代数方程式の有理数解と楕円曲線

東京理科大学 理学部第一部 数学科 講師　吉川（よしかわ）　祥（しょう）

1．はじめに

$\frac{5}{3}$ や $2=\frac{2}{1}$ のように，二つの整数の比としてあらわされる数のことを**有理数**といいます．中学校のとき，$\sqrt{2}$ が有理数でないことを学んだ人も多いかと思います．これは，数の世界には有理数以外の数もあるということを初めて知る機会でもあり，背理法という証明の手法に触れるほぼ最初の機会でもあります．$\sqrt{2}$ が有理数でないことは，「方程式 $x^2=2$ を満たす有理数 x は存在しない」と言い換えることもできます．

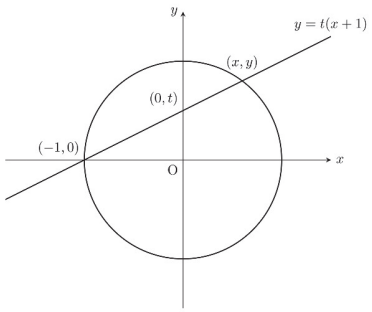
この方程式を少しだけずらした方程式 $x^2=1.9999899241$ を考えると，これを満たす有理数 x は実際に存在します（$x=\pm\frac{141421}{100000}$）．しかし，更にほんの少しだけずらして $x^2=1.999989924$ を考えると，これを満たす有理数 x は途端になくなってしまいます．方程式を満たす有理数というものは，気まぐれに現れたり現れなかったりする，とても微妙なものと言えます．

このことは，有理数という数たちが「数直線の上に粒子のように隙間なくぎっしりと詰まっているが，べったりとは広がっておらず，実はスカスカに分布している」という事情からきています．すなわち，有理数というものは非常に素朴で身近であるものの，海の中を漂う無数の微生物たちをキャッチするのが難しいように，（実数や複素数まで広げた）数の世界に漂う有理数たちを正確に捉えるのは難しいのです．

2．方程式の有理数解

先ほど，$x^2=2$ という方程式を考えましたが，もう少し難しくして，C: $x^2+y^2=1$ という方程式を考えてみましょう．この方程式は，視覚的には，座標平面上の単位円（原点を中心とした半径 1 の円）を表しています．この方程式には，どのような**有理数解**（この方程式を満たす有理数の組 (x,y)）があるでしょうか．つまり，1 がどのような二つの有理数の平方和として表されるだろうか，ということです．図形的に言い換えれば，単位円の上に，x 座標も y 座標も有理数であるような点（**有理点**といいます）はどのくらいあるか，という問いになります．

まず，円 C 上には $(\pm1,0)$，$(0,\pm1)$ という有理点があることに気付きます．実は，そのほかの有理点もすべて列挙することができます．有理点 $(x,y)\neq(-1,0)$ があったとすると，$(-1,0)$ と (x,y) を結ぶ直線を考えることにより，直線と y 軸との交点が（y 軸の）有理点を定めます．逆に，y 軸上の有理点 $(0,t)$ があれば，$(-1,0)$ と $(0,t)$ とを通る直線を考え，その直線と C との交点をとることにより C 上の有理点が得られます．C 上の $(-1,0)$ 以外の有理点は，y 軸（つまり数直線）の有理点一つ一つと対応していることになります**【図 1】**．



【図 1】

詳細は略しますが，以上をまとめると，C 上の有理点は $(-1,0)$ と $\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$（$t$ は有理数）で尽くされることになります．

2．1．代数方程式

$x^2+y^2=1$ は，（整数係数の）**代数方程式**の一例ということができます．ほかにはどのような代数方程式があるでしょうか．代数方程式とは，$x^2y-yz+z^4=3$，$y^2=x^3-2$，$x^5+y^5=1$，… などのように，いくつかの未知数の足し算や掛け算を組み合わせて作られる方程式のことです．もちろん，このような方程式は無数にあります．

整数論という数学の分野において非常に基本的で重要な問いは，「こうした代数方程式が有理数解を持つか？」「もし持つなら有理数解を求められるか？」という問いです．このような問いは素朴であることが多いですが，先に述べたように「数の世界の中で有理数を捉えるのが難しい」という事情に起因して，代数方程式の有理数解を決定する問題は，一般には非常に困難になります．

