

整数論、幾何と L -関数

坂内健一

私の専門は整数論で、特にその中でも数論幾何学を研究しています。数論幾何学とは、幾何学的な直感を導入して、整数論の問題にアプローチする分野です。ここでは、整数論において非常に面白いと思われる楕円曲線の Birch and Swinnerton-Dyer 予想 (BSD 予想) について解説し、方程式の有理数解を求める問題に幾何がどう関わってくるか、紹介します。

1. DIOPHANTINE 問題と幾何

方程式が与えられたとき、その方程式の整数解や有理数解を求める問題は、Diophantine 問題と呼ばれています。

Example 1.1. 例えば $x^2 + y^2 = 1$ という方程式が与えられたとき、この場合の Diophantine 問題は、この方程式をみたす $x, y \in \mathbb{Z}$ や $x, y \in \mathbb{Q}$ がどれだけあるか調べるという問題です。ちなみにこの場合、整数解は、 $(x, y) = (\pm 1, 0), (0, \pm 1)$ です。有理数解がどれだけあるか、わかりますでしょうか？

Example 1.2. もっとも有名な Diophantine 問題として、1994 年、Andrew Wiles によって解決された、Fermat 予想があります。これは n を 3 以上の整数とすると、 $X^n + Y^n = Z^n$ をみたす 0 と異なる整数 X, Y, Z は存在しない、という主張です。両辺を Z で割り、 $x = X/Z, y = Y/Z$ を取ると、

$$x^n + y^n = 1$$

をみたす 0 と異なる有理数は存在しない、という主張と同値になることがわかります。

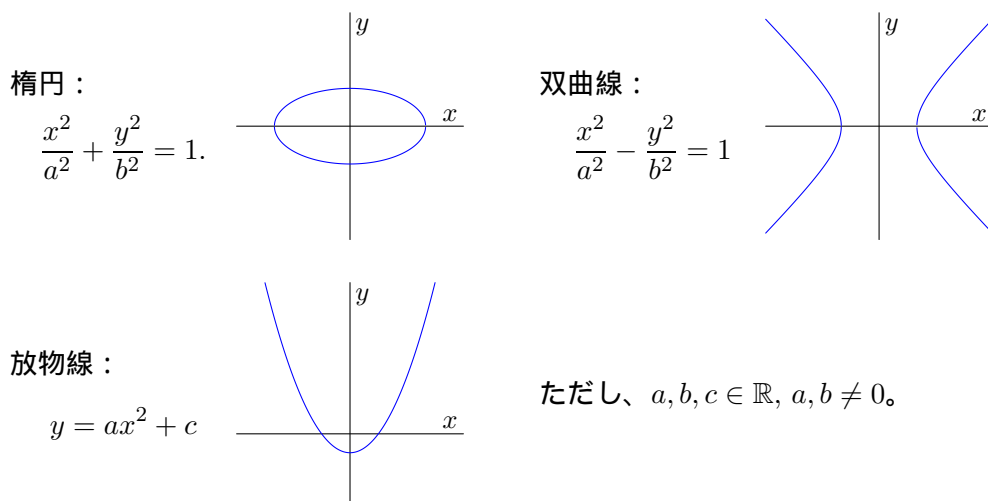
$x^n + y^n = 1$ などの方程式は実平面の中の曲線を描きます。こう解釈すると、Diophantine 問題は、平面 (あるいは空間) の中の図形の有理点、すなわち座標が有理数で表される点を求めるという問題に置き換わります。この様な幾何学的な直感を導入して、これから Diophantine 問題を 2 次曲線の場合と楕円曲線の場合に考えて行きましょう。

2. 2次曲線の DIOPHANTINE 問題

2次曲線とは一般的な方程式で

$$a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0, \quad (a_1, \dots, a_6 \in \mathbb{R})$$

という形で表される曲線です。ただし退化している場合、すなわち、つまらないものになってしまう場合は除外しておきます。例えば $x^2 - y^2 = 0$ は $(x+y)(x-y) = 0$ となり、2つの直線 $x = y, x = -y$ の合併になってしまうため除外しておきます。退化しない2次曲線を適当に変数変換すると、以下の3つの場合に帰着されることが知られています。



以下では2次曲線が \mathbb{Q} 上定義された場合、すなわち $a, b, c \in \mathbb{Q}$ の場合のみ考えます。2次曲線が扱いやすい理由は、パラメーター表示を持つからです。例えば Example 1.1 をパラメーター表示で考えてみましょう。

