数理解析研究所講究録 1256 巻 2002 年 17-24

ある種の楕円曲線の族の Mordell-Weil ランクの有界性と Lang 予想

東京電機大・理工　山岸日出(Hizuru Yamagishi)
College of Science and Engineering
Tokyo Denki Univ.

Mordell-Weil ランクの高い楕円曲線は楕円曲線論において興味が持たれているものであるが, 自分はランクの高いものだけでなく, むしろ各ランクごとにできるだけ多くの(あるいはすべての)楕円曲線を構成する, という問題を考えている. これにはランクのみを考えるときもあるが, トーションパートの構造や j-invariant などの条件も満たすものを考える場合もある. このことからどのような楕円曲線が存在しないか, という問題も自然に導かれる.

k を数体, E を

$$y^2 = ax^4 + bx^2 + c \tag{1}$$

で定義される k 上の楕円曲線, $f(x)$ を (1) 式の右辺とし, E^ℓ で E の ℓ 個の直積を表わすものとする. このとき E^ℓ の定義式は

$$y_i^2 = f(x_i), \qquad i = 1,\ 2,\ \ldots,\ \ell$$

で表わされる. また ι_i を i 個目の E の involution で

$$\iota_i(x_i,\ y_i), \qquad i = 1,\ 2,\ \ldots,\ \ell$$

で定義されるものとし, さらに $V_\ell = E^\ell / < (\iota_1,\ \ldots\ , \iota_\ell) >$ とおくと V_ℓ の定義式は

$$y_i^2 = f(x_1)f(x_{i+1}), \qquad i = 1,\ 2,\ \ldots,\ \ell - 1$$

である. また 2 次拡大 $k(E^\ell)/k(V_\ell)$ による E のツイストを $E_{f(x_1)}$ とするとこれは

$$f(x_1)y^2 = f(x) \tag{2}$$

で定義され, $E_{f(x_1)}$ 上には ℓ 個の $k(V_\ell)$-有理点 $(x_1,\ 1)$, $(x_{i+1},\ y_i/f(x_1))$ $(i=1,\ 2,\ \ldots,\ \ell-1)$ がある. このとき $E_{f(x_1)}$ を V_ℓ の k-有理点で specialize すると ℓ 個の k-有理点をもつ k 上の楕円曲線が得られるので, V_ℓ の k-有理点に興味が持たれる. また一方, 次を示すことができる.

定理 1 E を *(1)* 式で定義される楕円曲線で, $(\alpha_i,\ \beta_i)$ $(i=1,\ 2,\ \ldots,\ \ell)$ を E の k-有理点とする. このときこれらの有理点をもつ E は $E_{f(x_1)}$ を V_ℓ の k-有理点 $(x_1,\ x_2,\ \ldots,\ x_\ell,\ y_1,\ y_2,\ \ldots,\ y_{\ell-1}) = (\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_\ell,\ \beta_1\beta_2,\ \beta_1\beta_3,\ \ldots,\ \beta_1\beta_\ell)$ で *specialize* することにより得られる.

証明. [5] と同様. □

次に V_ℓ の見方を変え, $x_{i+1}=\alpha_i$ $(i=0,\ 1,\ \ldots,\ \ell-1)$ とおき, 不定元とする. また, $K=k(\alpha_0,\ \alpha_1,\ldots,\ \alpha_{\ell-1})$ とおき, $a,\ b,\ c,\ y_1,\ y_2,\ \ldots,\ y_{\ell-1}$ を変数とし, V_ℓ を K 上の多様体と考える. この V_ℓ について K-有理点を調べる. まず, 次のことが示される.

定理 2 V_{n+1} は W_n と *K-birational* である. ここで W_n は

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \alpha_i^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & \alpha_i^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_i^2 \end{vmatrix} = 0, \qquad i=3,\ 4,\ \ldots,\ n$$

で定義される $\mathbf{P}^n(K)$ の部分多様体である. また $W_2=\mathbf{P}^2$ とする.

注意 3 W_n は非特異で $(2,\ 2,\ \ldots,\ 2)$-完全交叉曲面である. また W_n には 2^n 本の直線が含まれており, その定義方程式は

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_i^2 \\ Y_0 & (-1)^{\varepsilon_1}Y_1 & (-1)^{\varepsilon_i}Y_i \end{vmatrix} = 0, \qquad i=2,\ 3,\ \ldots,\ n, \tag{3}$$

ここで $\varepsilon_i = 0$ または 1, $i=1,\ \ldots,\ n$

である. これらの直線を W_n の trivial line と呼ぶ.

一方, Vojta の結果で次のようなものがある.

定理 4 ([3]) $n > 2$ に対し X_n を

$$x_i^2 - 2x_{i+1}^2 + x_{i+2}^2 = 2x_0^2, \qquad i = 1,\ 2,\ \ldots,\ n-2 \tag{4}$$

で定義される曲面とし, $n = 2$ のときは $X_2 = \mathbf{P}^2$ とする. X_n に含まれる 2^n 本の直線

$$\pm x_1 = \pm x_2 - x_0 = \pm x_3 - 2x_0 = \cdots = \pm x_n - (n-1)x_0 \tag{5}$$

を X_n の *trivial line* と呼ぶ. $n \geq 8$ のとき X_n の種数 0 または 1 の曲線は *trivial line* のみである.

この結果に関する背景を簡単に述べる. こちらは楕円曲線とは関係のない背景を持っており, Hilbert の第 10 問題を起源にもっている. Hilbert の第 10 問題は Matiyasevich によって既に解かれているがこれに関連して Büchi は次の問題を提起した.