たとえば，Fermat の最終定理ということばを耳にしたことはあるでしょうか．これは，「n が 3 以上の整数のとき，$X^n+Y^n=Z^n$ という方程式を満たすような整数 $X,Y,Z(\neq 0)$ は存在しない」というものです．有理数解ではなく整数解に関する問題ですが，（両辺を Z^n で割って $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$ と置き換えることで）「n が 3 以上の整数のとき，$x^n+y^n=1$ の有理数解は $(x,y)=(\pm 1,0),(0,\pm 1)$ のみである（マイナスは n が偶数のときのみ）」と言い換えられます．Fermat の最終定理は，Fermat が本の余白に（証明をつけずに）書き残したもので，完全に解決されるまでには 360 年もの歳月を要した難問として有名です．Fermat の最終定理とその解決にまつわる物語は非常にドラマティックなので，ぜひ参考文献 4) を読んでいただきたいと思います．

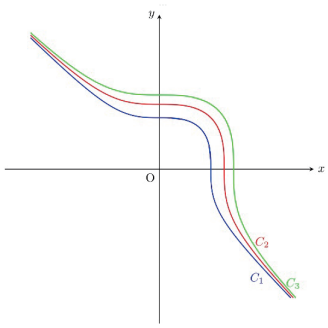
話を戻すと，一つの方程式の有理数解の問題ですら大変な困難となり得るのですから，あらゆる代数方程式の有理数解を統一的に求めることはほとんど不可能のように思われます．一方，特定の方程式に注目すれば，有理数解を求めることができるのです．特に面白いのは，方程式が他の数学と結びついていたり，方程式自身がより深い構造を持っていたりする場合です．本稿では，方程式が楕円曲線と呼ばれる曲線を定める場合に絞って説明します．

2．2．特別な代数方程式と楕円曲線

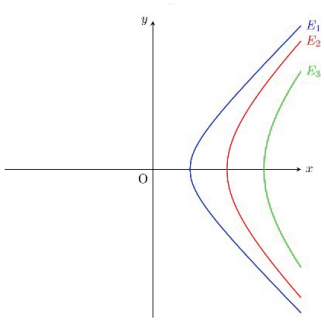
ここでは，$x^3+y^3=1$, $x^3+y^3=2$, ... のように，

$$C_d\colon x^3+y^3=d\ （\text{ただし，}d=1,2,3,\ldots）$$

という方程式の有理数解に注目してみましょう．つまり，$d=1,2,3,\ldots$ が二つの有理数の立方和として書けるかどうか？ということです．この C_d は座標平面上の曲線を定めており，その曲線上の有理点について知りたいというわけです．以下でも，「方程式の有理数解」と「曲線上の有理点」は同じ意味で用いることにします．



【図 2】



【図 3】

まず，$C_1\colon x^3+y^3=1$ は Fermat の最終定理の $n=3$ の場合に相当します．この場合は Euler によって研究されており，上述のように有理数解は $(x,y)=(1,0),(0,1)$ のみであることが知られています．

では，一般の $d=1,2,3,\ldots$ に対して，C_d の有理数解はどのようになっているでしょうか．実は C_d は**楕円曲線**と呼ばれるものになっています．楕円曲線の導入については，松本雄也氏の記事をあわせてご覧ください．楕円曲線は $y^2=x^3+ax+b$（ここで a, b は $4a^3+27b^2\neq 0$ をみたす有理数）という形の方程式によってあらわされる曲線（に無限遠点をひとつ加えたもの）だということが出来ますが，一見すると C_d は楕円曲線とは別物のように思えます．しかし，C_d において

$$x=\frac{36d-Y}{6X},\ y=\frac{36d+Y}{6X}$$

と置き換えて式を整理すると，楕円曲線

$$E_d\colon Y^2=X^3-432d^2$$

が現れます．逆に，この楕円曲線 E_d の式に対して

$$X=\frac{12d}{y+x},\ Y=36d\,\frac{y-x}{y+x}$$

のように置き換えると，もともとの $C_d\colon x^3+y^3=d$ が復元できます**【図 2，図 3】**．置き換えの具体的な式はさておき，重要なことは，

- C_d を考えることと E_d を考えることは本質的に同じであり，
- C_d の有理点と E_d の有理点は（上述の置き換えの式によって）ぴったり対応している，

ということです．

3．楕円曲線の有理点；Mordell-Weil 群

松本氏の記事でも強調されているように，楕円曲線のもつ特筆すべき性質は，「曲線の上にある 2 点 P,Q から新しい点 $P+Q$ や $-P$ を作り出す規則がある」

