복소해석(complex analysis)을 써서 소수를 세는 **해석적 정수론**(analytic number theory), 그리고 페르마의 마지막 정리(Fermat's Last Theorem)의 증명과 상금 백만 달러가 걸린 일곱 개의 밀레니엄 문제(Millennium Prize Problems) 가운데 하나의 바탕에 있는 **타원곡선**(elliptic curves) 이론이 그것이다.

이 장을 관통하는 질문들

이 장의 STEP 문제 아홉 개는 세 가지 큰 질문을 중심으로 돈다. 문제를 푸는 동안 이 질문들을 마음에 담아 두자. 장의 끝에서 다시 돌아올 것이다.

1. **소수는 얼마나 많으며, 어떻게 분포해 있을까?** 소수가 무한히 많다는 것은 누구나 안다. 그렇다면 소수는 얼마나 드물어지며, 어떤 종류의 논증이 그것을 알려 줄 수 있을까?
2. **어떤 수가 분수가 아님을 어떻게 증명할까?** 어떤 수가 유리수(rational)임을 보이려면 예 하나면 충분하다. 무리수(irrational)임을 보이려면 무한히 많은 가능성을 배제해야 한다. 대체 그것을 어떻게 해낼까?
3. **어떤 방정식이 정수 해를 가지며, 수 체계를 바꾸면 무슨 일이 일어날까?** 때로는 방정식이 해를 전혀 갖지 않음을 보일 수 있다. 때로는 정수를 이해하는 가장 좋은 방법이 정수 바깥으로, 복소수나 곡선 위로 나가는 것이다.

증명에 관한 장

이 세 질문의 밑바탕에는 네 번째 주제가 흐른다. 바로 **증명하는 방법**이다. 각 절은 서로 다른 증명 방법이 실제로 쓰이는 모습을 보여 준다는 이유도 있어서 골랐으며, 이들을 모으면 대학 1학년생에게 꽤 쓸 만한 도구 상자가 된다.

§	주제	사고 방식
1.1	페르마 수	무한히 많은 소수를 **필요로 하는** 무한한 수의 모임
1.2	소수의 곱	강한 귀납법(strong induction); 이항계수(binomial coefficients)에 숨은 정보
1.3	다시 $\sqrt{2}$	"가장 작은 것을 잡아라": 정렬 원리(well-ordering principle)
1.4	e와 e^2	정수를 0과 1 사이에 가두기
1.5	불가능한 방정식	무한 강하법(infinite descent); 법 n으로 계산하기
1.6	두 제곱수의 합	무대 바꾸기: 복소수
1.7	이상한 수 체계	당연하게 여기던 것을 의심하기
1.8	분수를 나열하기	전단사(bijection) 만들기; 거꾸로 하는 강하법
1.9	세제곱수와 곡선	산술 문제를 푸는 기하

이 장을 읽는 방법

각 절은 출제된 그대로의 STEP 문제로 가는 링크로 시작한다. 계속 읽기 전에 먼저 적어도 30분 동안 직접 풀어 보자. 읽기만 한 문제보다 씨름해 본 문제에서 훨씬 많은 것을 배우게 된다. 계속 읽을 때, **스스로 물어보기** 상자는 답이 나오기 전에 멈추고 생각해 보라는 권유이고, **잠깐 풀어 보기** 상자는 핵심 아이디어가 손에 닿을 만한 곳에 있는 순간을 표시한다. 그리고 각 절의 **숨은 수학** 부분은 시험 너머, 대학에서 만나게 될 수학을 내다본다.

절들은 대체로 뒤로 갈수록 수준이 높아지지만, 대부분 서로 독립적이다. 어떤 절이 마음을 끌지 않으면 다음으로 넘어갔다가 나중에 다시 돌아와도 된다.

1.1 소수 공장

문제

STEP II 2002, 3번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/02-s2-q3`

도입

소수(prime)가 무한히 많다는 사실은 아마 이미 알고 있을 것이다. 유클리드(Euclid)가 기원전 300년 무렵에 이를 증명했고, 이것은 누구나 가장 먼저 접하는 증명 가운데 하나이다. 그렇다면 STEP 문제는 왜 이것을 다시 증명하라고 하는 것일까?

이 증명은 완전히 다른 방식으로 작동하기 때문이다. 유클리드의 논증은 이렇게 말한다. 소수를 유한 개 나열한 목록을 아무것이나 주면, 그 목록이 불완전하다는 것을 보여 주겠다. 반면 이 증명은 이렇게 말한다. 여기 미리 구체적으로 적어 둔 하나의 수열이 있는데, 그 각 항은 다른 어떤 항에도 들어 있지 않은 소수를 하나씩 품고 있다. 이것은 새로운 소수를 만들어 내는 기계이며, 이 기계가 작동하는 이유는 문제가 차근차근 이끌어 주는 아름답고 단순한 항등식 하나에 있다.

그 과정에서 페르마 자신마저 속아 넘어간 수들을 만나게 될 것이다.

시작하기 전에

문제를 한 번 끝까지 읽고 그 구조를 살펴보자. 문제는 네 단계로 이루어져 있다.

1. 몇 가지 예를 계산한다.
2. 규칙을 찾아내고(사실은 문제가 알려 준다), 그것을 앞의 예로 확인한다.
3. 그 규칙을 일반적으로 증명한다.
4. 그 규칙을 두 번 활용한다. 먼저 공약수(common factor)에 관한 사실을, 다음으로 소수에 관한 사실을 이끌어 낸다.

이러한 "예시 → 추측 → 증명 → 결론"의 구조는 실제로 수많은 수학이 이루어지는 방식이며, STEP 문제도 이를 따르는 경우가 많다. 이런 구조를 보면, 앞부분은 대개 단순한 준비 운동이 아니다. 나중에 필요할 직관을 쌓는 곳이다.

> **생각해 보기** 마지막 줄은 **무한히 많은 소수**에 대해 묻는다. 가운데 부분은 **공약수**에 대해 묻는다. "두 페르마 수(Fermat number)는 공약수를 갖지 않는다"는 사실과 "소수는 무한히 많다"는 사실은 도대체 어떻게 연결될 수 있을까?

이 질문을 기억해 두자. 나중에 다시 돌아올 것이다.

차근차근 풀기

1단계 수에 대한 감 잡기

표기에 주의하자. 2^{2^n}은 $(2^2)^n$이 아니라 $2^{(2^n)}$을 뜻한다. 지수 자체가 2의 거듭제곱이므로 이 수들은 매우 빠르게 커진다.

$$F_0 = 2^1 + 1 = 3, \qquad F_2 = 2^4 + 1 = 17,$$
$$F_1 = 2^2 + 1 = 5, \qquad F_3 = 2^8 + 1 = 257.$$

> **생각해 보기** 이 네 수에서 무엇을 알아챌 수 있는가?

모두 소수이다. (257을 확인해 보자. 이 수는 $2, 3, 5, 7, 11$이나 13으로 나누어떨어지지 않고, $17^2 = 289 > 257$이므로 여기서 멈춰도 된다.) 그다음 수인 $F_4 = 2^{16} + 1 = 65537$도 소수이다. 피에르 드 페르마(Pierre de Fermat)는 1640년에 바로 이 점을 알아채고, 이런 꼴의 수는 **모두** 소수라고 추측(conjecture)했다. 이 점을 기억해 두자. 그가 옳았는지는 나중에 살펴볼 것이다.

2단계 항등식 확인하기

이제 작은 k에 대해 $(*)$를 확인해 보자.

- $k = 1$: 좌변은 그냥 $F_0 = 3$이고, $F_1 - 2 = 3$이다. ✓
- $k = 2$: $F_0 F_1 = 3 \times 5 = 15$이고, $F_2 - 2 = 15$이다. ✓
- $k = 3$: $F_0 F_1 F_2 = 15 \times 17 = 255$이고, $F_3 - 2 = 255$이다. ✓

> **생각해 보기** $k = 2$에서 $k = 3$으로 넘어가는 단계를 보자. 15에 17을 곱해서 255를 얻었다. 페르마 수로 말하면 $(F_2 - 2) \times F_2$를 계산해서 $F_3 - 2$를 얻은 것이다. 이것은 우연일까?

이 관찰이 바로 증명 전체의 축소판이다. 왜 이것이 성립해야 하는지 살펴보자.

3단계 항등식 증명하기

> **잠깐, 직접 해 보기** 계속 읽기 전에 다음을 직접 보여 보자.
>
> $$(F_k - 2)\,F_k = F_{k+1} - 2.$$
>
> 힌트: 모든 것을 2의 거듭제곱으로 나타내 보자. $F_k - 2$는 어떤 모양인가?

$F_k - 2 = 2^{2^k} - 1$이고 $F_k = 2^{2^k} + 1$이므로

$$(F_k - 2)\,F_k = \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right).$$

> **생각해 보기** 이것은 $(a-1)(a+1)$ 꼴의 곱이다. 이것은 무엇과 같은가?

이것은 제곱의 차(difference of two squares) $a^2 - 1$이다. $a = 2^{2^k}$로 두면

$$a^2 = \left(2^{2^k}\right)^2 = 2^{2\cdot 2^k} = 2^{2^{k+1}},$$

이므로

$$(F_k - 2)\,F_k = 2^{2^{k+1}} - 1 = F_{k+1} - 2. \tag{†}$$

이것이 원동력이다. 제곱이 하는 일에 주목하자. 제곱하면 지수가 두 배가 되고, 2^k를 두 배 하면 2^{k+1}이 된다. 페르마 수의 정의는 제곱의 차 인수분해에 꼭 맞게 맞춰져 있다.

이제 귀납법은 거의 자동으로 따라온다.

> **생각해 보기** 귀납 단계에서 정확히 무엇을 보여야 하는가?

어떤 $k \geq 1$에 대해 $(*)$가 성립한다고 가정하자.

$$F_0 F_1 \cdots F_{k-1} = F_k - 2,$$

그리고 이것이 $k+1$에 대해서도 성립함을 보이고자 한다.

$$F_0 F_1 \cdots F_{k-1} F_k = F_{k+1} - 2.$$

가정의 양변에 F_k를 곱하고 (†)를 이용하면

$$F_0 F_1 \cdots F_{k-1} F_k = (F_k - 2)\,F_k = F_{k+1} - 2.$$

$k = 1$인 경우는 이미 확인했으므로, 수학적 귀납법(induction)에 의해 $(*)$는 모든 $k \geq 1$에 대해 성립한다. ■

생각해 보기 귀납법을 아예 쓰지 않을 수도 있었을까?

그렇다. 그 방법도 살펴볼 만하다. $F_0 - 2 = 1$에서 시작하여 $(\dagger)$를 거듭 적용하면

$$F_k - 2 = (F_{k-1} - 2)F_{k-1} = (F_{k-2} - 2)F_{k-2}F_{k-1} = \cdots = (F_0 - 2)\,F_0F_1 \cdots F_{k-1}.$$

$F_0 - 2 = 1$이므로 증명이 끝난다. 이렇게 "풀어 쓰는" 것은 사실 같은 귀납법을 전부 펼쳐 적은 것에 지나지 않지만, 어떤 사람들에게는 이쪽이 더 잘 보인다.

4단계 공약수가 없다

$m \neq n$이면 F_m과 F_n이 1보다 큰 공약수를 갖지 않음을 보이고자 한다.

생각해 보기 $m < n$이고 어떤 수 d가 F_m과 F_n을 모두 나눈다고 하자. $(*)$에서 F_m은 어디에 나타나는가?

$(*)$에서 $k = n$으로 두면

$$F_0F_1 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

$m < n$이므로 F_m은 좌변의 인수 가운데 하나이다. 따라서 d가 F_m을 나누면 d는 좌변 전체를 나눈다. 즉 d는 $F_n - 2$를 나눈다.

생각해 보기 이제 d는 F_n 과 $F_n - 2$를 모두 나눈다. 그렇다면 d는 또 무엇을 나누어야 하는가?

두 수의 차를 나눈다. 즉 d는 $F_n - (F_n - 2) = 2$를 나눈다. 따라서 $d = 1$ 또는 $d = 2$이다.

생각해 보기 d가 2일 수 있는가?

그럴 수 없다. 모든 페르마 수는 2의 거듭제곱에 1을 더한 수이므로 홀수이다. 따라서 $d = 1$이고, 서로 다른 두 페르마 수는 1보다 큰 공약수를 갖지 않는다. ∎

수학자들은 이를 페르마 수들이 **쌍마다 서로소**(*pairwise coprime*)라고 말한다.

5단계 무한히 많은 소수

이제 처음에 던졌던 질문으로 돌아가 보자.

생각해 보기 1보다 큰 모든 자연수는 적어도 하나의 소인수(prime factor)를 갖는다. 각 페르마 수에서 소인수를 하나씩 고르자. 고른 소수들에 대해 무엇을 말할 수 있는가?

p_n을 F_n을 나누는 임의의 소수라 하자. 만약 이 가운데 두 개가 같다면, 즉 $m \neq n$인데 $p_m = p_n$이라면, 그 소수는 F_m과 F_n의 1보다 큰 공약수가 된다. 이는 방금 불가능하다고 보

인 일이다. 따라서 소수들

$$p_0,\ p_1,\ p_2,\ p_3,\ \ldots$$

은 모두 **서로 다르다**. 페르마 수는 무한히 많으므로, 서로 다른 소수도 무한히 많다. ■

각 페르마 수를 **어떤** 소수가 나누는지, 심지어 페르마 수 자체가 소수인지조차 알 필요가 전혀 없었다는 점에 주목하자. 필요한 것은 페르마 수들이 결코 공약수를 갖지 않는다는 사실뿐이었다. 각 페르마 수는 다른 어떤 페르마 수도 쓸 수 없는 소수를 적어도 하나씩 "차지할" 수밖에 없다.

n	$F_n = 2^{2^n} + 1$	소인수분해
0	3	소수
1	5	소수
2	17	소수
3	257	소수
4	65 537	소수
5	4 294 967 297	$641 \times 6\,700\,417$
6	18 446 744 073 709 551 617	$274\,177 \times 67\,280\,421\,310\,721$

그림 1.1.1 처음 몇 개의 페르마 수. 페르마는 이 수들이 모두 소수라고 추측했지만, 1732년에 오일러가 F_5의 인수 641을 찾아냈으며, F_4보다 뒤의 페르마 수 가운데 소수로 알려진 것은 하나도 없다. 그렇더라도 항등식 $(*)$는 서로 다른 페르마 수의 인수가 결코 겹치지 않음을 보여 준다. 각 행은 새로운 소수를 가져온다.

돌아보기

무엇이 이 풀이를 가능하게 했는지 잠시 멈춰서 살펴볼 만하다. 같은 아이디어가 이 책에서 여러 번 다시 등장하기 때문이다.

- **예시는 장식이 아니었다.** $15 \times 17 = 255$가 "$(F_2 - 2) \times F_2 = F_3 - 2$"임을 알아챈 것이 바로 핵심 아이디어였다. 문제가 작은 경우들을 제시하면, 수가 맞는지만 보지 말고 각 단계가 무엇을 하고 있는지 물어보자.
- **항등식 하나가 모든 일을 해냈다.** 모든 것이 $(a-1)(a+1) = a^2 - 1$에서 흘러나왔다. 어려워 보이는 STEP 문제도 단순한 대수 하나로 움직이는 경우가 많다.
- **마지막 논증은 크기가 아니라 구조에 관한 것이다.** 새로운 소수를 하나도 찾지 않고 소수가 무한히 많음을 증명했다. 그 대신 무한히 많은 수의 모임을 만들어 내려면 무한히 많은 소수가 **필요하다**는 것을 보였다.

숨은 수학

페르마는 옳았을까?

아니다. 1732년에 레온하르트 오일러(Leonhard Euler)는 다음을 보였다.

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

오일러가 641을 운 좋게 찾아낸 것은 아니다. 그는 F_n의 소인수가 반드시 매우 특별한 꼴이어야 함을 증명했고($n = 5$인 경우에는 64의 배수보다 1만큼 커야 한다), 이로써 후보를 크게 줄였다. 이 사실은 연습문제 4에서 직접 증명해 볼 수 있다.

그 뒤로 지금까지 누군가 판정에 성공한 페르마 수는 F_5부터 F_{32}까지 모두 합성수(composite)로 밝혀졌다. 알려진 바로는 F_0부터 F_4까지가 **유일한** 페르마 소수일지도 모르지만, 아무도 이를 증명하지 못했다. 이것은 진정한 미해결 문제이다.

유쾌한 반전은 우리의 증명이 이런 것에 전혀 개의치 않는다는 점이다. 소수이든 합성수이든, 페르마 수들은 여전히 무한히 많은 소수를 만들어 낸다.

페르마 소수와 다각형의 작도

페르마 소수는 꽤 뜻밖의 곳에서 등장한다. 고대 그리스인들은 자와 컴퍼스로 정삼각형과 정오각형을 작도하는 방법을 알고 있었는데, $3 = F_0$이고 $5 = F_1$임에 주목하자. 이천 년 동안 아무도 변의 개수가 소수인 다른 정다각형을 작도하지 못했다. 그러다 1796년, 열아홉 살이던 카를 프리드리히 가우스(Carl Friedrich Gauss)가 **정십칠각형**을 작도하는 방법을 보였는데, $17 = F_2$이다.

가우스는 더 나아갔다. 정N각형을 자와 컴퍼스로 작도할 수 있는 것은 정확히 N이 2의 거듭제곱에 **서로 다른 페르마 소수**들을 곱한 수일 때이다. (Pierre Wantzel이 1837년에 이 증명을 완성했다.) 따라서 어떤 다각형을 작도할 수 있는지는 페르마 소수가 몇 개인지에 달려 있다. 가우스의 정십칠각형 뒤에 숨은 핵심 계산은 Section 6.2(STEP II 1991, 문제 4)에서 만나게 되며, 전체 이야기는 학부 과정의 백미 가운데 하나인 **갈루아 이론**(*Galois theory*)에 속한다.

하나의 정리, 여러 가지 증명

수학자들은 왜 같은 정리를 굳이 여러 번 증명할까? 증명이 다르면 드러나는 것도 다르기 때문이다. 흔히 크리스티안 골드바흐(Christian Goldbach)가 1730년에 오일러에게 보낸 편지에서 나온 것으로 알려진 이 증명은, 1보다 큰 자연수들로 이루어진 쌍마다 서로소인 수열이라면 **어떤** 것이든 무한히 많은 소수를 강제한다는 것을 보여 준다. 페르마 수는 편리한 예 가운데 하나일 뿐이다. (연습문제 3에서 또 다른 예를 볼 수 있다.)

이 증명은 유클리드의 증명보다 더 많은 것을 알려 주기도 한다. 소수 $p_0, p_1, \ldots, p_{n-1}$은 n개의 서로 다른 소수이고, 각각은 F_{n-1} 이하이다. 따라서 $2^{2^{n-1}}+1$보다 크지 않은 소수가 적어도 n개 있다. 이것은 소수가 어떻게 분포하는지에 대한 **정량적**(*quantitative*) 명제이다. 매우 약한 결과이지만(실제로는 훨씬 더 좋다), 소수가 얼마나 드물어지는지를 정확히 기술하는 19세기 수학의 위대한 결과 가운데 하나인 **소수 정리**(*Prime Number Theorem*)를 향한 첫걸음이다. Section 1.2에서 그다음 걸음을 내디딘다.

