1.9 三次曲線の接線

ワークシート

問題

STEP I 2009、問 2

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

ヒント

まずは自力で問題に取り組んでみよう。行き詰まったら、ヒントを**一つずつ**読み、そのたびに問題に戻ること。**手を止めて、やってみよう**と記したヒントが重要な段階である。各ヒントの後には計算用の余白がある。

? **考えてみよう**　点 $(-a, b)$ はこの曲線上にある。なぜか。また、そのことは立方数の和とどう関係するのか。

段階 1 接線

考えてみよう $y^3 = x^3 + a^3 + b^3$ を陰関数微分（implicit differentiation）せよ。a と b は定数であることに注意する。

手を止めて、やってみよう 点 $(-a, b)$ における傾きを求め、その点を通る直線の方程式を書き、分母を払え。

段階 2 接線が曲線と再び交わる点

考えてみよう 接線を $y = \ldots$ の形に書き、$y^3 = x^3 + 9$ に代入せよ。

考えてみよう　展開してすべての項を一方の辺に集め、係数の共通因数を探せ。

段階 3　3 次方程式を解く

考えてみよう　接点から、この 3 次方程式（cubic equation）の解の一つはすでにわかっている。

手を止めて、やってみよう　接線は曲線に接するので、接点の x 座標は**重解**（repeated root）である。$(x+1)^2$ で割って 3 つ目の解を求め、接線が曲線と再び交わる点を求めよ。

考えてみよう その点は $y^3 = x^3 + 9$ 上にある。分母を払え。残った項は立方数ではないが、$9 = 1^3 + 2^3$ である。

背後にある数学

弦と接線の方法

$y^3 = x^3 + 9$ や、より標準的な形 $y^2 = x^3 + Ax + B$ のような三次曲線を考える。その上にある有理数座標の点を二つ知っていれば、それらを通る直線は曲線とちょうどもう一点で交わり、その点も有理数座標をもつ（**振り返り**での議論による）。一点しか知らなければ、代わりにその点での接線を使えばよい。いずれにしても、既知の有理点から新しい有理点が生まれる。

驚くべきことに、この「弦（chord）と接線」による構成は、曲線上の点を**足し合わせる**方法に仕立てることができ、そのとき有理点全体は**群**（group）をなす。群とは、大学 1 年次で学ぶ代数的構造である。Louis Mordell は 1922 年に、この群が有限個の点で生成されることを証明した。すなわち、有理点がどれだけたくさんあっても、そのすべては有限個の点から弦と接線を用いて作り出せる。彼の証明は、Section 1.5 で扱ったフェルマー（Fermat）の無限降下法（descent）の一種である。

今日の楕円曲線

このような曲線は**楕円曲線**とよばれる（楕円であるからではなく、楕円の弧長との歴史的なつながりによる）。楕円曲線は現代数学のいたるところに現れる。

- **フェルマーの最終定理。** 1980 年代、Gerhard Frey は、$x^n + y^n = z^n$ の解が存在すれば、非常に奇妙な楕円曲線が生じることに気づいた。1994 年、アンドリュー・ワイルズ（Andrew Wiles）はそのような奇妙な曲線が存在しえないことを証明し、こうしてフェルマーの最終定理を証明した。

- **バーチ・スウィンナートン＝ダイアー予想（Birch and Swinnerton-Dyer conjecture）。**有理点のなす群には、生成元（generator）がいくつ必要なのだろうか。1960 年代に、ケンブリッジで行われた数学における最初期のコンピュータ実験をもとに立てられた予想は、素数を法として点を数えることから作られる関数を用いて、その答えを予言している。これは七つのミレニアム懸賞問題（Millennium Prize Problems）の一つである。

- **暗号（cryptography）。**有限の数の体系の上の楕円曲線では、点 P を自分自身に n 回足す計算は、n が何百桁もあっても速く行える（高い累乗を二乗の繰り返しで計算するのと同じように、P を繰り返し 2 倍すればよい）。ところが、P と結果 nP が与えられたとき、n を求めることはきわめて難しいと考えられている。これが**楕円曲線離散対数問題**（elliptic-curve discrete logarithm problem）である。この非対称性が、今日のオンライン通信の多くを守っている。

同じ次数の累乗の和

三つの正の立方数の和となる最小の立方数は $6^3 = 3^3 + 4^3 + 5^3$ である。接線の方法で見つかった $20^3 = 7^3 + 14^3 + 17^3$ はその倍数ではなく、この方法を繰り返すと新しい恒等式が次々に得られる（ただし負の数を含むものもある）。ある k 乗数を作るには、k 乗数がいくつ必要だろうか。オイラー（Euler）は 1769 年に、ある k 乗数を作るには少なくとも k 個の k 乗数が必要であると予想した。4 乗と 5 乗については、この予想は誤りであった。1966 年、Leon Lander と Thomas Parkin はコンピュータによる探索で

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

を発見し、1988 年には Noam Elkies が楕円曲線を用いて 4 乗の場合の反例を見つけた。

次の一歩

1. **円上の有理点。**$(-1, 0)$ を通り傾きが t の直線は、円 $x^2 + y^2 = 1$ ともう一点で交わる。その点が $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$ であることを示し、これを用いてピタゴラス数（Pythagorean triples）を無数に作れ。

2. **交わらない弦。**点 $(1, 2)$ と $(2, 1)$ は $x^3 + y^3 = 9$ 上にある。これらを通る直線は、曲線とほかの点では交わらないことを示せ。「三つ目の点」はどこへ行ったのだろうか。（**無限遠点**（point at infinity）について調べてみよ。）

3. **技法を繰り返す。**$\left(\frac{17}{7}, \frac{20}{7}\right)$ における $y^3 = x^3 + 9$ の接線と、それが曲線と交わる三つ目の点を求めよ。（数式処理システム（computer algebra system）を使うとよい。数がいかに急速に大きくなるかに注目せよ。）

4 **タクシー数（taxicab numbers）。** $1729 = 1^3 + 12^3 = 9^3 + 10^3$ である。$(1, 12)$ と $(9, 10)$ を通る直線が曲線 $x^3 + y^3 = 1729$ と交わる三つ目の点を求め、$p^3 = q^3 + r^3 + s^3$ の形の新しい恒等式を導け。

さらに学ぶために

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves***（Springer）。邦題『楕円曲線論入門』。学部生向けに書かれており、第 1 章は A レベル（A level、英国の大学入学資格試験）を超える知識を必要としない。
- **Avner Ash & Robert Gross, *Elliptic Tales***（Princeton University Press）。バーチ・スウィンナートン＝ダイアー予想へと至る一般向けの解説書。
- **Simon Singh, *Fermat's Last Theorem***。邦題『フェルマーの最終定理』。楕円曲線が 350 年来の難問を解決するに至った経緯を描く。

詳しい解説付きの解答は第 1.9 節にある：

https://beyondstep.keithmcnulty.org/ja/ch01/tangents-cubic.html

毎週 1 問の STEP の問題を丁寧に解き明かす The STEP Up。メールで無料配信中：keithmcnulty.substack.com