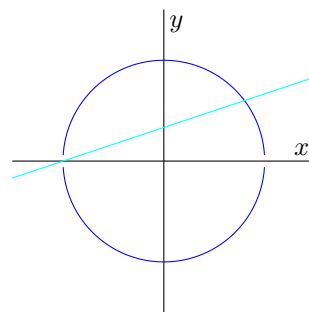
まず始めに点 $(-1, 0)$ は単位円上の有理点です。次にこの点を通り、傾きが t の直線 $y = t(x + 1)$ を考えます。この直線と単位円の交点を計算するために

$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x + 1) \end{cases}$$

を連立させると、 $(t^2 + 1)x^2 + 2t^2x + t^2 - 1 = 0$ となるので、 $(-1, 0)$ と異なる直線と円の交点は

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right)$$

であることが分かります。



t が有理数であれば、 (x, y) も有理数となり、逆に交点 (x, y) が有理数であれば、 $(-1, 0)$ と (x, y) を結ぶ直線の傾きも有理数になります。また、直線 $x = -1$ は点 $(-1, 0)$ で円と接するので、 $x = -1$ の傾きを便宜上 $t = \infty$ と呼ぶことにすると、単位円 $x^2 + y^2 = 1$ の有理点は、

$$t \in \mathbb{Q} \cup \{\infty\}$$

と 1 対 1 に対応していることが分かります。 $\mathbb{Q} \cup \{\infty\}$ は射影直線と呼ばれ、 $\mathbb{P}^1(\mathbb{Q})$ などと記されます。すなわち単位円 $x^2 + y^2 = 1$ の点は、射影直線 $\mathbb{P}^1(\mathbb{Q})$ の点と 1 対 1 に対応することが導かれました。双曲線でも似たようなことができます。

Problem 2.1. 双曲線 $x^2 - y^2 = 3$ の有理点を求めよ。

上の問題では、2 つの漸近線のかなたに無限点があるとして下さい。そうするとこの場合でも、2 つの無限遠点を含めた有理点の集合は $\mathbb{P}^1(\mathbb{Q})$ の点と 1 対 1 に対応することが導かれます。

2 次曲線に有理点が 1 つでも存在すれば、以上の方法で、その 2 次曲線の無限点も含めた有理点全体の集合は $\mathbb{P}^1(\mathbb{Q})$ の点と 1 対 1 に対応していることが分かります。それでは、2 次曲線には必ず有理点が少なくとも 1 つは存在するのでしょうか？実平面の中には有理点がびっしりと詰まっているので、有理点を避けて通る曲線なんて無いような気がしてしまうかもしれません。しかし、有理点を持たない 2 次曲線も、実はいっぱい存在するのです。

Proposition 2.2. $x^2 + y^2 = 3$ をみたす有理数 $x, y \in \mathbb{Q}$ は存在しない。

Proof. 背理法で証明する。有理数解 x, y が存在すると仮定する。通分すると、 $x = X/Z$ 、 $y = Y/Z$ 、ただし $X, Y, Z \in \mathbb{Z}$ と書ける。方程式は $X^2 + Y^2 = 3Z^2$ として良い。 X, Y, Z の最大公約数を d としたとき、 $X' = X/d$ 、 $Y' = Y/d$ 、 $Z' = Z/d$ において X, Y, Z のかわりに用いることで、 X, Y, Z の最大公約数は 1 であると仮定して良い。求める方程式を $\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z}$ の中で考えると、

$$X^2 + Y^2 \equiv 0 \pmod{3}$$

となる。 $X, Y \equiv 0, 1, 2$ に対して、 $X^2 \equiv 0, 1, Y^2 \equiv 0, 1$ となる。従って、上の方程式をみたすのは、 $X^2 \equiv Y^2 \equiv 0$ 、すなわち $X \equiv Y \equiv 0$ のときだけである。これは、 X と Y が 3 の倍数であることを意味し、方程式から Z も 3 の倍数となってしまふ。これは X, Y, Z の最大公約数が 1 であることに矛盾している。従って、有理数解 x, y は存在しない。 \square

平面に半径3の単位円を書いてみて下さい。上の結果から、この円上のどの点をとっても、それは有理点でないことが分かります。平面上にびっしりと有理点があるにも関わらず、この円は、なぜか有理点をうまく避けています。

