1.9 삼차곡선의 접선

학습지

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

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

1단계 접선

생각해 보기 $y^3 = x^3 + a^3 + b^3$을 음함수 미분(implicit differentiation)한다. a와 b는 상수임을 기억한다.

잠깐, 직접 해 보기 점 $(-a, b)$에서의 기울기(gradient)를 구하고, 그 점을 지나는 직선의 방정식을 쓴 뒤 분모를 없앤다.

2단계 접선이 곡선과 다시 만나는 점

생각해 보기 접선을 $y = \ldots$ 꼴로 쓰고 $y^3 = x^3 + 9$에 대입한다.

생각해 보기 전개하여 모든 항을 한쪽으로 모은 다음, 계수들의 공약수를 찾는다.

3단계 삼차방정식 풀기

생각해 보기 접점으로부터 삼차방정식(cubic)의 근 하나를 이미 알고 있다.

잠깐, 직접 해 보기 접선은 곡선에 접하므로 접점은 **중근**(repeated root)이다. $(x+1)^2$으로 나누어 세 번째 근을 구하고, 접선이 곡선과 다시 만나는 점을 찾는다.

생각해 보기 그 점은 $y^3 = x^3 + 9$ 위에 있다. 분모를 없앤다. 남은 항은 세제곱수가 아니지만 $9 = 1^3 + 2^3$이다.

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.

더 도전하기

1 **원 위의 유리점.** $(-1, 0)$을 지나고 기울기가 t인 직선은 원 $x^2 + y^2 = 1$과 다시 만난다. 다른 교점이 $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$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.

안내에 따른 전체 풀이는 제 1.9절에 있다:
https://beyondstep.keithmcnulty.org/ko/ch01/tangents-cubic.html

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