사고 기술

구조적 성질로부터 논증 세우기

A 유형의 대상이 무한히 많이 존재함을 보이려면, 각각이 자기만의 *A* 유형 대상을 필요로 하는 *B* 유형의 대상을 무한히 많이 찾으면 된다.

여기서 A는 소수, B는 페르마 수이고, "자기만의 것을 필요로 한다"는 것은 "다른 어떤 것과도 공유하지 않는 소인수를 갖는다"는 뜻이다. 같은 패턴이 세기 논증, 선형대수학(linear algebra)(일차독립인 벡터가 무한히 많으면 차원이 무한이 된다), 해석학(analysis)에서도 나타난다.

또한 **귀납법**을 연습했고, 특히 "k에서 $k+1$로 넘어가는 단계는 실제로 무슨 일을 하는가?"라고 묻는 습관을 길렀다. 이 질문은 형식적인 틀보다 더 유용할 때가 많다.

더 도전하기

1 **유클리드의 증명.** 소수가 무한히 많다는 유클리드의 증명을 적어 보자. 그 증명은 어떤 의미에서 "귀류법(by contradiction)"이고, 페르마 수를 이용한 증명은 어떤 의미에서 "구성적(constructive)"인가?

2 **일의 자리 숫자.** $n \geq 2$일 때 페르마 수 F_n의 일의 자리 숫자가 7임을 보여라.

3 **실베스터 수열(Sylvester's sequence).** $a_1 = 2$, $a_{n+1} = a_n^2 - a_n + 1$로 정의하면, 수열은 $2, 3, 7, 43, 1807, \ldots$로 시작한다.

   (a) $a_{n+1} - 1 = a_1 a_2 \cdots a_n$임을 보여라.

   (b) 이 수열의 항들이 쌍마다 서로소임을 이끌어 내고, 이를 이용하여 소수가 무한히 많다는 또 다른 증명을 제시하여라.

   (c) 심화 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$임을 보여라.

4 **오일러의 기법.** 이 문제에는 페르마의 소정리(*Fermat's Little Theorem*)가 필요하다: p가 소수이고 $p \nmid a$이면 $a^{p-1} \equiv 1 \pmod{p}$이다. 소수 p가 F_n을 나눈다고 하자.

(a) $2^{2^n} \equiv -1 \pmod{p}$임을 보이고, 이로부터 $2^{2^{n+1}} \equiv 1 \pmod{p}$임을 보여라.

(b) d를 $2^d \equiv 1 \pmod{p}$를 만족하는 가장 작은 양의 정수라 하자. d가 2^{n+1}은 나누지만 2^n은 나누지 않음을 보이고, $d = 2^{n+1}$이라고 결론지어라.

(c) 페르마의 소정리를 이용하여 d가 $p-1$을 나눔을 보여라. 이로부터 $p \equiv 1 \pmod{2^{n+1}}$임을 이끌어 내어라.

(d) $n = 5$일 때, 이 결과는 F_5의 모든 소인수가 $64k+1$ 꼴임을 말해 준다. 641이 이 꼴임을 확인하여라. 641보다 작은 이 꼴의 소수는 몇 개인가?

5 **소수의 상계.** 하나의 정리, 여러 가지 증명의 논증을 이용하여 n번째 소수가 $2^{2^{n-1}}+1$ 이하임을 보여라. $n = 5$일 때 이 상계는 얼마나 좋은가?

더 읽을거리

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK*** (Springer), 제1장 "Six proofs of the infinity of primes"(소수가 무한함에 대한 여섯 가지 증명). 이 증명을 유클리드의 증명 및 다른 네 가지 증명과 함께 싣고 있으며, 그 가운데 하나는 위상수학(topology)을 이용한다. 대학 입학 전에 읽을 수 있는 최고의 책 가운데 하나이다.
- **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press), 제1–2장. 소수와 소인수분해에 대한 아름답게 쓰인 입문서로, 대학 입학 전 여름에 읽기에 이상적이다.
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers*** (Springer, 2001). 오일러의 인수분해부터 가우스의 다각형까지, 페르마 수에 관한 모든 것을 담고 있다. 앞쪽 장들을 골라 읽어 보자.
- **Ian Stewart, *Why Beauty Is Truth*** (Basic Books), 가우스에 관한 장. 일반 독자를 위해 풀어 쓴 정십칠각형 이야기이다.

1.2 소수는 얼마나 드문드문 흩어져 있는가?

문제

STEP III 2016, 5번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/16-s3-q5`

도입

Section 1.1에서 소수(prime)가 무한히 많다는 것을 보았다. 그러나 "무한히 많다"는 것은 투박한 말이다. 소수는 분명히 점점 드물어진다. 100 미만의 소수는 25개이지만, 900과 1000 사이의 소수는 14개뿐이다. 그렇다면 소수는 **얼마나** 드물어지는가?

이 문제는 꽤 소박해 보이는 사실을 증명한다. n 이하의 모든 소수를 곱하면 그 값이 4^n보다 작다는 것이다. 그러나 이 순진해 보이는 부등식(inequality)은 "얼마나 드문가?"라는 물음에 답하는 첫 번째 진정한 발걸음이며, 1932년 젊은 에르되시(Paul Erdős)가 내놓은, 수학에서 가장 유명한 짧은 증명 가운데 하나의 핵심 보조정리(lemma)이다.

시작하기 전에

기호 $P_{r,s}$는 까다로워 보이지만 생각은 단순하다. 어떤 범위에 있는 소수들을 모두 곱하는 것이다. 예시를 꼭 이해하고 넘어가자. $P_{3,7}$은 3보다 크고 7 이하인 소수, 곧 5와 7을 사용하므로 그 값은 35이다.

? **생각해 보기** 문항 (iv)는 **모든** $n \geq 2$에 대하여 어떤 명제를 증명하라고 한다. 문항 (iii)은 $2m$ 이하의 모든 k에 대하여 그 명제가 성립한다고 가정한다. 이것은 어떤 종류의 귀납법(induction)인가?

이것은 **강한** 귀납법(strong induction)이다. n인 경우를 증명할 때, 바로 앞의 경우만이 아니라 그 이전의 **모든** 경우를 가정해도 된다. 이 점을 기억해 두자. 문제가 이런 식으로 구성된 까닭이 바로 이것이다.

차근차근 풀기

1단계 이항계수는 너무 크지 않다

생각해 보기 $(1+x)^{2m+1}$의 이항전개(binomial expansion)에 $x=1$을 대입하면 무엇을 얻는가?

다음을 얻는다.

$$2^{2m+1} = \binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{2m+1}.$$

모든 항이 양수이므로 각 항은 2^{2m+1}보다 작다. 하지만 이것으로는 충분하지 않다. 우리가 원하는 것은 그 절반인 2^{2m}이다.

생각해 보기 파스칼의 삼각형(Pascal's triangle)은 대칭이다. 합에서 $\binom{2m+1}{m}$과 같은 다른 항은 무엇인가?

대칭성에 의해 $\binom{2m+1}{m} = \binom{2m+1}{m+1}$이고, 이 둘은 합에서 **서로 다른** 두 항이다($m \neq m+1$이므로). 따라서

$$2\binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} < 2^{2m+1},$$

이며, 합에는 $\binom{2m+1}{0} = 1$과 같은 다른 양수 항도 들어 있으므로 등호 없는 부등식이 성립한다. 양변을 2로 나누면 $\binom{2m+1}{m} < 2^{2m}$을 얻는다. ■

2단계 그 이항계수를 나누는 소수는 무엇인가?

이항계수(binomial coefficient)를 풀어 쓰면 다음과 같다.

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!} = \frac{(m+2)(m+3)\cdots(2m+1)}{m!}.$$

생각해 보기 p를 $m+1 < p \leq 2m+1$인 소수라 하자. p는 분자를 나누는가? 분모를 나눌 수 있는가?

분자 $(m+2)(m+3)\cdots(2m+1)$은 p 자신을 인수로 포함하므로 p는 분자를 나눈다. 분모 $m!$은 모두 p보다 작은 수들의 곱이다. p는 소수이므로, 어느 인수도 나누지 못하는 수들의 곱을 나눌 수 없다. 따라서 p는 분자는 나누지만 분모는 나누지 않으며, 그러므로 p는 이항계수 전체를 나눈다(이항계수가 정수라는 점을 기억하자).

잠깐, 직접 해 보기 이제 범위 안의 각 소수가 $\binom{2m+1}{m}$을 나눈다는 것을 알았다. 그렇다면 왜 그들의 곱 $P_{m+1,2m+1}$도 이 수를 나누는가? (주의: 4와 6이 모두 어떤 수를 나눈다고 해서 24가 그 수를 나누는 것은 아니다.)

차이는 우리의 소수들이 **서로 다른 소수**(distinct primes)라는 데 있다. 서로 다른 소수 $p_1, p_2, \ldots$가 각각 N을 나누면 그들의 곱도 N을 나눈다. $N = p_1 N_1$이라 쓰자. 그러면 p_2는 $p_1 N_1$을 나누지만 p_1은 나누지 않으므로 N_1을 나눈다. 이와 같이 계속하면 된다. (여기서는 소수가 곱을 나누면 그 인수 가운데 하나를 나눈다는 사실을 사용했다. 이 사실은 잠시 경의를 표할 만하다. Section 1.7에서는 이와 비슷한 성질이 무너지는 세계를 보여 준다.)

따라서 $P_{m+1,2m+1}$은 $\binom{2m+1}{m}$을 나누고, 양수의 약수(divisor)는 그 수보다 크지 않으므로

$$P_{m+1,\,2m+1} \le \binom{2m+1}{m} < 2^{2m}. \qquad \blacksquare$$

3단계 곱을 나누기

생각해 보기 $2m+1$ 이하의 모든 소수의 곱인 $P_{1,2m+1}$을 이미 알고 있는 곱들로 어떻게 만들 수 있는가?

$2m+1$ 이하의 소수를 $m+1$ 이하인 것과 $m+1$보다 큰 것으로 나누자.

$$P_{1,2m+1} = P_{1,m+1} \times P_{m+1,2m+1}.$$

2단계에 의해 두 번째 인수는 $2^{2m} = 4^m$보다 작다. 첫 번째 인수에 대해서는, 2부터 $2m$까지의 모든 k에 대하여 $P_{1,k} < 4^k$라고 가정해도 되며, $k = m+1$은 이 범위 안에 있다($m \ge 1$이면 $2 \le m+1 \le 2m$이므로). 따라서

$$P_{1,2m+1} < 4^{m+1} \times 4^m = 4^{2m+1}. \qquad \blacksquare$$

바로 여기서 강한 귀납법이 제 몫을 한다. $2m+1$을 다루기 위해 필요했던 것은 바로 앞의 경우가 아니라, 대략 그 절반 크기인 $m+1$인 경우였다.

4단계 모든 n

생각해 보기 문항 (iii)은 홀수를 다룬다. 짝수 $n = 2m+2$이면 어떻게 되는가? 이 수는 소수인가?

처음 경우를 확인하자. $P_{1,2} = 2 < 16$이고 $P_{1,3} = 6 < 64$이다. 이제 $n \ge 4$일 때, 2부터 $n-1$까지의 모든 k에 대하여 $P_{1,k} < 4^k$라고 가정하자.

- n이 짝수이면, n은 소수가 아니다(2보다 크므로). 따라서 n 이하의 소수는 $n-1$ 이하의 소수와 같다. 그러므로 $P_{1,n} = P_{1,n-1} < 4^{n-1} < 4^n$이다.

- n이 홀수이면, $m \geq 2$인 m에 대하여 $n = 2m + 1$로 쓰자. 그러면 문항 (iii)에 의해 곧바로 $P_{1,n} < 4^n$이다.

강한 귀납법에 의해, 모든 $n \geq 2$에 대하여 $P_{1,n} < 4^n$이다. ■

돌아보기

- **이항계수는 수론적 정보를 담고 있다.** $\binom{2m+1}{m}$은 작으면서(4^m보다 작다) 많은 소수로 나누어떨어질 수밖에 없는 하나의 수이다. 많은 소수를 작은 수 안에 밀어 넣으면, 그런 소수가 너무 많을 수는 없다는 것을 알 수 있다.
- **문제가 스스로를 절반으로 줄일 때는 강한 귀납법이 자연스러운 도구이다.** $2m + 1$인 경우는 $m + 1$인 경우에 의존했다.
- **작은 경우는 따로 확인해야 한다.** 귀납법은 $n \geq 4$가 되어서야 작동하므로, $n = 2$와 3은 직접 처리해야 했다.

숨은 수학

4^n에서 소수 정리까지

결과에 로그(logarithm)를 취하면 $\ln P_{1,n} < n \ln 4$, 곧

$$\sum_{p \leq n} \ln p < (\ln 4)\, n \approx 1.39\, n.$$

1850년대에 체비쇼프(Pafnuty Chebyshev)는 바로 이런 종류의 상계와 **하계**를 증명하여, $\sum_{p \leq n} \ln p$가 n에 비례하여 증가함을 보였다. 가우스(Gauss)는 약 15세 무렵 이미 표를 보고 n 이하의 소수의 개수가 대략 $n / \ln n$이라고 추측했다. 이것이 **소수 정리**(Prime Number Theorem)가 되었으며, 1896년 아다마르(Jacques Hadamard)와 드 라 발레 푸생(Charles de la Vallée Poussin)이 복소해석학(complex analysis)을 이용하여 마침내 증명하였다. 로그 형태로 쓰면 소수 정리는

$$\sum_{p \leq n} \ln p \sim n,$$

을 말하며, 따라서 n 이하의 소수의 곱은 대략 e^n이다. 우리가 얻은 상계 4^n은 전혀 동떨어진 값이 아니다. 그림 1.2.1에 세 가지를 모두 나타내었다.

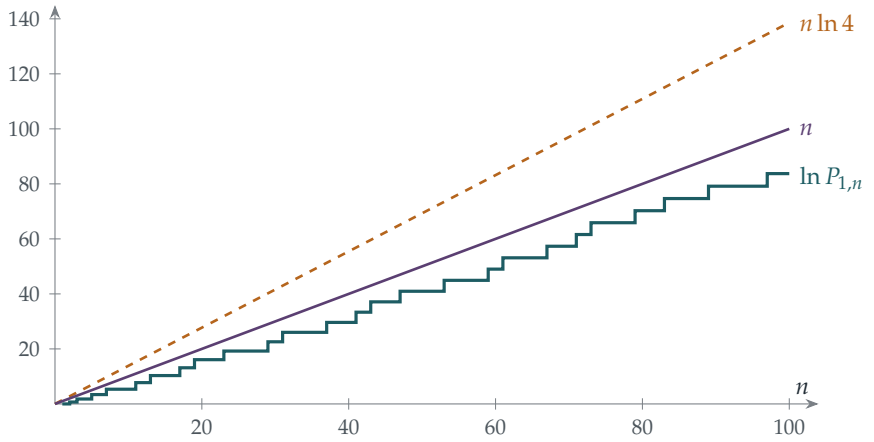


그림 1.2.1 n 이하의 모든 소수의 곱의 로그(청록색). 각 소수 p에서 $\ln p$만큼 뛰어오른다. 이 절에서는 이 값이 $n \ln 4$(호박색, 점선) 아래에 머문다는 것을 증명한다. 소수 정리에 따르면 이 값은 n(자주색)처럼 증가한다.

베르트랑 공준

1845년 베르트랑(Joseph Bertrand)은 모든 $n \geq 1$에 대하여 n과 $2n$ 사이에 항상 소수가 존재한다고 추측했다. 체비쇼프는 1852년에 이를 증명했다. 80년 뒤, 약관 19세의 에르되시가 아름다운 초등적 증명을 찾아냈다. 그 핵심 재료는 이 문제의 보조정리와, **가운데** 이항계수 $\binom{2n}{n}$을 나누는 소수가 무엇인지에 대한 세심한 분석이다. Martin Aigner와 Günter Ziegler는 수학에서 가장 우아한 증명들을 모은 책 *Proofs from THE BOOK*의 제2장으로 이 증명을 골랐다.

이 다음은

소수의 정확한 분포는 리만 제타 함수(Riemann zeta function)

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

의 영점에 의해 결정된다. 이 함수는 Section 2.4에서 훨씬 소박한 모습으로 만나게 되는데, 거기서 $\zeta(2) = \pi^2/6$이다. 그 영점들이 정확히 어디에 있는지 예측하는 **리만 가설**(Riemann Hypothesis)이 참이라면, 소수 정리의 오차를 가능한 한 가장 정밀하게 잡아낼 수 있다. 리만 가설은 아마도 수학에서 가장 유명한 미해결 문제이며, 밀레니엄 문제(Millennium Prize Problems) 가운데 하나이다.

사고 기술

강한 귀납법, 그리고 영리한 대상에서 정보 끌어내기

n인 경우가 $n-1$보다 훨씬 작은 경우에 의존한다면, 이전의 모든 경우를 한꺼번에 가정하라.

여기에 담긴 또 하나의 아이디어는 더 미묘하며 정수론(number theory)의 특징을 잘 보여 준다. 어떤 범위의 모든 소수에 대해 무언가를 보이려면, 그 소수들이 모두 나누어야만 하면서 동시에 너무 크지 않다는 것도 보일 수 있는 하나의 대상(여기서는 이항계수)을 찾아라.

더 도전하기

1 **수를 느껴 보기.** $n = 10, 20, 30$에 대하여 $P_{1,n}$을 계산하고, 4^n 및 e^n과 비교하여라. (여기서는 계산기를 써도 좋다.)

2 **가운데 이항계수.** $\binom{2m}{m}$이 $(1+1)^{2m}$의 전개에 나오는 $2m+1$개의 항 가운데 가장 큼을 보이고, 이로부터 $\binom{2m}{m} \geq \dfrac{4^m}{2m+1}$임을 유도하여라.

3 **소수는 너무 많지 않다.** $\pi(n)$을 n 이하의 소수의 개수라 하자. $\sqrt{n}$과 n 사이의 모든 소수는 $\sqrt{n}$보다 크고, 그들의 곱은 많아야 $P_{1,n} < 4^n$이다. 이로부터

$$\pi(n) - \pi(\sqrt{n}) < \frac{2\ln 4}{\ln n}\, n,$$

임을 유도하고, 따라서 $\pi(n) < 2.8\, n/\ln n + \sqrt{n}$임을 보여라. 이를 소수 정리의 $\pi(n) \approx n/\ln n$과 비교하여라.

4 **베르트랑 확인하기.** $n = 1, 2, \ldots, 50$ 각각에 대하여 n과 $2n$ 사이의 소수를 찾아 베르트랑 공준(Bertrand's postulate)을 확인하여라. 각 소수가 바로 앞 소수의 두 배보다 작은 짧은 소수 목록을 이용하여 효율적으로 할 수 있는가?

더 읽을거리

- **Aigner & Ziegler, *Proofs from THE BOOK***, 제2장, "Bertrand's postulate"(베르트랑 공준).
- **Marcus du Sautoy, *The Music of the Primes*** (Fourth Estate). 소수 정리와 리만 가설의 역사를 다룬 대중서이다.

- **G. J. O. Jameson, *The Prime Number Theorem*** (Cambridge University Press). 엄밀하면서도 친절하며 학부생을 위해 쓰였다. 앞쪽 장들은 A 레벨(A level, 영국의 대학 입학 자격 시험) 수준의 미적분만 있으면 읽을 수 있다.