というものです．数学では，この性質を「楕円曲線の点は群をなす」と表現します．このことをより噛み砕いて表現すると，**楕円曲線の点同士の足し算や引き算ができる**ということです．特に，ひとつの点 P からはじめて，$2P=P+P$，$3P=2P+P$，$4P=3P+P$ や $-2P=-(2P)$，$-3P=-(3P)$，$-4P=-(4P)$ のように，多くの点を作り出すことができます．また，P と Q が有理点なら，新たに作られる $P+Q$ などもまた有理点になっていることも大事な点です．

私たちが考えている楕円曲線 E_d: $Y^2=X^3-432d^2$ においては，E_d 上の 2 点 $P=(x_P,y_P), Q=(x_Q,y_Q)$ に対して，$P+Q=(x_{P+Q},y_{P+Q})$ や $-P=(x_{-P},y_{-P})$ や $2P=(x_{2P},y_{2P})$ は以下のように具体的に計算されます：

$$x_{P+Q}=k^2-x_P-x_Q,\ y_{P+Q}=-kx_{P+Q}+kx_P-y_P$$

（ただし，$k=\dfrac{y_Q-y_P}{x_Q-x_P}$ とおく．）

$$x_{-P}=x_P,\qquad y_{-P}=-y_P$$

$$x_{2P}=k^2-2x_P,\qquad y_{2P}=-kx_{2P}+kx_P-y_P$$

（ただし，$k=\dfrac{3x_P^2}{2y_P}$ とおく．）

やや込み入っていますが，ここでは，$P+Q$，$-P$，$2P$ が以上のように具体的な式として計算できるという事実が重要です．

松本氏の記事でも紹介されているように，以下に述べる **Mordell の定理**は，楕円曲線の有理点に関する極めて重要な定理です．

定理（Mordell の定理）

E がどのような楕円曲線であっても，E の有理点全体のなす群は有限生成である．

「有限生成」や「群」という言葉は聞き馴染みがない方も多いかと思います．定理の意味を噛み砕いて説明すると以下のようになります．すなわち，

「E の有理点自体は無限にたくさんあるかもしれないが，いくつか（有限個！）の有理点 $P_1,\ldots,P_n$ を上手に選んでくれば，E のどんな有理点でも $P_1,\ldots,P_n$ たちの足し算や引き算を繰り返すことによって作ることができる」

ということです．

楕円曲線については古くから様々な研究があり，多くの場合にこのような「うまい有理点」$P_1,\ldots,P_n$ を求める手続き（アルゴリズム）が知られています．

さて，私たちの楕円曲線 E_d の有理点に関する事実をいくつか述べてみましょう．

- E_1: $y^2=x^3-432$ の有理点は $(x,y)=(12,36)$ と $(12,-36)$ のみである．これは，C_1: $x^3+y^3=1$ の有理数解が $(1,0)$ と $(0,1)$ のみであることに対応している．
- E_2: $y^2=x^3-432\cdot 2^2$ の有理点は $(x,y)=(12,0)$ のみである．
- E_3, E_4, E_5 の有理点は存在しない．（正確には，「無限遠点のみ」というべきではあります．）
- E_6: $y^2=x^3-432\cdot 6^2$ の有理点は，無限にたくさん存在する．正確には，$P=(28,80)$ とすると，P，$-P$，$2P$，$-2P$，$3P$，$-3P$，... によって有理点が全て尽くされ，どの 2 つも異なる有理点である．
- E_{10}: $y^2=x^3-432\cdot 10^2$ の有理点は存在しない．
- E_{19}: $y^2=x^3-432\cdot 19^2$ の有理点は，無限にたくさん存在する．正確には，$P=(57,171)$，$Q=(228,3420)$ とすると，$mP+nQ$（ただし m,n は整数で $(m,n)\neq(0,0)$）によって有理点がすべて尽くされ，これらのどの 2 つも異なる有理点である．

E_6 では，たった一つの有理点 $(28,80)$ から無限個のあらゆる有理点を作り出すことが出来る（！）ということになります．また，E_{19} では，二つの有理点 $P=(57,171)$，$Q=(228,3420)$ を組み合わせることによって，あらゆる有理点を作り出せることになります．このように，あらゆる有理数解がシステマティックに求められるということは非常に驚くべきことではないでしょうか．

4．E_d の階数

最後に少し進んだ話をしたいと思います．

4．1．楕円曲線の階数

実は，E_d という楕円曲線の特殊事情により，E_1 と E_2 以外の E_3, E_4, ... の有理数解の様子はいずれも次のどちらかとなっています：

（i）存在しない．

（ii）無限に多く存在する．それらはいくつかの有理点 $P_1,\ldots,P_r$ の足し算や引き算を組み合わせることで表せる．さらに，そうして得られる有理点はすべて互いに異なる．