Problem 2.3. $x^2 - 2y^2 = 3$ をみたす有理数 $x, y \in \mathbb{Q}$ は存在するか？

以上のことから、2次曲線の無限遠点を含めた有理点の集合は、 $\mathbb{P}^1(\mathbb{Q})$ が空集合のいずれかになることが分かります。

3. 楕円曲線の DIOPHANTINE 問題

\mathbb{Q} 上定義された楕円曲線とは、 $a_1, a_2, \dots, a_6 \in \mathbb{Q}$ に対し、

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

で表される曲線です。ただし2次曲線の場合と同様、退化する場合は除いておきます。この曲線は

$$y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{Q})$$

という形の標準形へ持って行くことができることが知られています。このとき、退化するのは「右辺=0」という方程式が重根を持つ場合、つまりは判別式 $\Delta := -16(4a^2 - 27b^2)$ が0となるときです。上の方程式で表される楕円曲線を E と書き、その有理点全体の集合を $E(\mathbb{Q})$ と記します。ただし無限遠点を1つ余分に付け加えておきます。すなわち、

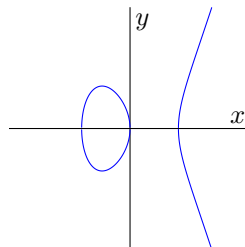
$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

とします。

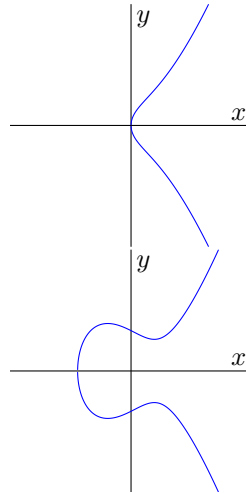
それでは、様々な楕円曲線に対して、有理点はどれだけあるのでしょうか？何個か知られている例をあげてみます。

$E : y^2 = x^3 - 4x$ のとき、

$$E(\mathbb{Q}) = \{(0, 0), (-2, 0), (2, 0), \infty\}.$$



$E : y^2 = x^3 + x$ のとき、
 $E(\mathbb{Q}) = \{(0, 0), \infty\}$.

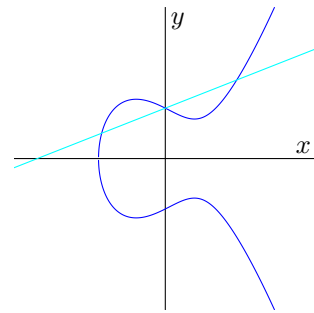


$E : y^2 = x^3 - x + 1$ のとき、
 $E(\mathbb{Q}) = \text{無限集合}$

点の数が有限個の場合もありますし、点の数が無限個の場合もあることが知られています。2次曲線の場合と様子が違うことが見て取れます。楕円曲線では有理点の個数が大きく変動することが知られています。これは、楕円曲線が2次曲線のようなパラメーター表示を持たないことが知られていることにも起因しています。

例えば楕円曲線に1つ有理点があったとして、その点を通る直線を考えてと、その直線は楕円曲線と合計3点で交わり、最初の点が有理点で直線の傾きが有理点だとしても、残りの2点が有理点であるとは限りません。楕円曲線の場合、パラメーター表示に代わる何かはあるのでしょうか？

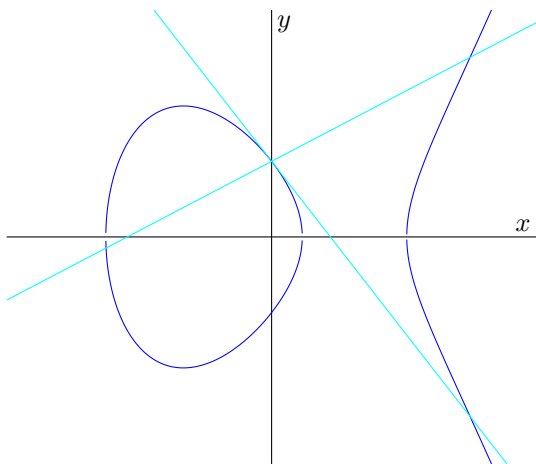
楕円曲線の2つの点 P, Q に対して、その2点を通る直線は、楕円曲線と3点目 R で交わります。 P, Q が有理点であるとする、そこを通る直線の傾きも有理数となり、点 R も有理点になることが分かります。また、楕円曲線の式からグラフは x 軸に対して対称となることから、点 R を x 軸でひっくり返した点 R' も有理点となることが分かります。以後、この様に得られた点 R' を、 $R' = P + Q$ と書きます。楕円曲線の有理点 $E(\mathbb{Q})$ は、この演算に関して無限遠点 ∞ を単位元とするアーベル群になっていることが知られています。