1.3 가장 작은 반례

문제

STEP III 2015, 5번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/15-s3-q5`

도입

$\sqrt{2}$가 무리수(irrational)라는 증명은 아마 본 적이 있을 것이다. $\sqrt{2} = a/b$를 기약분수(lowest terms)로 놓고 양변을 제곱한 다음, a가 짝수이고 이어서 b도 짝수임을 이끌어 내어 모순을 얻는다. 훌륭한 증명이다. 그러나 이 증명은 **짝수**에 관한 요령에 기대고 있어서 다른 경우로 쉽게 일반화되지 않는다. $\sqrt[3]{2}$는 어떨까? $\sqrt{7}$은?

이 문제는 다른 증명을 제시하는데, 그 핵심 아이디어는 놀라울 만큼 단순하다. 바로 **가장 작은 것을 보라**는 것이다. 같은 아이디어가 이 장에서 모습을 바꾸어 여러 번 다시 등장한다.

시작하기 전에

이 문제는 STEP 문제로서는 특이하다. 증명의 뼈대를 주고 빠진 근거를 채우라고 요구하기 때문이다. 이것이 바로 대학생이 수학을 읽는 법을 배우는 방식이다. 교과서의 증명은 흔히 "명백히" 또는 "따라서 ∎"라고 말하는데, 그것이 정말로 그런지 확인하는 것도 읽는 사람의 일이다.

생각해 보기 4단계에서는 "k를 S에 속하는 가장 작은 양의 정수로 정의한다"고 한다. 왜 그렇게 할 수 있을까? S가 양의 **실수**의 집합이라도 이렇게 할 수 있을까?

공집합이 아닌 양의 정수의 집합에는 언제나 가장 작은 원소가 있다. 이를 **정렬성 원리**(well-ordering principle)라 하며, 이는 수학적 귀납법(mathematical induction)의 원리와 동치이다. 양의 실수의 집합에 대해서는 이것이 **거짓**이다. 집합 $\{x : x > 0\}$에는 가장 작은 원소가 없다. 따라서 4단계는 3단계(S가 공집합이 아니어야 한다는 것)와 S가 정수로 이루어져 있다는 사실에 의존한다.

차근차근 풀기

1단계 3단계: S는 공집합이 아니다

생각해 보기 양의 정수 a, b에 대해 $\sqrt{2} = a/b$라면, S의 원소 하나를 적을 수 있는가?

$\sqrt{2} = a/b$이면 $b\sqrt{2} = a$이고, 이는 정수이다. 따라서 b는 S에 속하고, S는 공집합이 아니다.

2단계 5단계: 더 작은 원소

이제 k가 S의 가장 작은 원소이므로 $k\sqrt{2}$는 정수이다. 이것을 j라 하자.

잠깐, 직접 해 보기 $(\sqrt{2}-1)k$가 S에 속함을 보이려면 세 가지를 확인해야 한다. 그것은 무엇인가?

$(\sqrt{2}-1)k$가 (a) 정수이고, (b) 양수이며, (c) 여기에 $\sqrt{2}$를 곱하면 정수가 됨을 보여야 한다.

- (a) $(\sqrt{2}-1)k = k\sqrt{2} - k = j - k$이므로 정수의 차이다.
- (b) $\sqrt{2} > 1$이므로 $\sqrt{2} - 1 > 0$이고, 따라서 $(\sqrt{2}-1)k > 0$이다.
- (c) $(\sqrt{2}-1)k \cdot \sqrt{2} = 2k - k\sqrt{2} = 2k - j$이므로 정수이다.

따라서 $(\sqrt{2}-1)k \in S$이다.

3단계 6단계: 모순

생각해 보기 $\sqrt{2} - 1$은 얼마나 큰가?

$1 < \sqrt{2} < 2$이므로 $0 < \sqrt{2} - 1 < 1$이고, 따라서 $(\sqrt{2}-1)k < k$이다. S의 가장 작은 원소인 k보다 더 작은 S의 원소를 찾은 것이다. 이는 불가능하므로 1단계의 가정이 거짓이었다. 즉 $\sqrt{2}$는 무리수이다. ∎

"기약분수"나 짝수와 홀수에 관한 어떤 사실도 필요하지 않았다는 점에 주목하라. 증명 전체는 세 가지 사실에 기대고 있다. $\sqrt{2} \cdot \sqrt{2}$가 정수라는 것, $\sqrt{2}$가 연속한 두 정수 사이에 엄격하게 놓여 있다는 것, 그리고 정수가 정렬성을 가진다는 것이다.

4단계 세제곱근: 두 수를 연결하기

$c = 2^{1/3}$이라 하면 $c^2 = 2^{2/3}$이고 $c^3 = 2$이다.

생각해 보기 c가 유리수(rational)이면 c^2도 유리수인가? 또 c^2이 유리수이면 곱셈과 나눗셈만으로 c로 되돌아갈 수 있는가?

c가 유리수이면 $c^2 = c \times c$도 유리수이다. 거꾸로 c^2이 유리수이면 $2/c^2 = c^3/c^2 = c$도 유리수이다. 따라서 $2^{1/3}$이 유리수일 필요충분조건은 $2^{2/3}$이 유리수인 것이다. ■

5단계 논증을 변형하기

생각해 보기 소문항 (i)에서 핵심은 $(\sqrt{2})^2 = 2$가 정수라는 것이었고, 그래서 S의 원소에 $\sqrt{2}$를 두 번 곱하면 다시 정수로 돌아온다. $c = 2^{1/3}$의 경우에는 세 번 곱해야 한다. 집합 S를 어떻게 바꾸어야 할까?

c가 유리수라고 가정하자. 그러면 c^2도 유리수이다. 다음과 같이 정의한다.

$$S = \{n \text{ 은 양의 정수} : nc \text{ 와} nc^2 \text{ 이 모두 정수}\}.$$

- **S는 공집합이 아니다.** $c = a/b$이고 $c^2 = a'/b'$이면 bb'는 S에 속한다.
- **S의 가장 작은 원소를 k라 하고** $(c-1)k$를 생각하자. $1^3 < 2 < 2^3$이므로 $1 < c < 2$이고, 따라서 $0 < (c-1)k < k$이다.
- **이것은 정수이다:** $(c-1)k = kc - k$.
- **c를 곱하면:** $(c-1)k \cdot c = kc^2 - kc$이므로 정수이다.
- **c^2을 곱하면:** $(c-1)k \cdot c^2 = kc^3 - kc^2 = 2k - kc^2$이므로 정수이다.

따라서 $(c-1)k \in S$이고 이것은 k보다 작으므로 모순이다. 그러므로 $2^{1/3}$은 무리수이고, 4단계에 의해 $2^{2/3}$도 무리수이다. ■

돌아보기

- **"가장 작은 것을 잡아라"는 하나의 증명 기법이다.** 반례가 존재한다고 가정하고, 그중 가장 작은 것을 잡은 다음, 그보다 더 작은 반례를 만들어 낸다. 이를 **극단 원리**(extremal principle) 또는 **최소 반례**(minimal counterexample) 논법이라 한다.
- **집합 S가 장부 정리를 맡았다.** 분자와 분모를 이리저리 다루는 대신 "좋은" 곱수를 모두 하나의 집합에 모았다.
- **일반화한다는 것은 증명이 실제로 무엇 때문에 성립했는지 묻는 것이었다.** $\sqrt{2}$의 경우에는 $\sqrt{2}$를 한 번 곱하는 것으로 충분했고, $\sqrt[3]{2}$의 경우에는 두 번이 필요했다. 이 점을 알아차리자 S를 어떻게 다시 정의해야 할지 정확히 알 수 있었다.

숨은 수학

그림으로 그릴 수 있는 증명

소문항 (i) 뒤에는 Stanley Tennenbaum이 고안한 아름다운 그림이 있다. $\sqrt{2} = a/b$이면 $a^2 = 2b^2$이다. 즉 한 변이 a인 정사각형의 넓이는 한 변이 b인 정사각형 두 개의 넓이와 같다. 그림 1.3.1처럼 두 개의 b-정사각형을 a-정사각형의 서로 마주 보는 모서리에 놓자. 둘은 작은 정사각형 하나에서 겹치고, 작은 정사각형 두 개를 덮지 못한 채 남긴다. 넓이가 같으므로 겹친 부분은 덮이지 않은 두 정사각형을 합한 것과 넓이가 같아야 하고, 따라서 같은 성질을 가진 **더 작은** 정수 쌍이 생긴다. 점점 더 작은 쌍이 끝없이 이어질 수는 없으므로 그런 정사각형은 존재하지 않는다. 더 작은 쌍은 정확히 $(2b - a,\ a - b)$이며, 이것은 바로 우리의 $(\sqrt{2} - 1)k$ 단계가 모습을 바꾼 것이다.

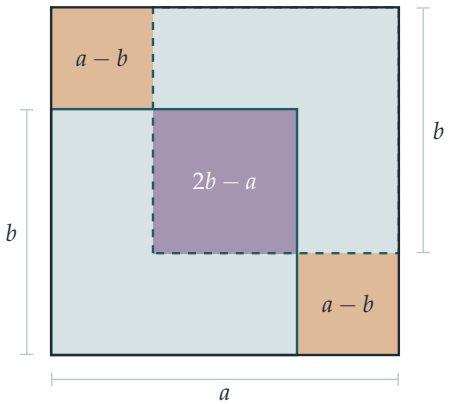


그림 1.3.1 Tennenbaum의 증명. 한 변이 b인 정사각형 두 개(청록색)가 한 변이 a인 정사각형의 마주 보는 모서리에 놓여 있다. $a^2 = 2b^2$이면 두 번 센 넓이(자주색으로 겹친 부분)는 빠진 넓이(호박색의 두 모서리)와 같아야 하므로 $(2b - a)^2 = 2(a - b)^2$이다. 즉 더 작은 해가 생긴다.

정렬성, 귀납법, 그리고 강하법

정렬성 원리와 귀납법의 원리는 논리적으로 동치이다. 즉 어느 하나로부터 다른 하나를 증명할 수 있다. 대학에서는 두 원리가 모두 자연수의 기초로 쓰이는 것을 보게 될 것이다. Section 1.5에서는 같은 원리를 다른 형태, 곧 페르마(Fermat)의 **무한 강하법**(method of infinite descent)으로 사용할 것이다. 양의 정수로 이루어진 무한한 순감소수열은 존재하지 않는다는 것이다.

어디까지 갈 수 있을까?

이 논증으로 N이 완전제곱수(perfect square)가 아닐 때마다 $\sqrt{N}$이 무리수임을 증명할 수 있으며(연습문제 참고), 더 일반적으로 자연수의 n제곱근은 자연수이거나 무리수임을 증명할 수 있다. 대학에서는 이것이 **대수적 정수**(algebraic integers)에 관한 명제가 된다. $x^3 - 2 = 0$처럼 정수 계수를 가지고 최고차항의 계수가 1인 다항식(monic polynomial) 방정식을 만족하는 유리수는 반드시 정수여야 한다. 이 아이디어는 Section 6.3에서 다시 만나게 된다.

피타고라스학파(Pythagoreans)가 $\sqrt{2}$의 무리성을 폭로했다는 이유로 히파소스(Hippasus)를 물에 빠뜨려 죽였다는 전설은 아마 사실이 아닐 것이다. 사실인 것은 이 발견 때문에 그리스 수학자들이 수에 대한 연구와 길이에 대한 연구를 분리할 수밖에 없었다는 점이며, 이 분열은 19세기에 이르러 데데킨트(Dedekind)가 실수를 구성하고 나서야 비로소 메워졌다.

사고 기술

극단 원리

어떤 일이 결코 일어나지 않음을 보이고 싶다면, 그 일이 일어난다고 가정하고, 가장 작은(또는 가장 큰, 또는 가장 단순한) 경우를 골라, 그것으로 그보다 더 작은 경우를 만들어라.

"가장 작은"이 무엇을 뜻하는지 정하는 것이 창의적인 단계이다. 여기서는 $n\sqrt{2}$를 정수로 만드는 가장 작은 n이었다.

더 도전하기

1 **다른 제곱근.** 이 논증을 변형하여 $\sqrt{3}$이 무리수임을 보여라. 어떤 수가 $\sqrt{2}-1$의 역할을 하는가?

2 **완전제곱수가 아닌 모든 수.** N을 완전제곱수가 아닌 양의 정수라 하고, m을 $m < \sqrt{N} < m+1$을 만족하는 정수라 하자. $(\sqrt{N} - m)k$를 생각하여 $\sqrt{N}$이 무리수임을 증명하여라.

3 **결함을 찾아라.** 이 논증을 $\sqrt{4}$에 적용해 보아라. 정확히 어느 단계가 실패하는가?

4 **Tennenbaum의 그림.** 그림 1.3.1을 이용하여 $a^2 = 2b^2$이면 $(2b-a)^2 = 2(a-b)^2$임을 보여라. 이 항등식을 대수적으로도 확인하여라.

더 읽을거리

- **Daniel Velleman, *How to Prove It*** (Cambridge University Press). 귀납법과 정렬성을 포함하여 증명을 꼼꼼하게 소개하는 입문서이다.
- **R. P. Burn, *A Pathway into Number Theory*** (Cambridge University Press). 세심하게 순서를 정한 질문들로만 이루어진 책으로, 대학 1학년 강의를 준비하기에 이상적이다.
- **John Conway & Joseph Shipman, "Extreme proofs I: the irrationality of $\sqrt{2}$"** (*Mathematical Intelligencer*, 2013). 하나의 사실에 대한 여러 증명을 재치 있게 비교한다.

1.4 e는 무리수이고, e^2도 그렇다

이 절에서는 두 문제를 다룬다. 1997년의 첫 번째 문제는 e가 무리수(irrational number)임을 증명(proof)한다. 2024년의 두 번째 문제는 같은 아이디어를 더 교묘하게 변형하여 e^2이 무리수임을 증명하는데, 이것은 실제로 훨씬 어렵다.

준비 문제

STEP III 1997, 7번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/97-s3-q7`

본 문제

STEP III 2024, 7번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 OCR에서 내려받을 수 있는 2024년 STEP 시험지 묶음(zip 파일) 가운데 STEP III 시험지에 있다:

`www.ocr.org.uk/Images/725753-2024-past-papers.zip`

도입

Section 1.3에서는 $\sqrt{2}$가 간단한 방정식 $x^2 = 2$를 만족한다는 사실을 이용하여 $\sqrt{2}$가 무리수임을 증명하였다. 그러나 e는 우리가 아는 한 그런 방정식을 전혀 만족하지 않는다. 우리가 가진 것은 그 급수(series)뿐이다.

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots .$$

급수가 어떻게 어떤 수가 분수가 아니라는 것을 알려 줄 수 있을까?

그 답은 수론(number theory)에서 가장 유용한 아이디어 가운데 하나이다. **정수**(*integer*)는 **0과 1 사이에 엄격하게 놓일 수 없다.** 어떤 양이 정수임을 보이고, 동시에 그 양이 0과 1 사이에 엄격하게 놓임을 보일 수 있다면 모순(contradiction)이 생긴다. 이 절의 모든 내용은 이 주제의 변주이다.

시작하기 전에

생각해 보기 $e = p/q$라고 가정하자. e에 q를 곱하면 정수가 된다. e의 급수의 각 항에 $q!$을 곱하면 어떻게 되는가?

$k \le q$이면 $\dfrac{1}{k!}$에 $q!$을 곱한 값은 정수이다. 따라서 $q!\,e$는 정수 부분(처음 $q+1$개의 항)과 "꼬리(tail)"(그 뒤의 모든 항)로 나뉜다. $e = p/q$이면 $q!\,e$ 자체가 정수이므로 꼬리도 정수여야 한다. 계획은 꼬리가 0과 1 사이에 엄격하게 놓임을 보이는 것이다.

차근차근 풀기

1단계 준비 문제: e는 무리수이다

급수 b_n은 첫째항과 공비가 모두 $\frac{1}{n+1}$인 등비급수(geometric series)이므로

$$b_n = \frac{1/(n+1)}{1 - 1/(n+1)} = \frac{1}{n}.$$

생각해 보기 a_n과 b_n을 항별로 비교하라. 어느 쪽이 더 큰가?

첫째항은 서로 같다. 그 뒤로는 $(n+1)(n+2) > (n+1)^2$이고, 일반적으로 $k \ge 2$일 때 $(n+1)(n+2)\cdots(n+k) > (n+1)^k$이므로, a_n의 이후 각 항은 b_n의 대응하는 항보다 작다. 따라서 $0 < a_n < b_n = 1/n$이다.

이제 a_n이 실제로 무엇인지 살펴보자. e의 급수에 $n!$을 곱하면

$$n!\,e = \underbrace{\frac{n!}{0!} + \frac{n!}{1!} + \cdots + \frac{n!}{n!}}_{\text{정수}} + \underbrace{\frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \cdots}_{=a_n}.$$

$0 < a_n < 1$이므로 $n!\,e$의 정수 부분(integer part)은 첫 번째 묶음이고 a_n은 소수 부분(fractional part)이다. 즉 $a_n = n!\,e - [n!\,e]$이다.

잠깐, 직접 해 보기 이제 증명을 마무리하라. $e = p/q$라고 가정하자. n의 값을 무엇으로 택해야 하는가?

$n = q$로 택한다. 그러면 $q!\,e = (q-1)!\,p$는 정수이므로 그 소수 부분 a_q는 0이다. 그런데 $a_q > 0$이다. 모순이다. 따라서 e는 무리수이다. ∎

이 증명은 1815년 무렵 푸리에(Joseph Fourier)가 제시한 것이다.

2단계 e^2이 더 어려운 이유

> **생각해 보기** 같은 아이디어를 e^2에 적용해 보라. 그 급수는 $\sum 2^k/k!$이다. $n!$을 곱하고 꼬리를 살펴보면 무엇이 잘못되는가?

이제 꼬리는 $\dfrac{2^{n+1}}{n+1} + \dfrac{2^{n+2}}{(n+1)(n+2)} + \cdots$이고, 2의 거듭제곱이 모든 것을 망쳐 버린다. 꼬리가 더 이상 작지 않은 것이다. $n!$을 곱해도 분자의 2^k에는 도움이 되지 않는다.

2024년 문제의 비결은 e^2을 아예 피하는 것이다. $e^2 = p/q$이면

$$qe = \frac{p}{e}.$$

이제 두 수 e와 $1/e$가 생기는데, 각각은 계승(factorial)으로 된 급수를 가지며 골치 아픈 2의 거듭제곱이 없다.

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}, \qquad \frac{1}{e} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}.$$

3단계 두 꼬리

소문항 (i)은 준비 문제와 정확히 같다. 즉 $0 < f(n) < 1/n$이다.

소문항 (ii)에서 $g(n)$은 항의 크기가 감소하는 **교대급수**(*alternating series*)이다.

> **생각해 보기** $t_1 > t_2 > t_3 > \cdots > 0$인 교대급수 $t_1 - t_2 + t_3 - \cdots$의 합이 왜 0과 t_1 사이에 있는가?