（ii）の状況で，あらゆる有理点を作るために必要な点の最小個数 r を**階数**といいます（E_1, E_2 や（i）の場合，階数は 0 であるといいます）．したがって，E_1, E_2, E_3, E_4, E_5, E_{10} の階数は 0 で，E_6 の階数は 1，E_{19} の階数は 2 となります．感覚的には，E_d に有理数解が無限にたくさんある場合でも，無限にも「大きさ」があり，その大きさを測る尺度が階数だということです．

また，E_d 以外の楕円曲線についても，ほぼ同様に「有理数解の多さを測る尺度」として階数が定義されます．

4．2．楕円曲線の階数の分布

先に説明したように，楕円曲線は $y^2=x^3+ax+b$ で表される曲線であり，a,b を取り替えることで無数の楕円曲線が得られます．そして，一つ一つの楕円曲線 E に対して，階数 $r(E)$ という数が定まります．この $r(E)$ は素朴で基本的なものですが，実はとてもミステリアスな数です．例えば，以下の問いは，未だに完全な解決には至っていません：

（1）楕円曲線の階数として取り得る整数としては，いくらでも大きいものがあるか？

（2）階数 0 の楕円曲線は，楕円曲線全体のなかでどのくらいの割合を占めるか？　同様に，階数 1, 2, 3, ... ではどうか？

（1）については松本氏の記事に指摘があるので，ここでは（2）について説明しましょう．経験上・数値的なデータ上では，階数が 2 以上の楕円曲線は稀であり，大きい階数の楕円曲線を見付けるのは困難となっていきます．この状況のもと，楕円曲線全体のうち（階数 2 以上のものもわずかに存在するが）大半は階数が 0 か 1 だろうと予想されており，更に階数 0 と 1 のものが半々ずつ現れるだろうと予想されています．この予想に関する進展として，例えば Bhargava と Shankar[1] による次の結果が知られています：楕円曲線全体のうち階数が 0 か 1 であるものの割合は $\frac{5}{8}$ 以上である．

4．3．E_d たちの階数

最後に，私たちの楕円曲線 E_d: $y^2=x^3-432d^2$ $(d=1, 2, ...)$ の階数 $r(E_d)$ に目を向けてみましょう．実は，この E_d たちの階数に関しては非常に微妙な事情があるようです．

1980 年代，Zagier と Kramarz[3] は「E_d たちの中には，$r(E_d)\geq 2$ のものが正の割合で存在するのではないか」と予想しました．彼らが 70000 以下の d で計算していったところ，$r(E_d)\geq 2$ となる E_d の割合はほぼ定常的で 12% 程度だったようです．つまり，すべての楕円曲線のうち階数が 2 以上のものはごくわずかであると予想されているが，E_d たちに限って考えればそうではない（！）という興味深い考察です．

しかし，2000 年代に，Watkins[2] が「$r(E_d)\geq 2$ である E_d の割合は，やはりごくわずかかもしれない」とする根拠を提示しました．彼の計算によれば，そのような E_d の割合は，10^6 以下の d では 10% 程度であり，10^7 以下の d では 9% 弱であるというデータが得られています．すなわち，「考える d の範囲を広げていくと，階数 2 以上の E_d の割合は（極めてゆるやかだが）0% に近づいていくように見える」(!!) ということです．

近年では，コンピュータの性能の進歩や計算方法の改良により，更に膨大な計算が可能となっています．Watkins による指摘は，そのような進歩に依るところもあったでしょう．ただ，たくさんのデータを与えたとしても，100% の確証をもって「$r(E_d)\geq 2$ である E_d の割合は 0 に近づいていく」と結論付けることはまだまだ難しいように思えます．また，膨大なデータから正しそうな結論が見出せたとしても，あくまでも「正しそうだ」という推測です．理論的に証明が与えられてこそ，数学的に正しいと結論付けられるのです．現時点では困難に思えますが，未来の数学では，この問題を解決するような理論や技術が確立されるかもしれません．

謝辞

原稿にコメントをくださった，創域理工学部数理科学科の松本雄也氏，理学部数学科の大山口菜都美氏と小境雄太氏に厚く感謝を申し上げます．

[参考文献]

1）M. Bhargava, A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Annals of Mathematics 181(2015) : 587–621.

2）M. Watkins, *Rank distribution in a family of cubic twists*, London Mathematical Society Lecture Note Series 341(2007) : 237.

3）D. Zagier, G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, The Journal of the Indian Mathematical Society, 52 (1987), 51–69.

4）サイモン・シン著(青木薫訳), フェルマーの最終定理, 新潮文庫.