これに関して、以下の結果が知られています。

Theorem 3.1 (Mordell の定理). $E(\mathbb{Q})$ は有限生成なアーベル群である。

アーベル群の基本定理から、 $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus$ 有限群 と表されることが知られています。 $r = \text{rank } E(\mathbb{Q})$ は $E(\mathbb{Q})$ のアーベル群としての階数ですが、この r を楕円曲線 E の階数とも呼ぶことにします。



楕円曲線の有理点 P が与えられたとき、 $2P = P + P$ は P での接線を用いて定義します。 $3P = 2P + P$, $4P = 3P + P$, \dots という操作を繰り返すことで、 P から別な有理点へと移って行きます。Mordell の定理が主張していることは、 $E(\mathbb{Q})$ は P_1, \dots, P_n という有限個の有理点から上の操作で生成されているということです。

任意に楕円曲線が与えられたとき、その楕円曲線の有理点を見つけるための有効なアルゴリズムは現在のところ知られていません。有理点を与えられたとき、加法構造を用いて新しい有理点を作ることもできますが、楕円曲線の有理点すべてを具体的に求めることは非常に興味深い問題でありながら、現在人類の持つ技術では難しい問題でもあります。

このような状況のなか、与えられた楕円曲線の階数の大きさを予想しているのが Birch and Swinnerton-Dyer 予想です。

4. BIRCH AND SWINNERTON-DYER 予想

Birch and Swinnerton-Dyer 予想は、楕円曲線の階数が L -関数と呼ばれる解析関数で記述されると予想しています。この予想は、幾何学的な対象の数論的な情報と L -関数の関係を調べるという数論幾何学の中心的なテーマに含まれています。まずは楕円曲線の L -関数の定義から始めます。

楕円曲線 E が与えられたとき、適当な変数変換をして

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (a_1, a_2, \dots, a_6 \in \mathbb{Z})$$

と、係数が整数のものとして表すことができます。この標準形の判別式は $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ 、ただし $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_3^2a_2 - a_4^2$ と表されます。楕円曲線 E に対して、以下では整数係数の標準形のうち、判別式を割る各素数の指数が最も少ないものを取ることになります。

L -関数とは、各素数ごとの情報を解析的に集めて作る複素関数です。 p を素数として、 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ を位数 p の有限体とします。また、 E の \mathbb{F}_p -有理点を

$$E(\mathbb{F}_p) := \{(x, y) \in \mathbb{F}_p \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

と定義し、 $E(\mathbb{F}_p)$ に含まれる元の個数を $\#E(\mathbb{F}_p)$ と記して

$$a_p := 1 + p - \#E(\mathbb{F}_p)$$

とおきます。 E の L -関数を次の様に定義します。

Definition 4.1. $s \in \mathbb{C}$ に対し、

$$L(E, s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1} \times \prod_{p \mid \Delta} (1 - a_p p^{-s})^{-1}.$$

上の無限積は s の実数部分 $\operatorname{Re}(s) > \frac{3}{2}$ のときに絶対収束し、 $L(E, s)$ は s の正則関数となります。この関数は全平面へ有理型関数として解析接続されることが知られています。Birch and Swinnerton-Dyer 予想は次の通りです。

Conjecture 4.2 (Birch and Swinnerton-Dyer 予想 (BSD 予想)).

$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E, s).$$

ただし $\operatorname{ord}_{s=1} L(E, s)$ は $L(E, s)$ の $s = 1$ での零の位数。

すなわち、 $E(\mathbb{Q})$ のアーベル群としての階数が、 $L(E, s)$ の $s = 1$ での零点の位数 $\operatorname{ord}_{s=1} L(E, s)$ で記述されていると予想しています。この予想はとても重要でありますが、Coates-Wiles, Gross-Zagier や Kolyvagin など多くの研究者の努力にも関わらず、次の限られた場合にしか確かめられていません。

$$\operatorname{ord}_{s=1} L(E, s) \leq 1 \quad \Rightarrow \quad \operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E, s).$$

多くの数値実験などにより、この予想が高階数の場合にも正しいことが期待されていますが、現在のところまだ証明されていません。

BSD 予想は、楕円曲線のより精密な数論的情報を L -関数で記述するという方向でも拡張されており、Deligne 予想、Beilinson 予想、Bloch-Kato の玉河数予想など、方程式で定義された幾何学的図形の数論的な情報と L -関数との関係を記述する様々な予想の出発点となっています。

この様な話から分かる様に、数論幾何は整数論のみならず、代数、幾何や解析の様々な分野の手法を用います。幅広い広がりの中に未解決な大予想を多く含みますが、手の届く素朴な問題もまた数多くあります。興味を持ったら遊びに来て下さい。お待ちしております。