항을 둘씩 묶으면 $(t_1 - t_2) + (t_3 - t_4) + \cdots$는 양수인 괄호들의 합이므로 양수이다. 다른 방식으로 묶으면 $t_1 - (t_2 - t_3) - (t_4 - t_5) - \cdots$는 t_1에서 양수인 괄호들을 뺀 것이므로 t_1보다 작다. 여기서 $t_1 = \frac{1}{n+1}$이고, 각 항은 앞의 항을 1보다 큰 수로 나눈 것이므로 항들은 감소한다. 따라서 $0 < g(n) < \frac{1}{n+1}$이다.

4단계 다시 정수

준비 문제에서와 똑같이 e에 $(2n)!$을 곱하고 꼬리를 떼어 내면

$$(2n)!\, e = (\text{정수}) + f(2n).$$

따라서 $(2n)!\, e - f(2n)$은 정수이다. 이제 $1/e$에 대해서도 같은 일을 하면

$$\frac{(2n)!}{e} = \sum_{k=0}^{2n} (-1)^k \frac{(2n)!}{k!} + \sum_{k=2n+1}^{\infty} (-1)^k \frac{(2n)!}{k!}.$$

생각해 보기 꼬리의 첫째항, 즉 $k = 2n+1$인 항의 부호는 무엇인가? 꼬리는 $g(2n)$과 어떤 관계인가?

꼬리의 첫째항에서 $k = 2n+1$은 홀수이므로 그 항은 음수이다. 꼬리는

$$-\frac{1}{2n+1} + \frac{1}{(2n+1)(2n+2)} - \cdots = -g(2n).$$

따라서 $\dfrac{(2n)!}{e} + g(2n)$은 정수이다. ■

문제에서 n 대신 $2n$을 쓰는 이유가 바로 이것이다. 곱하는 수가 짝수이면 $1/e$의 꼬리는 정확히 $-g$가 되어 부호를 예측할 수 있다.

5단계 모순

$qe = p/e$라고 가정하자. 양변에 $(2n)!$을 곱하고 단계 4를 이용하면

$$q\big(\text{정수} + f(2n)\big) = p\big(\text{정수} - g(2n)\big).$$

정리하면 $qf(2n) + pg(2n)$은 정수들의 조합과 같으므로 정수이다. 이것이 소문항 (iv)이다.

잠깐, 직접 해 보기 이제 단계 3에서 구한 범위를 이용하라. n이 매우 클 때 $qf(2n) + pg(2n)$은 어떻게 되는가?

$f(2n)$과 $g(2n)$은 모두 양수이므로 $qf(2n) + pg(2n) > 0$이다. 또한

$$qf(2n) + pg(2n) < \frac{q}{2n} + \frac{p}{2n+1} < \frac{p+q}{2n}.$$

$n > (p+q)/2$로 택하자. 그러면 $qf(2n) + pg(2n)$은 0과 1 사이에 엄격하게 놓인 정수이다. 이는 불가능하므로 e^2은 무리수이다. ■

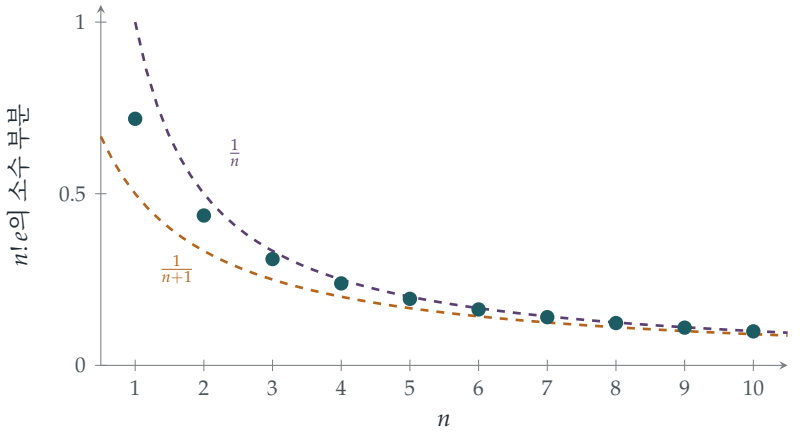


그림 1.4.1 꼬리 $a_n = n!\,e - [n!\,e]$(청록색)는 $n!\,e$의 소수 부분이다. 이 값은 언제나 $\frac{1}{n+1}$과 $\frac{1}{n}$ 사이에 엄격하게 놓인다. 결코 0이 아니지만 1보다는 작다. 만약 e가 분수 $\frac{p}{q}$라면 $n \geq q$인 모든 n에 대하여 $n!\,e$는 정수가 되고, 청록색 점들은 0이 될 것이다.

돌아보기

- **핵심 동력은 "0과 1 사이에 엄격하게 놓인 정수는 없다"는 사실이다.** 두 증명 모두 반드시 정수여야 하는 양을 만들고 그 양을 가두어 버린다.
- **계승은 꼬리를 작게 만든다.** $n!$을 곱하면 급수의 앞부분은 정수가 되고, $1/n$처럼 줄어드는 꼬리가 남는다.
- **정면 공격이 실패하면 식을 바꾸어 써라.** $e^2 = p/q$를 정면으로 공략하는 대신 $qe = p/e$로 바꾸어 써서, 어려움을 더 쉬운 두 수에 나누어 실었다.
- **세부 사항이 중요하다.** n 대신 $2n$을 택함으로써 꼬리의 부호가 정해졌다. 많은 증명이 이런 작은 세부 사항에 달려 있다.

숨은 수학

e는 얼마나 무리수인가?

리우빌(Joseph Liouville)은 1840년에 e^2이 무리수임을, 더 나아가 정수 계수(coefficient)를 갖는 어떤 이차방정식(quadratic equation)도 만족하지 않음을 증명하였다. 1873년 에르미트(Charles Hermite)는 훨씬 더 나아가 e가 **초월수**(*transcendental number*)임을, 즉 정수 계수를 갖는 어떤 다항식(polynomial)의 근도 아님을 증명하였다. 그의 증명은 바로

위의 논증, 즉 정수를 만들고 그것이 0과 1 사이에 엄격하게 놓임을 보이는 논증을 정교하게 발전시킨 것이다. 9년 뒤 린데만(Ferdinand von Lindemann)은 에르미트의 방법을 응용하여 π가 초월수임을 보였고, 이로써 자와 컴퍼스로 "원을 정사각형으로 만드는" 고대의 문제가 불가능하다는 것이 마침내 증명되었다.

아직 모르는 것

이 방법들이 이토록 강력한데도, 민망할 정도로 간단한 질문들이 여전히 풀리지 않은 채 남아 있다. $e+\pi$는 무리수인가? $e\pi$는? 둘 중 적어도 하나는 초월수여야 하지만(연습문제 4), 아무도 모른다. $\zeta(3) = 1 + \frac{1}{8} + \frac{1}{27} + \cdots$은 무리수인가? 그렇다. 아페리(Roger Apéry)가 1978년에 이를 증명하여 수학계를 놀라게 하였다. $\zeta(5)$는? 아무도 모른다.

근사

이 증명들의 바탕에는 더 깊은 아이디어가 있다. 어떤 수가 분수로 **지나치게 잘** 근사된다면 그 수는 무리수라는 것이다. e의 급수의 부분합(partial sum)은 매우 빠르게 e에 아주 가까워지는 분수들이다. 분수는 다른 분수들로 그만큼 잘 근사될 수 없다. 이것이 **디오판토스 근사**(*Diophantine approximation*)의 출발점이다. 이 수론의 분야는 Section 2.9에서 더 탐구할 수 있는데, 그곳에서는 다른 적분들의 모임이 e에 더욱 가깝게 다가가는 분수들을 만들어 낸다.

사고 기술

정수 가두기

어떤 수가 무리수임을 증명하려면, 그 수가 분수라고 가정하고, 그로부터 반드시 정수여야 하는 양을 만든 다음, 그 양이 0과 1 사이에 엄격하게 놓임을 보인다.

기술의 핵심은 그 양을 고르는 데 있다. 여기서는 계승을 곱하여 급수의 대부분을 정수로 만들고, 작지만 양수인 꼬리를 남겼다.

더 도전하기

1 **$1/e$만 이용하기.** $1/e = p/q$라고 가정하고 $1/e$의 교대급수만을 이용하여 e가 무리수임을 증명하라.

2 $\sin 1$**은 무리수이다.** $\sin 1 = 1 - \frac{1}{3!} + \frac{1}{5!} - \cdots$을 이용하여 $\sin 1$이 무리수임을 증명하라. (적당한 홀수의 계승을 곱하라.)

3 π**는 왜 안 되는가?** 이 방법이 π에 직접 적용되지 않는 이유를 설명하라. 그런 다음 급수 대신 적분을 이용하여 π가 무리수임을 보인 Ivan Niven의 한 쪽짜리 증명(1947)을 찾아보라. 실력 있는 A 레벨(A level, 영국의 대학 입학 자격 시험) 학생이라면 충분히 이해할 수 있다.

4 **둘 중 하나는 초월수이다.** 심화 e와 π가 $x^2 - (e+\pi)x + e\pi = 0$의 근임을 보여라. 계수가 대수적 수(algebraic number)인 다항식의 근은 그 자체로 대수적 수이며, π는 대수적 수가 아니라는 사실(린데만)을 가정해도 좋다. 이로부터 $e+\pi$와 $e\pi$ 중 적어도 하나는 초월수임을 이끌어 내라.

더 읽을거리

- **Aigner & Ziegler,** ***Proofs from THE BOOK***, 제8장 "Some irrational numbers"(몇 가지 무리수). 바로 이 아이디어들을 이용하여 e, e^2, e^4, π^2이 무리수임을 증명한다.
- **Ivan Niven,** ***Irrational Numbers*** (Mathematical Association of America). $\sqrt{2}$부터 초월성까지 모든 것을 다루는 짧은 고전이다.
- **Julian Havil,** ***The Irrationals*** (Princeton University Press). 무리수의 역사를 읽기 쉽게 풀어 쓴 책이다.

1.5 무한 강하법

문제

STEP III 2022, 2번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 OCR에서 내려받을 수 있는 2022년 STEP 시험지 묶음(zip 파일) 가운데 STEP III 시험지에 있다:

`www.ocr.org.uk/Images/696587-2022-past-papers.zip`

도입

방정식에 정수해가 **없음**을 어떻게 증명할 수 있을까? 모든 경우를 다 확인해 볼 수는 없다. 경우가 무한히 많기 때문이다. 1630년대에 페르마(Pierre de Fermat)가 한 가지 방법을 찾아냈다. 어떤 해가 있다면 그로부터 **더 작은** 수로 이루어진 또 다른 해가 만들어지고, 다시 그보다 더 작은 해가 만들어지며, 이것이 끝없이 계속된다는 것을 보이는 것이다. 그런데 양의 정수는 영원히 계속 작아질 수 없다. 따라서 애초에 해는 존재하지 않았던 것이다.

페르마는 이것을 **무한 강하법**(method of infinite descent)이라 불렀고, 이 방법을 무척 자랑스러워했다. 이는 Section 1.3에서 본 정렬 원리(well-ordering principle)의 뒷면이며, 지금도 방정식에 해가 없음을 증명하는 주요 도구 가운데 하나이다.

시작하기 전에

네 소문항은 모두 구조가 같다. 해가 있다고 가정하고, 그 해를 줄이고, 모순을 이끌어 낸다. 문제는 **어떻게** 줄이느냐이다.

생각해 보기 소문항 (i)에서 $a^3 + 2b^3 + 4c^3 = 0$을 보자. 세 항 가운데 두 항은 분명히 짝수이다. 이것은 나머지 한 항에 대해 무엇을 알려 주는가?

모든 강하는 바로 이런 관찰에서 시작한다. 어떤 나누어떨어짐(divisibility)이 저절로 강제되는 것이다.

차근차근 풀기

1단계 첫 번째 강하

$a^3 = -2b^3 - 4c^3$이므로 a^3은 짝수이고, 따라서 a도 짝수이다(홀수의 세제곱은 홀수이다). $a = 2p$로 놓자. 그러면 $|p| = |a|/2 < |a|$이고, 대입하면

$$8p^3 + 2b^3 + 4c^3 = 0 \quad \Longrightarrow \quad 4p^3 + b^3 + 2c^3 = 0.$$

> **생각해 보기** 새 방정식은 $4p^3 + b^3 + 2c^3 = 0$이다. 계수는 같고 순서만 돌아갔다. 같은 방법을 다시 쓸 수 있을까?

이제 $b^3 = -4p^3 - 2c^3$이 짝수이므로 $b = 2q$이고 $|q| < |b|$이며, 2로 나누면 $2p^3 + 4q^3 + c^3 = 0$을 얻는다. 한 번 더, c는 짝수여야 한다. $c = 2r$이고 $|r| < |c|$이며, 2로 나누면

$$p^3 + 2q^3 + 4r^3 = 0.$$

이것은 a, b, c 자리에 p, q, r가 들어간 **원래** 방정식이다. 각각은 크기가 절반이고, 어느 것도 0이 아니다. 0이 아닌 수를 반으로 나누어 0이 될 수는 없기 때문이다.

> **잠깐, 직접 해 보기** 이것을 0이 아닌 해가 존재하지 않는다는 증명으로 바꾸어 보라. 정확히 무엇을 "가장 작다"고 가정해야 할까?

0이 아닌 정수로 이루어진 모든 해 가운데 $|a|$가 가장 작은 해를 하나 고른다. (해가 하나라도 있다면 정렬 원리에 의해 이렇게 할 수 있다.) 위의 논증은 $|p| < |a|$인 또 다른 0이 아닌 해를 만들어 내므로 최소성에 모순이다. 따라서 0이 아닌 해는 없다. ■

같은 내용을 이렇게 말할 수도 있다. 해가 하나 있으면 $|a| > |p| > \cdots$인 해들의 무한수열, 곧 양의 정수로 이루어진 무한한 순감소수열을 만들 수 있는데, 이는 불가능하다.

2단계 다른 소수

> **생각해 보기** $9a^3 + 10b^3 + 6c^3 = 0$에서는 홀짝성(parity)이 바로 도움이 되지는 않는다. 계수 9, 10, 6을 보자. 이 가운데 두 개를 나누는 소수는 무엇인가?

소수 3은 9와 6을 나누므로 3은 $10b^3$을 나누고, 따라서 3은 b를 나눈다. $b = 3q$로 놓고 3으로 나누면

$$3a^3 + 90q^3 + 2c^3 = 0.$$

이제 3이 $2c^3$을 나누므로 $c = 3r$이다. 다시 3으로 나누면 $a^3 + 30q^3 + 18r^3 = 0$이다. 따라서 3은 a를 나눈다. $a = 3p$로 놓고 한 번 더 3으로 나누면

$$9p^3 + 10q^3 + 6r^3 = 0.$$

정확히 원래 방정식이고, 수는 더 작은 0이 아닌 수이다. 같은 강하 논증에 의해 0이 아닌 해는 없다. ■

3단계 3을 법(modulo)으로 한 제곱수

> **생각해 보기** 모든 정수는 $3n, 3n+1, 3n-1$ 가운데 하나의 꼴이다. 이들의 제곱을 3으로 나눈 나머지는 무엇인가?

$(3n \pm 1)^2 = 9n^2 \pm 6n + 1 = 3(3n^2 \pm 2n) + 1$로, 3의 배수보다 1 크다. 그리고 $(3n)^2$은 3의 배수이다. 따라서 제곱수를 3으로 나눈 나머지는 0 또는 1이고, 결코 2가 아니다.

이제 $a^2 + b^2$이 3의 배수라면, 가능한 나머지의 합은 $0+0, 0+1, 1+0, 1+1$이고, 이는 각각 0, 1, 1, 2가 된다. 이 가운데 3의 배수는 첫 번째뿐이므로 a와 b는 모두 3의 배수여야 한다.

> **생각해 보기** $a^2 + b^2 = 3c^2$이고 $a = 3p$, $b = 3q$이면 c에 대해 무엇을 말할 수 있는가?

$9p^2 + 9q^2 = 3c^2$이므로 $c^2 = 3(p^2 + q^2)$은 3의 배수이고, 따라서 $c = 3r$이다. 그러면 $9p^2 + 9q^2 = 27r^2$이므로 $p^2 + q^2 = 3r^2$이다. 같은 방정식에 더 작은 수이다. 다시 강하이다. ■

4단계 변형: 방정식이 바뀐다

> **생각해 보기** $a^2 + b^2 + c^2 = 4abc$에서 우변은 4의 배수이다. 제곱수를 4로 나눈 나머지는 어떠한가?

짝수의 제곱은 4의 배수이고 홀수의 제곱은 4의 배수보다 1 크다($(2n+1)^2 = 4n^2 + 4n + 1$). 따라서 $a^2 + b^2 + c^2$을 4로 나눈 나머지는 a, b, c 가운데 홀수가 몇 개인지에 따라 0, 1, 2, 3 중 하나이다. 우변이 4의 배수이므로 이들 가운데 어느 것도 홀수일 수 없다. $a = 2p$, $b = 2q$, $c = 2r$로 놓으면

$$4(p^2 + q^2 + r^2) = 32\,pqr \quad \Longrightarrow \quad p^2 + q^2 + r^2 = 8\,pqr.$$

> **생각해 보기** 이것은 같은 방정식이 아니다. 4가 8로 바뀌었다. 그래도 강하가 통할까?

여기서 쓰는 요령은 **더 강한 명제를 증명하는 것**이다. 다음 꼴의 모든 방정식을 생각하자.

$$x^2 + y^2 + z^2 = 2^m\,xyz \qquad \text{단, } m \geq 2.$$

이러한 m 각각에 대해 우변은 4의 배수이므로, 완전히 같은 논증으로 x, y, z가 모두 짝수임을 보일 수 있다. 이들을 반으로 나누면 2^{m+1}이 들어간 방정식의 해가 되고, 이 방정식 역시

같은 꼴이다. 따라서 m 방정식의 0이 아닌 해로부터 $m+1$ 방정식의 더 작은 0이 아닌 해를 얻는다. 이 족의 어느 방정식이든 상관없이, 그 해들 가운데 $|x|$가 가장 작은 해를 택하면 모순이 생긴다. 특히 $a^2+b^2+c^2=4abc$는 0이 아닌 해를 갖지 않는다. ■

때로는 증명하려는 명제가 너무 약해서 스스로의 귀납법(induction)을 떠받치지 못한다. 이때의 처방은 스스로를 떠받칠 수 **있는** 더 일반적인 명제를 증명하는 것이다. 이는 대학에서 놀라울 만큼 자주 쓰이는 요령이다.

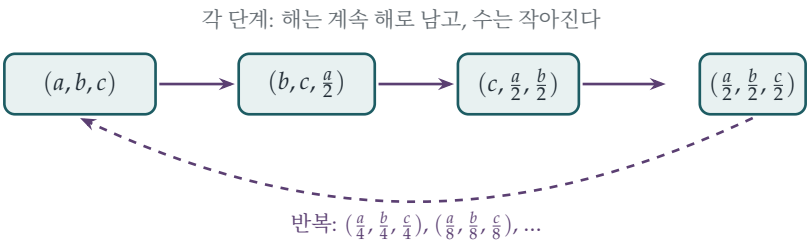


그림 1.5.1 소문항 (i)의 강하. $a^3+2b^3+4c^3=0$의 해로부터 세 단계를 거치면 모든 성분이 절반이 된 또 다른 해가 나온다. 이를 끝없이 반복하면 양의 정수로 이루어진 끝없는 감소수열 $|a|>|\frac{a}{2}|>|\frac{a}{4}|>\cdots$을 얻게 되는데, 이는 불가능하다. 따라서 처음부터 해는 없었다.

돌아보기

- **강하에는 나누어떨어짐의 원천이 필요하다.** 매번 모든 변수를 나누도록 강제되는 소수 p(여기서는 2 또는 3)를 찾아서 그것으로 나누어 없앴다.
- **그것을 찾는 방법은 n을 법으로 생각하는 것이다.** mod 2, 3 또는 4로 나머지를 살펴보니 "무엇이든 될 수 있을까?"라는 물음이 짧은 유한 검사로 바뀌었다.
- **방정식이 바뀌면 일반화하라.** 소문항 (iv)에서는 강하 단계에 대해 닫혀 있는 방정식의 족 전체가 필요했다.

숨은 수학

페르마, 강하법, 그리고 마지막 정리

페르마는 무한 강하법을 이용하여 $x^4+y^4=z^2$이 양의 정수해를 갖지 않음을 증명하였다. 이것은 그 유명한 "마지막 정리"(Last Theorem) 가운데 그가 증명을 남긴 유일한 경우이며, $x^n+y^n=z^n$의 $n=4$인 경우를 해결한다. 이후 오일러(Euler)가 강하법을 써서 $n=3$인 경우를 증명했는데, 그 증명에 있던 빈틈은 나중에 메워졌다. 강하법은 지

금도 현대 이론의 출발점이다. Section 1.9에 나온 것과 같은 곡선에 관한 모델-베유 정리(Mordell–Weil theorem)의 증명은 정교한 강하법이다.

국소적 장애

이 절의 모든 증명은 어떤 수를 법으로 한 나머지를 살펴보는 방식이었다. 어떤 방정식이 어떤 n에 대해 n을 법으로 해를 갖지 않거나 실수해를 갖지 않는다면, 당연히 정수해도 갖지 않는다. 이러한 이유를 **국소적 장애**(local obstructions)라 하며, 대학에 가면 $p, p^2, p^3, \ldots$를 법으로 한 모든 나머지를 한꺼번에 연구하는 방법인 p-**진수**(p-adic numbers)를 만나게 된다.

하세(Hasse)와 민코프스키(Minkowski)의 멋진 정리에 따르면, $a^2 + b^2 = 3c^2$과 같은 이차 방정식에서는 국소적 장애가 유일한 장애이다. 즉 실패할 "국소적" 이유가 없다면 실제로 유리수해가 존재한다. 삼차 방정식에서는 이것이 극적으로 무너진다. 1951년 Ernst Selmer는

$$3x^3 + 4y^3 + 5z^3 = 0$$

이 모든 정수를 법으로 해를 갖고 실수해도 갖지만, 0이 아닌 정수해는 갖지 않음을 보였다. "국소-대역" 원리(local-to-global principle)가 언제, 왜 실패하는지 설명하는 것은 현대 정수론의 주요 주제이다.

해를 갖는 방정식

소문항 (iv)에는 유명한 사촌이 있다. 바로 $x^2 + y^2 + z^2 = 3xyz$, 곧 **마르코프 방정식**(Markov equation)이다. 이 방정식은 $(1,1,1)$, $(1,1,2)$, $(1,2,5)$, $(1,5,13)$, $(2,5,29)$로 시작하는 양의 정수해를 무한히 많이 가지며, 이 해들은 무리수가 분수로 얼마나 잘 근사될 수 있는지와 관련되어 있다. 연습문제 4를 보라.

사고 기술

무한 강하법

방정식에 해가 없음을 보이려면, 어떤 해든 그보다 엄격하게 더 작은 해를 만들어 냄을 보여라. 그러면 가장 작은 해는 존재할 수 없다.

이를 n을 법으로 생각하는 방법과 짝지어 강하를 이끄는 나누어떨어짐을 찾고, 명제가 강하 단계에서 보존되지 않으면 명제를 일반화할 준비를 하라.

더 도전하기

1 **STEP I 준비 운동.** (*STEP I 2010 8*번 문항.) $a^3 + 3b^3 = 9c^3$의 유일한 정수해가 $a = b = c = 0$임을 보여라. 그다음, 일의 자리 숫자를 생각하여 $p^4 + 2q^4 = 5r^4$에 대해서도 같은 사실을 보여라.

2 **강하가 필요 없는 법.** 4를 법으로 생각하는 것만으로 $x^2 + y^2 = 4z + 3$이 정수해를 전혀 갖지 않음을 보여라.

3 **유리점.** 소문항 (iii)을 이용하여 원 $x^2 + y^2 = 3$ 위에 **유리수** 좌표를 갖는 점이 없음을 보여라. ($(1,1)$을 지나는 $x^2 + y^2 = 2$와 비교해 보라.)

4 **마르코프 세쌍.** (x,y,z)가 $x^2 + y^2 + z^2 = 3xyz$를 만족하면 $(x,y,3xy - z)$도 이를 만족함을 보여라. $(1,1,1)$에서 시작하여 위에 나열한 세쌍들을 만들어 보라. (이 "도약" 요령은 강하와 반대 방향이다.)

더 읽을거리

- **Harold Davenport, *The Higher Arithmetic,*** 2장과 5장.
- **Joseph Silverman, *A Friendly Introduction to Number Theory*** (Pearson). 매우 읽기 쉽다. $x^4 + y^4 = z^2$에 대한 페르마의 강하법 증명이 실려 있다.
- **Simon Singh, *Fermat's Last Theorem*** (Fourth Estate). 페르마가 여백에 남긴 메모부터 와일스(Wiles)의 증명까지의 이야기를 일반 독자를 위해 풀어낸 책이다.

1.6 두 제곱수의 합

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`

도입

어떤 자연수를 두 제곱수의 합(sum of two squares)으로 나타낼 수 있을까? $5 = 1^2 + 2^2$와 $13 = 2^2 + 3^2$는 그렇게 나타낼 수 있지만, 3, 7, 21은 그렇지 않다. 그런데 이상한 사실이 하나 있다. $65 = 5 \times 13$은 $1^2 + 8^2$와 $4^2 + 7^2$의 **두** 가지 서로 다른 방법으로 두 제곱수의 합으로 나타낼 수 있다. 이런 수 두 개를 곱하면 왜 또 이런 수가 되며, 왜 그 방법이 두 가지일까?

답은 뜻밖의 방향에서 나온다. 이 문제는 자연수를 떠나 **복소수**(*complex number*)를 다루도록 요구한다. 복소수에서는 두 제곱수의 합이 단순해지고, 언뜻 당혹스러워 보이는 계산이 거의 기계적인 작업이 된다.

시작하기 전에

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

그 값은 $a^2 + b^2$, 곧 두 제곱수의 합이다. 따라서 "N이 두 제곱수의 합이다"는 정확히 "실수부와 허수부가 정수인 어떤 복소수 z에 대하여 $N = |z|^2$이다"라는 뜻이다. 이와 같은 복소수를 **가우스 정수**(*Gaussian integers*)라고 한다. 이 바꿔 읽기를 꼭 기억해 두자. 문제 전체가 여기에 달려 있다.

차근차근 풀기

1단계 **절댓값은 곱해진다**

생각해 보기 zw를 a, b, c, d로 나타내어 보자. $|zw|^2$에 대하여 무엇을 보여야 하는가?

$zw = (ac - bd) + \mathrm{i}(ad + bc)$이므로

$$|zw|^2 = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2,$$

이다. 교차항 $-2abcd$와 $+2abcd$가 서로 지워지기 때문이다. 그리고 이 식은 다음과 같이 인수분해된다.

$$a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = |z|^2|w|^2.$$

양변의 제곱근을 취하면 $|zw| = |z||w|$이다. ■

이제 이것을 자연수에 대한 명제로 읽어 보자.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (\star)$$

두 제곱수의 합 두 개를 곱하면 다시 두 제곱수의 합이 된다. 그리고 복소수는 그 두 제곱수가 정확히 무엇인지 알려 준다.

2단계 활용하기

소문항 (ii): $5 = |2 + \mathrm{i}|^2$이고 $221 = 10^2 + 11^2 = |10 + 11\mathrm{i}|^2$이다. 그러므로 곱하면

$$(2 + \mathrm{i})(10 + 11\mathrm{i}) = 20 + 22\mathrm{i} + 10\mathrm{i} - 11 = 9 + 32\mathrm{i},$$

이고, 따라서 $5 \times 221 = 9^2 + 32^2$이다. (검산: $81 + 1024 = 1105$.)

생각해 보기 대신 $10 + 11\mathrm{i}$에 $2 - \mathrm{i}$를 곱하면 어떻게 될까? 이 수는 $2 + \mathrm{i}$와 절댓값(modulus)이 같다.

$(2 - \mathrm{i})(10 + 11\mathrm{i}) = 20 + 22\mathrm{i} - 10\mathrm{i} + 11 = 31 + 12\mathrm{i}$이므로 $1105 = 31^2 + 12^2$이기도 하다. $2 + \mathrm{i}$를 고르느냐 그 켤레복소수(conjugate)를 고르느냐에 따라 서로 다른 표현이 나온다. 도입에서 본 65의 두 가지 표현도 이것으로 설명된다(그림 1.6.1). $65 = |(2 + \mathrm{i})(3 + 2\mathrm{i})|^2 = |4 + 7\mathrm{i}|^2$이고 $65 = |(2 - \mathrm{i})(3 + 2\mathrm{i})|^2 = |8 + \mathrm{i}|^2$이다.

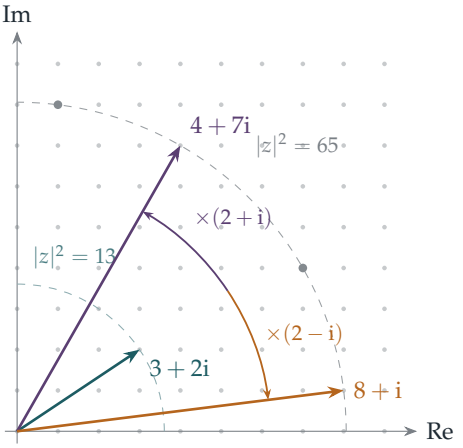


그림 1.6.1 $2 \pm \mathrm{i}$를 곱하면 길이가 $\sqrt{5}$배가 되고 약 26.6°만큼 회전한다. $2+\mathrm{i}$는 시계 반대 방향, $2-\mathrm{i}$는 시계 방향으로 회전시킨다. 원 $|z|^2 = 13$ 위의 $3+2\mathrm{i}$에서 출발하면, 두 선택은 원 $|z|^2 = 65$ 위의 서로 다른 격자점(lattice point)에 도달한다. 회색 점은 이 두 점을 직선 $y = x$에 대하여 대칭이동한 점이다.

3단계 먼저 인수분해하기

? **생각해 보기** 8045는 일의 자리 숫자가 5이다. 이것은 무엇을 시사하는가?

$8045 = 5 \times 1609$이다. 1609를 두 제곱수의 합으로 나타내야 하는데, 1609보다 조금 작은 제곱수들을 시험해 보면 곧 $1609 = 40^2 + 3^2$을 찾을 수 있다. 그러면

$$(2+\mathrm{i})(40+3\mathrm{i}) = 77 + 46\mathrm{i}, \qquad \text{이므로} \qquad 8045 = 77^2 + 46^2,$$

이고, 켤레복소수를 쓰면 $8045 = 83^2 + 34^2$도 얻는다.

소문항 (iv)는 더 빠르다. $36 = 6^2 + 0^2$이고, 6을 곱하는 것은 단지 크기를 늘리는 것이므로 $36 \times 50805 = 612^2 + 1206^2$이다.

4단계 세 가지 방법

? **생각해 보기** 25는 두 제곱수의 합으로 나타내는 방법이 둘 이상이다. 부호와 순서 바꾸기를 같은 것으로 볼 때, 절댓값이 5인 가우스 정수는 몇 개인가?

$25 = 5^2 + 0^2 = 3^2 + 4^2$이고, 이는 5, $3+4\mathrm{i}$, $3-4\mathrm{i}$에 대응한다. 다음으로 1002082를 보자. $1001^2 = 1002001$이므로 $1002082 = 1001^2 + 9^2$이다. $1001 + 9\mathrm{i}$에 세 수를 각각 곱하면 다음

을 얻는다.

$$5\,(1001+9\mathrm{i}) = 5005+45\mathrm{i},$$
$$(3+4\mathrm{i})(1001+9\mathrm{i}) = 2967+4031\mathrm{i},$$
$$(3-4\mathrm{i})(1001+9\mathrm{i}) = 3039-3977\mathrm{i}.$$

따라서 세 순서쌍 (r,s)는 $(45,5005)$, $(2967,4031)$, $(3039,3977)$이다.

5단계 나누기

> **잠깐, 직접 해 보기** 소문항 (vi)은 이 장치를 거꾸로 돌린다. $109 = 10^2+3^2$이고 $1002037 = 1001^2+6^2$임을 알고 있다. 일일이 찾아보지 않고 9193을 두 제곱수의 합으로 나타내려면 어떻게 해야 할까?

가우스 정수를 곱하면 절댓값이 곱해지므로, **나누면** 절댓값도 나누어질 것이다. 다음을 계산해 보자.

$$\frac{1001+6\mathrm{i}}{10+3\mathrm{i}} = \frac{(1001+6\mathrm{i})(10-3\mathrm{i})}{109} = \frac{10028-2943\mathrm{i}}{109} = 92-27\mathrm{i}.$$

나누어떨어지므로 $9193 = 92^2+27^2$이다. (검산: $8464+729=9193$.)

> **생각해 보기** 대신 $10-3\mathrm{i}$로 나누면 어떻게 될까?

그러면 $(1001+6\mathrm{i})(10+3\mathrm{i})/109 = (9992+3063\mathrm{i})/109$를 얻는데, $9992/109$가 정수가 아니므로 이것은 가우스 정수가 **아니다**. 주어진 자연수를 나누는 소수(prime)가 일부뿐인 것처럼, 두 "109의 인수" 가운데 하나만이 $1001+6\mathrm{i}$를 나눈다. 가우스 정수에는 그 나름의 소수와 그 나름의 인수분해가 있다.

돌아보기

- **바꿔 읽고, 풀고, 다시 바꿔 읽기.** "두 제곱수의 합"은 "가우스 정수의 절댓값의 제곱"이 되었다. 그 언어로 보면 문제는 쉬웠다.
- **먼저 인수분해하기.** 모든 소문항은 큰 수를, 표현을 쉽게 찾을 수 있는 작은 수들로 쪼개는 것에서 시작했다.
- **켤레복소수는 새로운 답을 준다.** 표현의 개수는 각 인수와 그 켤레복소수 가운데 하나를 고르는 방법이 몇 가지인지에 따라 정해진다.

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 계속 소수로 남는다. 예를 들어 $5 = (2 + i)(2 - i)$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 $\pm i$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 $\mathbb{Z}[i]$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.

사고 기술

> **무대 바꾸기**
>
> 한 수 체계에서 다루기 어색한 문제가 더 큰 수 체계에서는 자연스러울 수 있다.
>
> 두 제곱수의 합은 정수에서는 다루기 어색하지만, 복소수에서는 그저 절댓값일 뿐이다. 수학자들은 끊임없이 이런 식으로 수 체계를 확장한다. 정수에서 유리수로, 유리수에서 실수로, 실수에서 복소수로. 확장할 때마다 오래된 문제 몇 가지가 쉬워진다.

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 $3 = (a+bi)(c+di)$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.

1.7 인수분해가 무너질 때

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`

도입

1보다 큰 모든 자연수는 소수(prime)의 곱으로 나타내는 방법이 정확히 한 가지뿐이다. 예를 들어 $60 = 2 \times 2 \times 3 \times 5$이며, 다른 방법은 없다. 아마 이 사실을 너무 자주 써 왔기 때문에 증명할 필요조차 없을 만큼 당연하게 느껴질 것이다.

이 문제는 겉보기에는 아주 그럴듯하지만 그 "당연한" 사실이 성립하지 않는 작은 수의 세계를 만든다. STEP I 문제이므로 수학 자체는 어렵지 않지만, 여기서 얻는 교훈은 깊다. 바로 이 교훈이 1847년에 시도된 페르마의 마지막 정리(Fermat's Last Theorem)의 유명한 증명을 무너뜨렸고, 대수학의 새로운 분야 하나를 탄생시켰다.

시작하기 전에

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

$S = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$이고 $T = \{3, 7, 11, 15, 19, 23, \ldots\}$이다. S에 속하는 수가 (1이 아닌) S의 더 작은 원소들의 곱으로 나타내어지지 않으면, 그 수를 S-소수라 한다. 보통의 정수에서는 $9 = 3 \times 3$이지만, 3이 S에 속하지 않으므로 9는 S-소수라는 점에 주목하자. 어떤 수가 "소수"인지는 어떤 수들을 쓸 수 있느냐에 달려 있다.

차근차근 풀기

1단계 합집합, 교집합, 곱

모든 홀수는 4로 나눈 나머지가 1 또는 3이므로, $S \cup T$는 모든 양의 홀수의 집합이다. 어떤 수도 서로 다른 두 나머지를 가질 수는 없으므로 $S \cap T$는 공집합이다.

> **생각해 보기** S의 일반적인 원소는 어떻게 나타낼까? 그런 원소 두 개의 곱은 무엇인가?

S의 원소는 $a \geq 0$에 대하여 $4a+1$ 꼴이고,

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1 \in S.$$

따라서 S는 곱셈에 대하여 닫혀 있다(closed under multiplication). T에 대해서는

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1,$$

이므로 이 값은 T가 아니라 S에 속한다. 예를 들어 $3 \times 7 = 21 \in S$이다. 따라서 T는 곱셈에 대하여 닫혀 있지 않다.

2단계 T에 속하는 소인수

> **생각해 보기** T에 속하면서 소수가 아닌 수를 하나 잡자. 그 수의 소인수는 모두 홀수이다. 소인수가 모두 S에 속한다면 어떻게 될까?

이 수는 홀수이므로 그 소인수(prime factor)도 모두 홀수이고, 각각 S 또는 T에 속한다. 소인수가 **모두** S에 속한다면, S는 곱셈에 대하여 닫혀 있으므로 그 곱도 S에 속한다. 그런데 그 곱은 바로 처음의 수이고, 이 수는 T에 속한다. 따라서 적어도 하나의 소인수는 T에 속한다. ■

3단계 홀수 개의 인수

> **생각해 보기** T의 원소를 짝수 개 곱하면 그 곱은 어디에 속할까? 홀수 개라면 어떨까?

T의 수 두 개를 곱하면 S의 수가 되고, S의 수끼리 곱하면 S의 수가 되므로, T의 인수가 짝수 개이면 곱은 S에 속한다. 홀수 개이면 곱은 (S에 속하는 수) $\times$ (T의 원소 하나)가 되고, 같은 종류의 계산에 의해 이는 T에 속한다.

이제 $t \in T$를 잡자. t가 T-소수이면 더 할 일이 없다. 그렇지 않으면 t를 T의 원소들의 곱으로 나타내는데, 각 원소는 1보다 크므로 t보다 작다. 이 중 T-소수가 아닌 것은 다시 더 분해

할 수 있고, 이를 계속 반복한다. 인수는 매번 더 작아지므로 이 과정은 언젠가 끝나고(이번에도 정렬성 원리(well-ordering)이다), 결국 t는 T-소수들의 곱으로 나타내어진다. 그 곱이 T에 속하므로 인수의 개수는 홀수여야 한다. ■

4단계 두 가지 인수분해

> **잠깐, 직접 해 보기** S-소수로의 인수분해가 본질적으로 서로 다른 두 가지인 S의 수를 찾아라. 힌트: 9처럼, 보통의 소인수가 S에 없기 때문에 비로소 S-소수가 되는 수를 이용하라.

S-소수는 $5, 9, 13, 17, 21, 29, 33, 37, 41, 49, \ldots$로 시작한다. 이제 $21 = 3 \times 7$, $9 = 3 \times 3$, $49 = 7 \times 7$은 모두 S-소수인데, 3과 7이 S에 속하지 않기 때문이다. 그리고

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

이처럼 441은 S-소수로의 인수분해(factorisation)를 서로 다른 두 가지로 가진다(그림 1.7.1). S에서는 유일 인수분해(unique factorisation)가 성립하지 않는다. ■

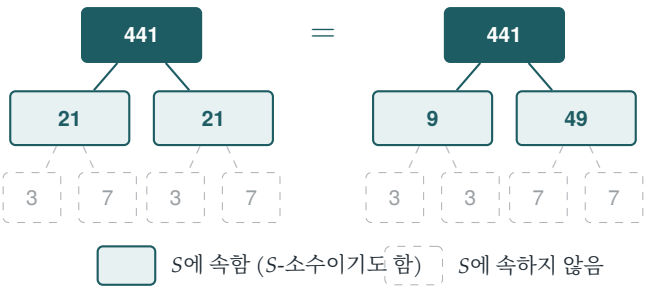


그림 1.7.1 441을 S-소수로 인수분해하는 두 가지 방법. 보통의 정수에서는 두 나무 모두 $3 \times 3 \times 7 \times 7$까지 내려가지만, 3과 7은 S에 속하지 않으므로 S 안에서는 인수분해가 둘째 줄에서 멈추고, 그 결과는 서로 다르다.

돌아보기

- **"소수"인지는 체계에 따라 달라진다.** 9와 21은 정수에서는 합성수(composite)이지만 S에서는 소수이다. 이들을 인수분해하는 데 필요한 수가 없기 때문이다.
- **닫혀 있는지가 중요하다.** S는 곱셈에 대하여 닫혀 있지만 T는 그렇지 않다. 이 하나의 차이가 소문항 (iii)과 (iv)를 이끌었다.
- **당연한 사실도 정리일 수 있다.** 정수에서 유일 인수분해가 성립한다는 것에는 증명이 필요하다. 이 문제가 그 이유를 보여 준다. 매우 비슷해 보이는 체계에서는 그것이 거짓이다.

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

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

(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.

사고 기술

당연하게 여기는 것을 의심하기

어떤 사실이 너무 당연해서 증명할 필요가 없어 보일 때, 그것이 무엇에 의존하는지 묻고, 그것이 성립하지 않는 상황을 찾아보라.

반례(counterexample), 즉 "당연한" 사실이 거짓이 되는 세계를 만들어 보는 것은 증명에 정말로 필요한 것이 무엇인지 알아내는 가장 좋은 방법 중 하나이다. 학부 대수학의 상당 부분은 정수의 익숙한 성질 중 어떤 것이 더 일반적인 체계에서도 살아남는지를 묻는 일이다.

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.

1.8 유리수 세기

문제

STEP III 2020, 8번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 OCR에서 내려받을 수 있는 2020년 STEP 시험지 묶음(zip 파일) 가운데 STEP III 시험지에 있다:

`www.ocr.org.uk/Images/696589-2020-past-papers.zip`

도입

양의 분수(fraction)를 모두 하나씩 차례로 나열하되, 모든 분수가 정확히 한 번씩 나타나게 할 수 있을까? 불가능해 보인다. 어떤 두 분수 사이에도 무수히 많은 분수가 있으므로, 받아 적을 "다음" 분수라는 것이 없기 때문이다. 그런데도 칸토어(Georg Cantor)는 1870년대에 이것이 가능하다는 것을 보였다. 이는 엄밀한 의미에서 분수가 자연수보다 많지 않다는 뜻이다.

칸토어의 목록은 깔끔하지 않았다. $\frac{1}{2}$뿐 아니라 $\frac{2}{4}$도 들어 있어서, 중복된 것은 지워야 했다. 이 문제는 터무니없이 간단한 규칙을 가진 수열로부터 중복이 전혀 없는 목록을 만든다. 이 목록은 2000년에 Neil Calkin과 Herbert Wilf가 발표했지만, 수열 자체는 1858년에 이미 Moritz Stern이 연구한 것이다.

시작하기 전에

생각해 보기 무엇이든 증명하기 전에 처음 열다섯 항 정도를 계산해 보자. 비 u_n/u_{n+1}에 대해 무엇을 알 수 있는가?

수열은 다음과 같이 시작하고

$$1,\ 1,\ 2,\ 1,\ 3,\ 2,\ 3,\ 1,\ 4,\ 3,\ 5,\ 2,\ 5,\ 3,\ 4,\ 1,\ 5,\ \ldots$$

비 u_n/u_{n+1}는 다음과 같다.

$$\frac{1}{1},\ \frac{1}{2},\ \frac{2}{1},\ \frac{1}{3},\ \frac{3}{2},\ \frac{2}{3},\ \frac{3}{1},\ \frac{1}{4},\ \frac{4}{3},\ \frac{3}{5},\ \frac{5}{2},\ \frac{2}{5},\ \frac{5}{3},\ \frac{3}{4},\ \frac{4}{1},\ \ldots$$

모든 분수가 기약분수(lowest terms)로 나타나고, 어느 것도 중복되지 않는다. 문제는 이 현상이 끝없이 계속되며, 모든 양의 분수가 언젠가는 나타난다는 것을 증명하라고 요구한다.

차근차근 풀기

1단계 홀수 번째가 짝수 번째보다 크다

연속한 두 항은 (u_{2k}, u_{2k+1}) 꼴이거나 (u_{2k+1}, u_{2k+2}) 꼴이다.

> **생각해 보기** 이 두 쌍을 각각 u_k와 u_{k+1}로 나타내어 보자. 어느 항이 더 큰가?

$(u_{2k}, u_{2k+1}) = (u_k,\ u_k + u_{k+1})$이고 $(u_{2k+1}, u_{2k+2}) = (u_k + u_{k+1},\ u_{k+1})$이다. 모든 항이 양의 정수이므로(간단한 수학적 귀납법(induction)으로 보일 수 있다), $u_k + u_{k+1}$은 u_k와 u_{k+1}보다 모두 크다. 유일한 예외는 첫 번째 쌍 $(u_1, u_2) = (1, 1)$인데, u_1이 직접 정의되므로 이 쌍은 어느 꼴에도 맞지 않는다. ■

2단계 연속한 두 항은 서로소이다

> **생각해 보기** $d > 1$이 u_{2k}와 u_{2k+1}을 모두 나눈다고, 즉 u_k와 $u_k + u_{k+1}$을 모두 나눈다고 하자. d는 또 무엇을 나누는가?

d는 $(u_k + u_{k+1}) - u_k = u_{k+1}$을 나누므로, d는 수열에서 더 앞에 있는 연속한 쌍 u_k, u_{k+1}을 나눈다. 다른 경우도 똑같다. d가 $u_k + u_{k+1}$과 u_{k+1}을 나누면 u_k도 나눈다.

따라서 연속한 쌍의 공약수는 더 앞의 쌍으로 넘어가고, 다시 그보다 앞의 쌍으로 넘어가는 식으로 계속된다. 위치는 끝없이 줄어들 수 없으므로(이번에도 정렬 원리(well-ordering)이다), 결국 d는 첫 번째 쌍 $u_1 = u_2 = 1$을 나누어야 한다. 이는 $d > 1$일 때 불가능하다. 그러므로 연속한 모든 쌍은 서로소(coprime)이다. ■

3단계 같은 쌍은 두 번 나타나지 않는다

> **잠깐, 직접 해 보기** 1단계에서 유용한 사실을 알 수 있다. 연속한 쌍 (a, b)를 보면, a가 홀수 번째 위치에 있는지 짝수 번째 위치에 있는지 알 수 있다. 어떻게 알 수 있을까? 그렇다면 2단계의 의미에서 그 앞의 쌍을 되찾을 수 있을까?

$a < b$이면 (1단계에 의해) b가 홀수 번째 위치에 있으므로, 어떤 k에 대하여 이 쌍은 $(u_{2k}, u_{2k+1}) = (u_k, u_k + u_{k+1})$이고, "부모" 쌍 (u_k, u_{k+1})은 $(a,\ b - a)$이다. $a > b$이면 이 쌍은 (u_{2k+1}, u_{2k+2})이고 그 부모는 $(a - b,\ b)$이다. $a = b$이면 1단계에 의해 이 쌍은 맨 첫 번째 쌍 $(1, 1)$이어야 한다.

따라서 첫 번째 쌍을 제외한 연속한 각 쌍은 자신의 부모 쌍과 **부모의 위치**를 결정한다(이 구조를 그림 1.8.1에서 트리(tree)로 볼 수 있다). 자식이 $2k$나 $2k+1$번째에 있으면 부모는 k번째에 있다. 이제 (a,b)가 서로 다른 두 위치에 나타났다고 하자. 그러면 그 부모들은 두 위치에 있는 같은 쌍이 되고, **그들의** 부모도 마찬가지이며, 이런 식으로 계속된다. 이를 거슬러 올라가면 결국 1이 아닌 위치에서 $(1,1)$을 찾게 되는데, 이는 1단계에 의해 불가능하다. ■

4단계 서로소인 모든 쌍이 나타난다

> ? **생각해 보기** 서로소인 어떤 쌍 (a,b)가 연속한 두 항으로 결코 나타나지 않는다고 하자. 그러한 쌍 중 어느 것을 살펴보아야 할까?

$a+b$의 값이 가장 작은 "빠진" 서로소 쌍, 즉 최소 반례(minimal counterexample)를 택하자. 이 쌍은 실제로 나타나는 $(1,1)$일 수 없으므로 $a \neq b$이다(서로소이면서 같으면 $a=b=1$이어야 한다).

- $a > b$인 경우: 쌍 $(a-b,b)$는 서로소이고($a-b$와 b의 공약수는 a를 나눈다), 그 합 a는 $a+b$보다 작다. 최소성에 의해 이 쌍은 나타나며, 그 위치를 $k, k+1$이라 하자. 그러면 $u_{2k+1} = u_k + u_{k+1} = a$이고 $u_{2k+2} = u_{k+1} = b$이므로, 결국 (a,b)가 나타난다.
- $a < b$인 경우: 마찬가지로 $(a,b-a)$가 어떤 $k, k+1$에 나타나고, 그러면 $(u_{2k}, u_{2k+1}) = (a,b)$이다.

어느 경우든 모순이다. 따라서 서로소인 양의 정수의 모든 쌍은 연속한 두 항으로 나타난다. ■

(문제에서는 (iv)를 무한강하법(descent)으로 표현한다. 빠진 쌍이 있으면 그보다 작은 빠진 쌍이 생긴다는 것이다. 이는 같은 논증을 반대 방향으로 읽은 것이다.)

5단계 모든 분수의 목록

모든 양의 유리수(rational number)는 a, b가 서로소인 기약분수 a/b로 유일하게 나타낼 수 있다. 4단계에 의해 (a,b)는 연속한 어떤 쌍 (u_n, u_{n+1})으로 나타나므로 $f(n) = a/b$이다. 즉 f의 치역(range)은 모든 양의 유리수이다. 3단계에 의해 이 쌍은 한 번만 나타나고, 2단계에 의해 모든 값 $f(n)$은 이미 기약분수이므로, 서로 다른 두 n이 같은 분수를 줄 수 없다. 그러므로 f는 양의 정수에서 양의 유리수로의 전단사 함수(bijection)이고, 역함수(inverse)를 가진다. ■

돌아보기

- **무한강하법과 그 역.** 공약수와 중복된 쌍은 수열의 처음으로 거슬러 추적했다. 빠진 쌍은 최소 반례를 이용해 앞으로 쌓아 나가며 다루었다.

- **전단사 함수에는 두 부분이 필요하다.** "모든 분수가 나타난다"(전사(onto))와 "어떤 분수도 두 번 나타나지 않는다"(단사(one-to-one))는 별개의 주장이며, 따로 증명했다.
- **먼저 계산하라.** 열다섯 항을 적어 보니 주장을 믿을 수 있게 되었고, 증명을 이끈 부모–자식 구조도 떠올릴 수 있었다.

숨은 수학

Calkin–Wilf 트리

양의 분수를 트리 모양으로 배열하자. 맨 위에 $\frac{1}{1}$을 놓고, 각 분수 $\frac{a}{b}$에 두 자식, 즉 왼쪽에 $\frac{a}{a+b}$, 오른쪽에 $\frac{a+b}{b}$를 준다. 트리를 한 줄씩 왼쪽에서 오른쪽으로 읽으면 정확히 이 문제의 목록 $f(1), f(2), f(3), \ldots$이 된다(그림 1.8.1). 3단계는 모든 분수가 유일한 부모를 가진다는 것이고, 4단계는 모든 분수가 트리 안에 있다는 것이다. 2003년에 Moshe Newman은 트리조차 필요 없다는 것을 발견했다. 목록의 각 분수는 바로 앞의 분수로부터 다음과 같이 계산할 수 있다.

$$x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}.$$

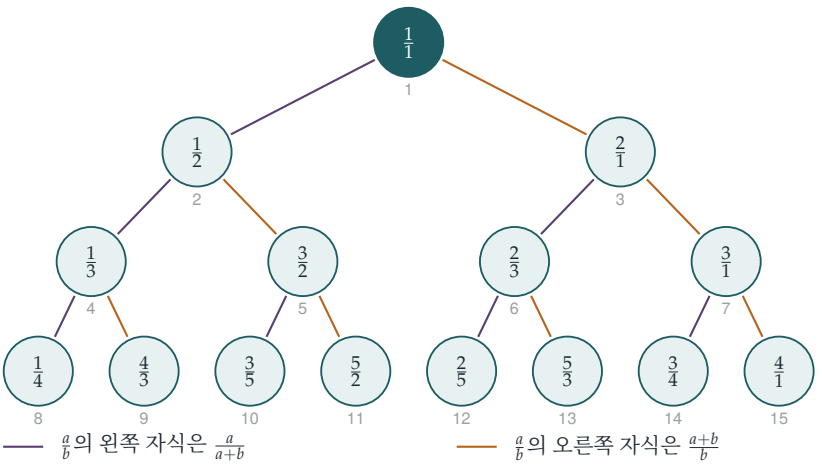


그림 1.8.1 Calkin–Wilf 트리의 처음 네 줄. 한 줄씩 왼쪽에서 오른쪽으로 읽으면 $f(1), f(2), f(3), \ldots$이 된다. 작은 회색 숫자는 위치 n이다. 모든 양의 분수가 기약분수로 정확히 한 번씩 나타난다.

무한의 서로 다른 크기

이처럼 나열할 수 있는 집합을 **가산**(countable) 집합이라 한다. 분수는 가산인데, 분수가 자연수보다 훨씬 많아 보이므로 이는 놀라운 일이다. 대학 첫 학기에는 칸토어의 **대각선 논**

법(diagonal argument)도 배우게 되는데, 이 논법은 **실수**(real number)가 가산이 아님을 보여 준다. 즉 실수의 어떤 목록이든 반드시 빠뜨리는 실수가 있다. 따라서 무한에는 정말로 서로 다른 크기가 있으며, 실수는 유리수보다 진짜로 더 큰 무한을 이룬다. 이것은 대학 1학년 과정에서 만나게 될 가장 놀라운 결과 중 하나이다.

Stern 수열

수열 u_n은 *Stern*의 **이원자 수열**(Stern's diatomic sequence)이며, 다른 곳에서도 여러 모습으로 등장한다. 예를 들어 u_{n+1}은 각 거듭제곱을 많아야 두 번 사용하여 n을 2의 거듭제곱의 합으로 나타내는 방법의 수이다. 이 수열은 *Stern–Brocot* **트리**(Stern–Brocot tree), 그리고 무리수에 대한 최良의 유리수 근삿값을 주는 연분수(continued fraction)와도 밀접하게 관련되어 있다.

사고 기술

전단사 함수 만들기

두 집합의 크기가 같음을 보이려면 두 집합을 정확히 짝지어라. 즉 목표 집합의 모든 원소가 대응됨(전사)과 어떤 원소도 두 번 대응되지 않음(단사)을 증명하라.

전단사 함수는 유한이든 무한이든 셈의 기초이며, 대학에서 끊임없이 사용하게 된다. 여기서는 두 부분 모두 구조를 출발점까지 거슬러 추적하여 증명했다.

더 도전하기

1 **분수 찾기.** 어떤 n에 대하여 $f(n) = \frac{3}{5}$인가? 또 $f(n) = \frac{5}{3}$인 n은? 부모 규칙을 이용해 $\frac{1}{1}$까지 거슬러 올라가 보라.

2 **Newman의 공식.** $x_1 = 1$에서 시작하여 Newman의 공식이 목록의 처음 열 개의 분수를 만들어 냄을 확인하라.

3 **칸토어의 대각선 논법.** 0과 1 사이의 모든 실수를 소수로 적은 목록이 있다고 하자. 목록의 n번째 수와 n번째 자리가 다른 소수를 만들어라. 이것이 왜 목록이 불완전함을 보여 주는가? ($0.0999\ldots = 0.1$과 같은 소수에는 어떤 주의가 필요한가?)

4 **가산 합집합.** 심화 양의 정수의 모든 쌍 (m, n)의 집합이 가산임을, 양의 정수와의 전단사 함수를 명시적으로 제시하여 보여라. ($2^{m-1}(2n-1)$을 시도해 보라.)

더 읽을거리

- **Neil Calkin & Herbert Wilf, "Recounting the rationals"** (*American Mathematical Monthly*, 2000). 유리수 다시 세기. 네 쪽 분량이며, 전부 읽을 만하다.
- **Aigner & Ziegler, *Proofs from THE BOOK***, 제 17장 "Sets, functions, and the continuum hypothesis"(집합, 함수, 연속체 가설). Calkin–Wilf 트리를 다룬다.
- **Ian Stewart & David Tall, *The Foundations of Mathematics*** (Oxford University Press). 대학 1학년 과정에서처럼 가산성, 칸토어, 실수를 다룬다.

1.9 삼차곡선의 접선

문제

STEP I 2009, 2번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/09-s1-q2`

도입

얼핏 보면 평범한 좌표기하 문제이다. 미분하고, 접선(tangent)을 구하고, 삼차방정식을 푼다. 그런데 마지막 줄에서 세 세제곱수의 합이 되는 세제곱수를 찾으라고 하고, 기하가 마치 마법처럼 그런 수를 만들어 낸다.

곡선 위의 이미 아는 점을 지나는 직선을 그어 새로운 점을 찾는 이 기법은 3세기 알렉산드리아의 디오판토스(Diophantus)까지 거슬러 올라간다. 현대에 와서 이 기법은 **타원곡선**(*elliptic curves*) 이론으로 발전했다. 타원곡선은 오늘날 정수론의 한가운데에 있고, 페르마의 마지막 정리(Fermat's Last Theorem)의 증명을 떠받치며, 전 세계 인터넷 통신의 상당 부분을 안전하게 지킨다.

시작하기 전에

? **생각해 보기** 점 $(-a, b)$는 곡선 위에 있다. 왜 그런가? 그리고 이것이 세제곱수의 합과 무슨 관계가 있는가?

대입하면 $(-a)^3 + a^3 + b^3 = b^3$이므로 그렇다. $y^3 = x^3 + a^3 + b^3$ 위에서 좌표가 **유리수**(*rational*)인 점이 바로 우리가 원하는 것이다. $x = q/s', y = p/s'$이면 분모를 없앴을 때 세제곱수들 사이의 관계식이 나오기 때문이다. 계획은 쉬운 점 하나에서 출발하여 기하를 이용해 덜 뻔한 점을 찾는 것이다.

차근차근 풀기

1단계 접선

$y^3 = x^3 + a^3 + b^3$을 음함수 미분(implicit differentiation)하면 $3y^2\dfrac{dy}{dx} = 3x^2$이므로 $\dfrac{dy}{dx} = \dfrac{x^2}{y^2}$이다. $(-a, b)$에서 기울기는 a^2/b^2이므로 접선은

$$y - b = \frac{a^2}{b^2}(x + a) \quad\Longrightarrow\quad b^2y - b^3 = a^2x + a^3 \quad\Longrightarrow\quad b^2y - a^2x = a^3 + b^3. \qquad \blacksquare$$

2단계 접선이 곡선과 다시 만나는 곳

$a = 1$, $b = 2$일 때 곡선은 $y^3 = x^3 + 9$이고, $(-1, 2)$에서의 접선은 $4y - x = 9$, 즉 $y = \dfrac{x+9}{4}$이다. 이를 곡선의 식에 대입하면

$$\frac{(x+9)^3}{64} = x^3 + 9 \quad\Longrightarrow\quad x^3 + 27x^2 + 243x + 729 = 64x^3 + 576,$$

이고, 정리하면 $63x^3 - 27x^2 - 243x - 153 = 0$이다. 양변을 9로 나누면 $7x^3 - 3x^2 - 27x - 17 = 0$을 얻는다. $\blacksquare$

3단계 삼차방정식 풀기

> **생각해 보기** 이 삼차방정식의 근 하나는 계산하지 않아도 이미 알고 있다. 그 근은 무엇이며, 왜 두 번 나타나야 하는가?

접선은 $x = -1$에서 곡선에 접하고(그림 1.9.1), "접한다"는 것은 중근(repeated root)을 뜻한다. 포물선의 접선이 포물선과 이차방정식의 중근에서 만나는 것과 같다. 따라서 $(x+1)^2$이 인수여야 한다. 확인해 보면 $7(-1)^3 - 3(1) - 27(-1) - 17 = -7 - 3 + 27 - 17 = 0$이고, 도함수 $21x^2 - 6x - 27$도 $x = -1$에서 0이 된다. 나누어 보면

$$7x^3 - 3x^2 - 27x - 17 = (x+1)^2(7x - 17).$$

> **잠깐, 직접 해 보기** 따라서 접선은 $x = \frac{17}{7}$에서 곡선과 다시 만난다. y를 구하고, 이 점을 세제곱수들 사이의 관계식으로 바꾸어 보아라.

$y = \dfrac{17/7 + 9}{4} = \dfrac{80/7}{4} = \dfrac{20}{7}$이다. 점 $\left(\frac{17}{7}, \frac{20}{7}\right)$은 $y^3 = x^3 + 9$ 위에 있으므로

$$\frac{20^3}{7^3} = \frac{17^3}{7^3} + 9 \quad\Longrightarrow\quad 20^3 = 17^3 + 9 \times 7^3.$$

생각해 보기 9×7^3을 두 세제곱수의 합으로 나타내고 싶다. 9가 어디에서 왔는지 떠올려 보아라.

$9 = a^3 + b^3 = 1^3 + 2^3$이므로 $9 \times 7^3 = 7^3 + 14^3$이다. 따라서

$$20^3 = 17^3 + 14^3 + 7^3.$$

검산: $8000 = 4913 + 2744 + 343$. ■

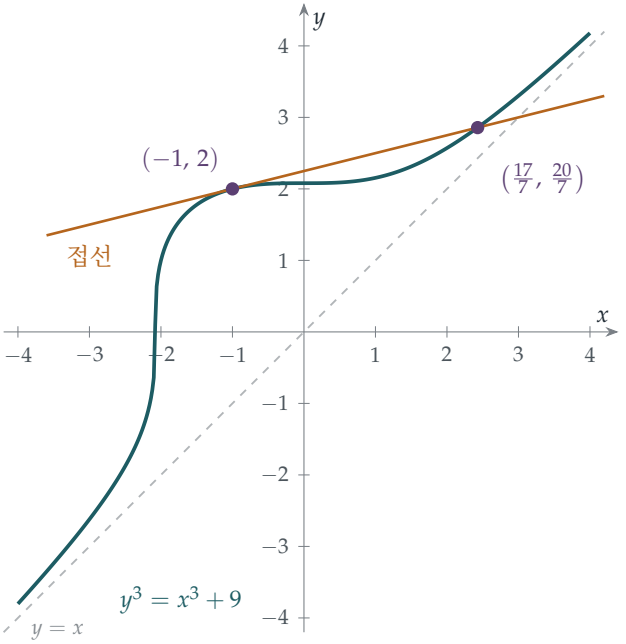


그림 1.9.1 곡선 $y^3 = x^3 + 9$(청록색)는 원점에서 멀어질수록 직선 $y = x$에 가까워진다. 유리점 $(-1, 2)$에서의 접선(호박색)은 그 점에서 곡선에 접하는데, 이는 두 번 만나는 것으로 센다. 그리고 접선은 또 다른 유리점 $\left(\frac{17}{7}, \frac{20}{7}\right)$에서 곡선과 한 번 더 만난다.

돌아보기

- **접한다는 것은 중근을 뜻한다.** 덕분에 뻔한 근이 없어 보이던 삼차방정식을 곧바로 인수분해할 수 있었다.
- **새 근은 저절로 유리수가 된다.** 세 근 중 두 근이 유리수이면(여기서는 둘 다 -1), 근의 합 $\frac{3}{7}$이 유리수이므로 나머지 한 근도 유리수여야 한다. 이것이 이 방법의 핵심이다.
- **기하가 산술을 만들어 냈다.** 우리는 세제곱수를 찾아 헤맨 적이 없다. 접선 하나가 그것을 찾아 주었다.

숨은 수학

할선–접선 방법

$y^3 = x^3 + 9$나 더 표준적인 꼴인 $y^2 = x^3 + Ax + B$ 같은 삼차곡선을 생각하자. 그 위에서 좌표가 유리수인 두 점을 알면, 두 점을 지나는 직선은 곡선과 정확히 한 점에서 더 만나고, 그 점의 좌표도 유리수이다(**돌아보기**의 논증에 의해). 한 점만 알 때에는 그 점에서의 접선을 대신 쓴다. 어느 쪽이든 기존의 유리점에서 새로운 유리점이 만들어진다.

놀랍게도 이 "할선–접선(chord–tangent)" 작도는 곡선 위의 점들을 **더하는** 방법으로 바꿀 수 있고, 그러면 유리점들은 **군**(*group*)을 이룬다. 군은 대학 1학년 때 배우게 될 대수적 구조이다. 1922년 Louis Mordell은 이 군이 유한개의 점으로 생성된다는 것을 증명했다. 즉 유리점이 아무리 많더라도 모두 유한집합에서 출발하여 할선과 접선으로 만들어 낼 수 있다. 그의 증명은 Section 1.5에서 다룬 페르마의 강하법(descent)의 한 형태이다.

오늘날의 타원곡선

이런 곡선을 **타원곡선**이라고 부른다(타원이어서가 아니라, 타원의 호의 길이와 역사적으로 연관되어 있기 때문이다). 타원곡선은 현대 수학 곳곳에 등장한다.

- **페르마의 마지막 정리.** 1980년대에 Gerhard Frey는 $x^n + y^n = z^n$의 해가 있다면 매우 이상한 타원곡선이 만들어진다는 것을 알아차렸다. 1994년 앤드루 와일스(Andrew Wiles)는 그런 이상한 곡선이 존재할 수 없음을 증명했고, 그리하여 페르마의 마지막 정리를 증명했다.
- **버치–스위너턴다이어 추측.** 유리점들의 군에는 생성원(generator)이 몇 개 필요할까? 1960년대에 케임브리지에서 수학 역사상 가장 이른 컴퓨터 실험 중 일부를 이용하여 세워진 추측(conjecture)은, 소수(prime)를 법으로 하여 점의 개수를 세어 만든 함수를 통해 그 답을 예측한다. 이 버치–스위너턴다이어 추측(Birch and Swinnerton-Dyer conjecture)은 7대 밀레니엄 문제(Millennium Prize Problems) 가운데 하나이다.
- **암호학.** 유한한 수 체계 위의 타원곡선에서는 점 P를 자기 자신에 n번 더하는 계산이 빠르다. n이 수백 자리 수라도 그렇다(거듭제곱을 반복 제곱으로 계산하듯 P를 거듭 두 배 하면 된다). 그러나 P와 결과 nP가 주어졌을 때 n을 찾는 것은 극도로 어려운 것으로 보인다. 이것이 **타원곡선 이산 로그 문제**(*elliptic-curve discrete logarithm problem*)이다. 이 비대칭성이 오늘날 온라인 통신의 상당 부분을 보호한다.

같은 차수의 거듭제곱의 합

세 양의 세제곱수의 합이 되는 가장 작은 세제곱수는 $6^3 = 3^3 + 4^3 + 5^3$이다. 접선 방법으로 찾은 $20^3 = 7^3 + 14^3 + 17^3$은 이것의 배수가 아니며, 이 방법을 되풀이하면 새로운 항등식이 계속 나온다(다만 음수가 섞인 것도 있다). 어떤 k제곱수를 만들려면 k제곱수가 몇 개 필요할까? 오일러(Euler)는 1769년에 다른 k제곱수를 만들려면 적어도 k개의 k제곱수가 필요하다고 추측했다. 네제곱과 다섯제곱에 대해서는 이 추측이 틀렸다. 1966년 Leon Lander와 Thomas Parkin은 컴퓨터 탐색으로

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

를 찾았고, 1988년 Noam Elkies는 타원곡선을 이용해 네제곱에 대한 반례를 찾았다.

사고 기술

> **산술을 푸는 기하**
>
> 방정식의 정수해나 유리수해를 찾으려면, 방정식을 곡선으로 보고 이미 아는 점을 지나는 직선을 찾아보아라.
>
> 그 뒤에 있는 대수는 간단하다. 유리수 계수 다항식의 근이 하나를 빼고 모두 유리수이면, 마지막 근도 유리수이다. 이처럼 그림과 방정식 사이를 오가는 것은 수학자가 지닐 수 있는 가장 강력한 습관 가운데 하나이다.

더 도전하기

1. **원 위의 유리점.** $(-1, 0)$을 지나고 기울기가 t인 직선은 원 $x^2 + y^2 = 1$과 다시 만난다. 다른 교점이 $\left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$임을 보이고, 이를 이용하여 피타고라스 세 쌍(Pythagorean triples)을 무수히 많이 만들어라.

2. **빗나가는 할선.** 점 $(1, 2)$와 $(2, 1)$은 $x^3 + y^3 = 9$ 위에 있다. 두 점을 지나는 직선이 곡선과 다른 점에서 만나지 않음을 보여라. "세 번째 점"은 어디로 갔을까? (**무한원점**(*point at infinity*)을 찾아보아라.)

3. **기법을 되풀이하기.** $\left(\frac{17}{7}, \frac{20}{7}\right)$에서 $y^3 = x^3 + 9$의 접선을 구하고, 그 접선이 곡선과 만나는 세 번째 점을 구하여라. (컴퓨터 대수 시스템이 도움이 된다. 수가 얼마나 빨리 커지는지 살펴보아라.)

4 **택시 수.** $1729 = 1^3 + 12^3 = 9^3 + 10^3$이다. $(1, 12)$와 $(9, 10)$을 지나는 직선이 곡선 $x^3 + y^3 = 1729$와 만나는 세 번째 점을 구하고, 이로부터 $p^3 = q^3 + r^3 + s^3$ 꼴의 새로운 항등식을 이끌어 내어라.

더 읽을거리

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves*** (Springer). 『타원곡선 위의 유리점』. 학부생을 위해 쓰인 책으로, 1장은 A 레벨(A level, 영국의 대학 입시 과목 시험) 이상의 지식이 필요하지 않다.
- **Avner Ash & Robert Gross, *Elliptic Tales*** (Princeton University Press). 『타원 이야기』. 버치–스위너턴다이어 추측까지 이어지는 대중서이다.
- **Simon Singh, *Fermat's Last Theorem***. 『페르마의 마지막 정리』. 타원곡선이 어떻게 350년 묵은 문제를 풀게 되었는지 들려준다.

우리가 배운 것

이 장을 시작하면서 우리는 자연수에 관한 세 가지 질문을 던졌고, 그 밑에 흐르는 네 번째 주제, 곧 무언가를 어떻게 증명(proof)하는가를 다루겠다고 약속했다. 이제 아홉 개의 STEP 문제가 우리를 얼마나 멀리 데려왔는지 살펴볼 때이다.

1. 소수는 얼마나 많고, 어떻게 분포하는가?

Section 1.1에서 우리는 새로운 소수(prime)를 하나도 찾지 않고 소수가 무한히 많다는 것을 증명하였다. 서로 공약수를 갖지 않는 수들의 무한한 모임인 페르마 수(Fermat numbers)를 만들었으므로, 각각의 수에는 자기만의 소수가 하나씩 필요하다. 이것은 크기가 아니라 **구조**에 관한 증명이다.

Section 1.2에서는 한 걸음 더 나아가 n 이하의 모든 소수의 곱이 4^n보다 작다는 것을 보였다. 이것은 우리의 첫 번째 **정량적** 명제였다. 즉 소수가 얼마나 빽빽하게 들어찰 수 있는지에 한계를 준다. 로그(logarithm)를 취하면 이 명제는 $\sum_{p \le n} \ln p < 1.39\, n$이 되는데, 소수 정리(Prime Number Theorem)에 따르면 실제 값은 약 n이다. 우리의 STEP 수준 논증이 이미 올바른 범위에 들어와 있었던 것이다.

우리가 **하지 않은** 것은 소수가 정확히 어떻게 분포하는지를 밝히는 일이다. 이는 리만(Riemann) 제타 함수(zeta function)가 좌우하며, 이를 정밀하게 만드는 것이 수학에서 가장 유명한 미해결 문제인 리만 가설(Riemann Hypothesis)이다. 여러분은 이제 그것이 무엇에 관한 문제인지 이해할 만큼은 알고 있다.

2. 어떤 수가 분수가 아님을 어떻게 증명할 수 있는가?

우리는 꽤 서로 다른 세 가지 방법을 찾았다.

- **가장 작은 것을 택하라** (Section 1.3). $\sqrt{2}$가 분수(fraction)라면 $k\sqrt{2}$를 정수로 만드는 가장 작은 양의 정수 k가 존재할 것이다. 그런데 그러면 $(\sqrt{2}-1)k$가 더 작은 그런 수가 된다. 같은 논증으로 세제곱근도 다루었다.
- **0과 1 사이에 정수를 가두어라** (Section 1.4). e나 e^2이 분수라면, 계승(factorial)을 곱했을 때 0과 1 사이에 엄격하게 놓인 정수가 생겨난다. 이것이 e와 π가 초월수(transcendental)임을 보인 에르미트(Hermite)와 린데만(Lindemann)의 증명 밑에 깔린 아이디어이다.

- **불가능한 나누어떨어짐을 찾아라** (Section 1.5, 연습문제 3). $x^2 + y^2 = 3$ 위에 유리점(rational point)이 없음을 보이는 것은, x가 유리수일 때 $\sqrt{3 - x^2}$이 결코 유리수가 아님을 보이는 것과 같다.

그리고 우리는 아직 모르는 것이 얼마나 많은지도 배웠다. 아직 아무도 $e + \pi$가 무리수(irrational)임을 증명하지 못했다.

3. 어떤 방정식이 정수해를 갖는가?

때로는 답이 **하나도 없다**이며, Section 1.5에서는 이를 증명하는 페르마의 방법을 보였다. 어떤 해든 그보다 작은 해를 만들어 내고, 이것이 끝없이 이어진다는 것이다. 잘 고른 소수를 법(modulo)으로 하여 계산하면 어떤 나누어떨어짐을 이용해야 하는지 알 수 있었다.

때로는 답이 **있다, 그리고 여기 해를 만들어 내는 기계가 있다**이다. Section 1.6에서는 복소수(complex numbers)가 두 제곱수의 합을 곱셈 규칙으로 바꾸어 주었다. Section 1.9에서는 3차 곡선(cubic curve)의 접선(tangent line)이 $20^3 = 17^3 + 14^3 + 7^3$을 만들어 냈다.

그리고 때로는 **수 체계를 바꾸는 것**이 올바른 수이다. 가우스(Gauss) 정수(Gaussian integers)는 두 제곱수의 합을 쉽게 만들어 주었다. 그러나 Section 1.7는 경고를 주었다. 완벽하게 그럴듯해 보이는 체계에서도 수가 서로 다른 두 가지 방식으로 "소수"의 곱으로 인수분해될 수 있다는 것이다. 1847년에 무시되었던 이 경고는 아이디얼(ideal)의 발명과 현대 대수학으로 이어졌다.

Section 1.8는 나름의 반전을 더했다. 자연수보다 훨씬 많아 보이는 분수들도 하나씩 나열할 수 있다는 것이다. 무한은 처음 보이는 것보다 더 많은 구조를 지니고 있다.

4. 증명의 도구 상자

다음은 이 장에서 여러분이 사용한 방법들이다. 이들 모두가 대학 수학 과정에서 거듭거듭 다시 등장할 것이다.

방법	사용한 곳
수학적 귀납법(induction)과 강한 귀납법(strong induction)	페르마 수(1.1); 소수의 곱(1.2)
정렬 원리(well-ordering), 최소 반례(minimal counterexample)	$\sqrt{2}$와 $\sqrt[3]{2}$(1.3); 분수 나열하기(1.8)
무한 강하법(infinite descent)	불가능한 방정식(1.5); 서로소(coprime)인 쌍(1.8)
귀류법(proof by contradiction)	전반에 걸쳐, 특히 1.3과 1.4
n을 법으로 하는 계산	1.5; 1.7
상계 잡기와 조이기(bounding and squeezing)	1.2; 1.4
전단사(bijection) 만들기	1.8
반례(counterexample) 구성하기	유일하지 않은 인수분해(1.7)
배경 바꾸기	복소수(1.6); 기하(1.9)

문제들을 돌아보면, STEP 출제자들이 종종 첫 단계를 알려 주었다는 것을 알아차릴 것이다. "이항전개(binomial expansion)를 고려하여...", "복소수 $2+\mathrm{i}$와 $10+11\mathrm{i}$를 고려하여..." 같은 식이다. 대학에서는 그런 도움이 점차 사라지고, 올바른 첫 단계를 **찾아내는** 것이 바로 기술이 된다. 가장 좋은 준비는 여러분이 지금까지 해 온 바로 그것이다. 문제를 다 풀고 나면 그 힌트가 **왜** 통했는지 물어보라. 그래야 다음번에는 스스로 그것을 떠올릴 수 있다.

다음은 어디로

이 장의 여러 실마리가 이 책의 다른 곳에서 이어진다.

- 분수에 의한 e의 근사는 Section 2.9에서, 리만 제타 함수는 Section 2.4에서 다시 등장하며, 그곳에서 $\zeta(2) = \pi^2/6$을 다룬다.
- 라메(Lamé)의 실패한 증명에 등장했던 단위근(roots of unity)은 Chapter 5의 주제이며, Section 1.1에서 약속한 가우스의 정17각형 작도는 Section 6.2에서 다룬다.
- Section 1.6에 나온 항등식의 네 제곱수 버전은 사원수(quaternions)를 통해 Section 7.8에 등장한다.

대학에 가기 전에 더 나아가고 싶다면

- **Harold Davenport, *The Higher Arithmetic***(고등 산술): 초등 정수론(number theory)에 대한 단 한 권의 입문서로 가장 좋은 책이다.
- **Aigner & Ziegler, *Proofs from THE BOOK***(하늘책의 증명): 1–4장, 8장, 17장이 이 장과 직접 연결된다.

- **Joseph Silverman, *A Friendly Introduction to Number Theory***(친절한 정수론 입문): 여기 나온 거의 모든 내용과 그 이상을 느긋한 속도로 다룬다.
- **Marcus du Sautoy, *The Music of the Primes***(소수의 음악)와 **Simon Singh, *Fermat's Last Theorem***(페르마의 마지막 정리): 수학 뒤에 숨은 사람들의 이야기이다.

정수론은 사람들을 끌어들이는 버릇이 있다. 그 질문들은 첫날에 던질 수 있을 만큼 단순하면서도, 평생을 바칠 만큼 깊다. 이 절들 가운데 몇몇이 여러분에게 그다음에 무슨 일이 일어나는지 알고 싶게 만들었다면, 그것이 바로 이 책이 노린 바이다.

더 도전하기 해답

여기에 실린 것은 완전한 풀이가 아니라 간단한 답과 힌트이다. 결과와 핵심 단계를 제시하므로 자신의 풀이를 확인하는 데 쓸 수 있다. 답을 보기 전에 각 연습문제를 제대로 풀어 보라.

1.1 소수 공장

1. $p_1, \ldots, p_k$가 소수(prime) 전부라고 가정하자. 그러면 $p_1 \cdots p_k + 1$은 이 목록에 없는 소인수(prime factor)를 가지므로 모순(contradiction)이다. 페르마 수(Fermat number)를 이용한 증명은 구성적(constructive)이다. 이 증명은 쌍마다 서로소(pairwise coprime)인 수 $F_0, F_1, \ldots$을 무한히 많이 제시하고, 이들 각각이 새로운 소수를 하나씩 제공한다.

2. $n \geq 2$이면 2^n은 4의 배수이므로 $2^{2^n} = 16^{2^{n-2}}$이고, 16의 거듭제곱은 모두 일의 자리가 6이다. 따라서 F_n의 일의 자리는 7이다.

3. (a) 수학적 귀납법(induction): $a_{n+1} - 1 = a_n(a_n - 1) = a_n \cdot a_1 \cdots a_{n-1}$. (b) a_m과 a_n $(m < n)$의 공약수는 $a_1 \cdots a_{n-1} = a_n - 1$과 a_n을 모두 나누므로 1이다. 따라서 각 항은 다른 어떤 항과도 공유하지 않는 소인수를 가진다. (c) $\frac{1}{a_n} = \frac{1}{a_n - 1} - \frac{1}{a_{n+1} - 1}$이고, 이 합은 망원급수(telescoping series)처럼 소거되어 $1 - \frac{1}{a_{n+1} - 1}$이 된다.

4. (a) $p \mid F_n$이면 $2^{2^n} \equiv -1$이고, 양변을 제곱하면 $2^{2^{n+1}} \equiv 1$이다. (b) d는 $2^e \equiv 1$을 만족하는 모든 e를 나누므로 $d \mid 2^{n+1}$이다. 한편 $2^{2^n} \equiv -1 \not\equiv 1$이므로($p$가 홀수이므로) $d \nmid 2^n$이다. 따라서 $d = 2^{n+1}$이다. (c) $2^{p-1} \equiv 1$이므로 $2^{n+1} \mid p - 1$이다. (d) $641 = 64 \times 10 + 1$이다. 641보다 작은 $64k + 1$ 꼴의 소수는 193, 257, 449, 577이다. 시험해 볼 후보가 네 개뿐이며, 오일러(Euler)는 이렇게 하여 641을 찾았다.

5. n번째 소수는 $F_0, \ldots, F_{n-1}$의 소인수 중 가장 큰 것 이하이므로 $p_n \leq F_{n-1} = 2^{2^{n-1}} + 1$이다. $n = 5$일 때 이 상계는 65 537인데 $p_5 = 11$이다. 옳은 부등식이지만 극도로 약하다.

1.2 소수는 얼마나 드문드문 흩어져 있는가?

1. $P_{1,10} = 210$, $P_{1,20} = 9\,699\,690$, $P_{1,30} = 6\,469\,693\,230$이다. $4^{30} \approx 1.15 \times 10^{18}$, $e^{30} \approx 1.07 \times 10^{13}$과 비교해 보자. 이 곱은 4^n보다 훨씬 작고 대략 e^n처럼 증가한다(실제로

$\ln P_{1,n} \sim n$이며, 이는 소수 정리(Prime Number Theorem)의 한 형태이다).

2. $\binom{2m}{k+1}/\binom{2m}{k} = \frac{2m-k}{k+1}$이고, 이 값은 정확히 $k < m$일 때 1보다 크다. 따라서 이항계수(binomial coefficient)는 가운데까지 증가했다가 그 뒤로 감소한다. 합이 4^m인 $2m+1$개의 항 중 가장 큰 것은 이들의 평균 이상이다.

3. $(\sqrt{n}, n]$에 있는 소수는 각각 $\sqrt{n}$보다 크고 그 곱은 4^n보다 작으므로 $(\sqrt{n})^{\pi(n)-\pi(\sqrt{n})} < 4^n$이다. 양변에 로그를 취하라. $2\ln 4 \approx 2.77$이고 $\pi(\sqrt{n}) \le \sqrt{n}$이므로 원하는 부등식이 따라 나온다. 이 상계는 올바른 꼴 $n/\ln n$을 가지며, 다만 상수가 참값 1 대신 2.8이다.

4. 각각 바로 앞 소수의 두 배보다 작은 소수 $2, 3, 5, 7, 13, 23, 43, 83$을 사용한다. $n \le 50$인 임의의 n에 대해, 이 목록에서 n보다 큰 첫 소수는 바로 앞 소수의 두 배보다 작고, 그 앞 소수는 n 이하이므로, 이 소수는 n과 $2n$ 사이에 있다.

1.3 가장 작은 반례

1. $k\sqrt{3}$이 정수가 되는 가장 작은 양의 정수 k가 있다면, $k' = (\sqrt{3}-1)k$는 더 작은 양의 정수이고 $k'\sqrt{3} = 3k - k\sqrt{3}$도 정수이다. 여기서는 $\sqrt{3}-1$이 $\sqrt{2}-1$의 역할을 한다.

2. $0 < \sqrt{N} - m < 1$이면 $k' = (\sqrt{N}-m)k$는 k보다 작은 양의 정수이고, $k'\sqrt{N} = kN - mk\sqrt{N}$은 정수이므로 모순이다.

3. $N = 4$이면 $m = 2 = \sqrt{4}$이므로 $\sqrt{N} - m = 0$이고, $k' = 0$은 양의 정수가 아니다. "$0 < \sqrt{N} - m$"이라는 단계가 성립하지 않는다.

4. 그림에서, 한 변이 a인 정사각형 안에 겹쳐 놓인 한 변이 b인 두 정사각형은 한 변이 $2b - a$인 가운데 정사각형을 두 번 덮고, 한 변이 $a - b$인 두 정사각형을 덮지 않은 채로 남긴다. 식으로 쓰면 $(2b-a)^2 - 2(a-b)^2 = 2b^2 - a^2 = 0$이다.

1.4 e는 무리수이고, e^2도 그렇다

1. $\frac{1}{e} = \frac{p}{q}$라면 $\frac{1}{e} = \sum_{k\ge 0} \frac{(-1)^k}{k!}$의 양변에 $q!$을 곱한다. $k \le q$인 항은 정수이고, 꼬리 $\sum_{k>q}(-1)^k q!/k!$는 항의 크기가 감소하는 교대급수(alternating series)이므로 그 절댓값은 0과 $\frac{1}{q+1}$ 사이에 엄격하게 놓인다. 따라서 $q!/e$는 정수가 아니므로 모순이다.

2. $\sin 1 = \frac{p}{q}$라면 $2n+1 \ge q$인 $(2n+1)!$을 곱한다. 좌변은 정수이고, 급수의 항 중 $\frac{1}{(2n+1)!}$까지도 정수가 된다. 꼬리는 첫 항의 크기가 $\frac{1}{(2n+2)(2n+3)} < 1$인 교대급수이므로 정수가 아니다.

3. 이 방법에는 $\frac{1}{k!}$처럼 꼬리가 분모가 커지는 속도보다 빨리 줄어드는, 유리수(rational) 항으로 이루어진 급수가 필요한데, π에 대해서는 그런 급수가 알려져 있지 않다. 니븐(Niven)의 증명은 $\int_0^{\pi} \frac{x^n(\pi-x)^n}{n!}\sin x\,\mathrm{d}x$를 이용한다. π가 유리수라면 큰 n에 대해

이 값은 1보다 작은 양의 정수가 되어야 한다.

4. $x^2 - (e+\pi)x + e\pi$의 근은 e와 π이다. $e+\pi$와 $e\pi$가 모두 대수적(algebraic)이라면 π는 대수적 계수를 갖는 다항식의 근이 되므로 대수적 수가 되어, 린데만 정리(Lindemann's theorem)에 모순이다.

1.5 무한 강하법

1. $3 \mid a$이다. $a = 3a_1$로 쓰면 $9a_1^3 + b^3 = 3c^3$이므로 $3 \mid b$이고, 그러면 $3a_1^3 + 9b_1^3 = c^3$이므로 $3 \mid c$이다. 따라서 (a_1, b_1, c_1)은 더 작은 해이며, 이것이 무한 강하법(descent)이다. $p^4 + 2q^4 = 5r^4$의 경우: 네제곱수는 5를 법으로(modulo) 0 또는 1이다(일의 자리가 0, 1, 5, 6 중 하나이다). 따라서 $p^4 + 2q^4 \equiv 0$이면 $5 \mid p$이고 $5 \mid q$이어야 한다. 그러면 $5^4 \mid 5r^4$이므로 $5 \mid r$이고, 다시 무한 강하법을 적용한다.

2. 제곱수는 4를 법으로 0 또는 1이므로 $x^2 + y^2$은 0, 1, 2 중 하나이고 결코 3이 아니다.

3. 유리점(rational point) $(\frac{a}{c}, \frac{b}{c})$가 있다면 $c \neq 0$인 $a^2 + b^2 = 3c^2$이 성립하게 되는데, 이는 소문항 (iii)에서 배제된다.

4. x, y를 고정하면 이 방정식은 이차방정식 $z^2 - 3xyz + (x^2 + y^2) = 0$이고, 두 근의 합은 $3xy$이다. $(1,1,1)$에서 시작하면 $(1,1,2)$를 얻는다. $(1,2)$의 맞은편에 있는 1을 바꾸면 $3 \cdot 1 \cdot 2 - 1 = 5$이므로 $(1,2,5)$를 얻고, 이어서 $(1,5,13)$과 $(2,5,29)$를 얻는다.

1.6 두 제곱수의 합

1. 제곱수는 4를 법으로 0 또는 1이므로, 두 제곱수의 합은 4를 법으로 결코 3이 아니다.

2. $65 = 1^2 + 8^2 = 4^2 + 7^2$이고 $85 = 2^2 + 9^2 = 6^2 + 7^2$이다. $65 = (2+\mathrm{i})(2-\mathrm{i})(3+2\mathrm{i})(3-2\mathrm{i})$로 쓰면 $(2+\mathrm{i})(3+2\mathrm{i}) = 4+7\mathrm{i}$이고 $(2+\mathrm{i})(3-2\mathrm{i}) = 8-\mathrm{i}$이다. 마찬가지로 85에 대해서는 $(2+\mathrm{i})(4\pm\mathrm{i})$에서 $7+6\mathrm{i}$와 $9-2\mathrm{i}$를 얻는다.

3. $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$이다. 5, 13, 17은 각각 가우스 정수(Gaussian integer)와 그 켤레(conjugate)의 곱으로 분해된다. 각 쌍에서 인수를 하나씩 고르면 8개의 곱이 생기는데, 이들은 서로 켤레인 것끼리 짝지어지므로(같은 두 제곱수의 합을 준다) 4개가 남는다.

4. 절댓값(modulus)의 제곱을 취하면 $9 = (a^2+b^2)(c^2+d^2)$이다. 3은 두 제곱수의 합이 아니므로 두 인수 중 하나는 1이다.

1.7 인수분해가 무너질 때

1. $693 = 9 \times 77 = 21 \times 33$이며, 네 인수 모두 S-소수이다. 만드는 법: $4k+3$ 꼴의 소수 네 개 p, q, r, s를 잡으면 $(pq)(rs) = (pr)(qs)$에서 S-소수로의 두 가지 인수분

해(factorisation)를 얻는다.

2. E-소수는 $2 \pmod 4$인 수들이다(두 짝수의 곱으로 나타낼 수 없기 때문이다). $60 = 2 \times 30 = 6 \times 10$이다.

3. $(ac - 5bd)^2 + 5(ad + bc)^2$을 전개하면 $N(zw) = N(z)N(w)$이다. $a^2 + 5b^2$은 결코 2나 3이 아니다. $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 6$이므로, 단원(unit)이 아닌 수들로 인수분해하려면 노름(norm)이 2 또는 3인 인수가 필요하다.

4. 서로 다른 두 가지 인수분해 $p_1 \cdots p_r = q_1 \cdots q_s$를 갖는 가장 작은 수를 n이라 하자. 유클리드 보조정리(Euclid's lemma)에 의해 p_1은 어떤 q_j를 나누므로 $p_1 = q_j$이다. 이를 약분하면 서로 다른 두 가지 인수분해를 갖는 더 작은 수가 생기므로 모순이다.

1.8 유리수 세기

1. $\frac{3}{5}$: 부모를 거슬러 올라가면 $(3,5) \leftarrow (3,2) \leftarrow (1,2) \leftarrow (1,1)$이고, 위치는 $1 \to 2 \to 5 \to 10$이므로 $f(10) = \frac{3}{5}$이다. $\frac{5}{3}$: $(5,3) \leftarrow (2,3) \leftarrow (2,1) \leftarrow (1,1)$이고, 위치는 $1 \to 3 \to 6 \to 13$이므로 $f(13) = \frac{5}{3}$이다.

2. Newman의 규칙 $x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}$을 적용하면 $1, \frac{1}{2}, 2, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, 3, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}$를 얻으며, 이는 $f(1), \ldots, f(10)$과 일치한다.

3. n번째 수의 n번째 자리 숫자가 5이면 4를, 그렇지 않으면 5를 n번째 자리 숫자로 고른다. 이렇게 만든 십진 소수(decimal)는 목록의 모든 수와 다르며, 0과 9를 피했으므로 십진 전개가 하나뿐이어서 실제로 다른 수이다.

4. 모든 양의 정수는 2의 거듭제곱과 홀수의 곱 $2^{m-1}(2n-1)$로 유일하게 나타나므로, $(m,n) \mapsto 2^{m-1}(2n-1)$은 전단사(bijection)이다.

1.9 삼차곡선의 접선

1. $y = t(x+1)$을 $x^2 + y^2 = 1$에 대입하면 $(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0$이고, 근은 -1과 $\frac{1-t^2}{1+t^2}$이다. $t = \frac{q}{p}$로 두면 그 점은 $\left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$이고, 이로부터 세 쌍 $(p^2-q^2, 2pq, p^2+q^2)$을 얻는다.

2. 직선은 $x + y = 3$이고, $x^3 + (3-x)^3 = 9$는 $9x^2 - 27x + 18 = 0$으로 정리된다. 삼차항이 소거되어 $x = 1, 2$만 남는다. 이 직선은 점근선(asymptote) $y = -x$와 평행하며, 세 번째 교점은 무한히 먼 곳에 있다.

3. 접선(tangent)의 기울기(gradient)는 $\frac{x^2}{y^2} = \frac{289}{400}$이고, 접선은 곡선과 $\left(-\frac{188479}{90391}, -\frac{36520}{90391}\right)$에서 다시 만난다. 분모를 없애면 $188479^3 = 36520^3 + 90391^3 + 180782^3$이다.

4. 직선은 $x^3 + y^3 = 1729$와 $\left(-\frac{37}{3}, \frac{46}{3}\right)$에서 다시 만나므로 $46^3 = 37^3 + 27 \times 1729 = 37^3 + 3^3 + 36^3$이다($27 = 3^3$과 $27 \times 1728 = 36^3$을 이용했다).

Beyond STEP

STEP은 대부분의 학생이 학창 시절에 치르는 수학 시험 가운데 가장 어려운 시험이다. 또한 가장 훌륭한 시험 가운데 하나이기도 하다. 문제는 짧고 낯설며 깊이가 있고, 그중 가장 뛰어난 문제들은 대학 수학의 작은 조각이 모습을 감추고 있는 것이다.

이 책은 1987년 첫 시험에 앞서 나온 예시 시험지(specimen papers)부터 2025년 시험지까지 가운데 가장 흥미로운 STEP 문제들을 골라, 각 문제를 하나의 문으로 삼는다. 모든 문제는 뛰어난 학생이 풀어 가면서 던질 법한 질문들과 함께 꼼꼼하게 풀이하고, 그런 다음 책은 그 문을 지나 한 걸음 더 나아간다. 그 아이디어가 어디에서 왔는지, 대학에서는 무엇으로 발전하는지, 그리고 다음에는 무엇을 읽으면 좋은지를 살펴본다.

이 책은 STEP을 준비하면서 기출 문제 연습 이상의 것을 원하는 재능 있는 예비 수학자를 위해 쓰였다. 수학과 학부생처럼 생각하기 시작하고, 앞으로 무엇이 자신을 기다리고 있는지 알아보고 싶은 학생들을 위한 책이다.

- 순수수학(pure mathematics), 역학(mechanics), 확률(probability)과 통계(statistics)를 아우르는 13개의 장
- 이 36개의 STEP 기출 문제와 각 문제의 안내식 풀이
- 모든 문제 뒤에 숨은 대학 수학
- 답이 실린 후속 연습 문제와 더 읽을거리

전체 13개 장 가운데 제1장. 책 전체와 모든 장,
모든 풀이를 다음 주소에서 무료로 읽고, 내려받고, 공유할 수 있다.

beyondstep.keithmcnulty.org

본문은 퍼블릭 도메인(CC0 1.0)으로 공개한다. STEP 문제 © Cambridge University Press & Assessment.