問題 5 (Büchi) 次の方程式を満たす整数解が存在するかどうかを判定するアルゴリズムは存在するか？

$$\sum_{j=1}^{n} a_{ij}x_j^2 = b_i, \qquad i = 1,\ 2,\ \ldots,\ m, \quad a_{ij},\ b_i \text{は整数}.$$

もしこの答えが「存在しない」であればこのことより Hilbert の第 10 問題がすぐに解ける. そして次の予想 6 が正しければ問題 5 の答えが「存在しない」である, ということを Büchi 自身が示した.

予想 6 (n squares problem) 整数 $x_1,\ x_2,\ \ldots,\ x_n$ に対し, 連立方程式

$$x_i^2 - 2x_{i+1}^2 + x_{i+2}^2 = 2, \qquad i = 1,\ 2,\ \ldots,\ n-2$$

を満たすことと, 連立方程式

$$\pm x_1 = \pm x_2 - 1 = \pm x_3 - 2 = \cdots = \pm x_n - (n-1)$$

を満たすことが同値であるような n が存在する.

さらに Vojta は Lang 予想

予想 7 X を k 上の一般型非特異射影部分多様体とするとき, k を含む任意の数体 K に対して $X(K)\backslash Z(K)$ が有限集合となるような X の *proper Zariski-closed subset* Z が存在する.

が成り立てば予想 6 が正しいことを示した．このことを示す途中で定理 4 を示した．W_n と X_n は非特異 $(2,\ 2,\ \ldots,\ 2)$-完全交叉曲面で 2^n 本の trivial line があるなど共通する特徴をいくつも持っているので，関係付けることを考える．

定義 8 $\tilde{X}_n$ を次式で定義される多様体とする．

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \beta_0 & \beta_1 & \beta_2 & \beta_i \\ \beta_0^2 & \beta_1^2 & \beta_2^2 & \beta_i^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_i^2 \end{vmatrix} = 0, \qquad i = 3,\ 4,\ \ldots,\ n. \tag{6}$$

注．$\beta_i = \alpha_i^2$ とおくと $\tilde{X}_n$ から W_n が得られる．
次のことが成り立つことに注意しておく．

補題 9 m と n を整数で $m \leq n$ が成り立つものとする．$\mathbf{a}_0,\ \ldots,\ \mathbf{a}_n$ を m 項列ベクトルとし，どの m 個のベクトルも 1 次独立とする．このとき次の 3 つは同値である．

$$(i) \quad rank\begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{n-1} & \mathbf{a}_n \\ x_0 & x_1 & \cdots & x_{n-1} & x_n \end{pmatrix} = m,$$

$$(ii) \quad \begin{vmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \cdots & \mathbf{a}_{m-1} & \mathbf{a}_i \\ x_0 & x_1 & \cdots & x_{m-1} & x_i \end{vmatrix} = 0, \quad i = m,\ m+1,\ \ldots,\ n,$$

$$(iii) \quad \begin{vmatrix} \mathbf{a}_0 & \mathbf{a}_i & \mathbf{a}_{i+1} & \cdots & \mathbf{a}_{i+m-1} \\ x_0 & x_i & x_{i+1} & \cdots & x_{i+m-1} \end{vmatrix} = 0, \quad i = 1,\ 2,\ \ldots,\ n-m+1.$$

定理 10 $\tilde{X}_n$ において $\beta_0 = 0,\ \beta_i = 1/i,\ Y_0 = x_0,\ Y_i = x_i/i\ (i = 1,\ 2,\ \ldots,\ n)$ とおくと X_n である．

注意 11 これと同じ specialization で trivial line も (3) から (5) が得られる．

この関連付けができたことが，主結果を得るために最も重要な役割を果たしたので証明は簡単であるが，これを特に述べる．

証明. 行列 A を

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \cdots & \beta_n \\ \beta_0^2 & \beta_1^2 & \beta_2^2 & \beta_3^2 & \beta_4^2 & \cdots & \beta_n^2 \\ Y_0^2 & Y_1^2 & Y_2^2 & Y_3^2 & Y_4^2 & \cdots & Y_n^2 \end{pmatrix}$$

とおく. β_i を specialize するとき, $\beta_i \neq \beta_j$ $(i \neq j$ のとき) であるならば $\begin{pmatrix} 1 \\ \beta_i \\ \beta_i^2 \end{pmatrix}$ $(i = 0,\ 1,\ \ldots,\ n)$ はどの異なる 3 つのベクトルも 1 次独立である.
そこで$\beta_0 = 0,\ \beta_i = 1/i,\ Y_0 = x_0,\ Y_i = x_i/i$ $(i = 1,\ \ldots,\ n)$ とおくと, 補題 9 より, (6) は

$$rankA = 3$$

と同値であり

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1/2 & 1/3 & 1/4 & \cdots & 1/n \\ 0 & 1/1^2 & 1/2^2 & 1/3^2 & 1/4^2 & \cdots & 1/n^2 \\ x_0^2 & (x_1/1)^2 & (x_2/2)^2 & (x_3/3)^2 & (x_4/4)^2 & \cdots & (x_n/n)^2 \end{pmatrix}$$

である. ここで第 i 列に $(i-1)^2$ $(i = 2,\ \ldots,\ n+1)$ を掛けて, 第 1 行と第 3 行を入れ替えると A は

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 1^2 & 2^2 & 3^2 & 4^2 & \cdots & n^2 \\ x_0^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 & \cdots & x_n^2 \end{pmatrix}$$

となる. この行列を B とする. 再び補題 9 を用いると,

$$rank(B) = 3$$

$$\begin{vmatrix} 0 & 1 & 1 & 1 \\ 0 & i & i+1 & i+2 \\ 1 & i^2 & (i+1)^2 & (i+2)^2 \\ x_0^2 & x_i^2 & x_{i+1}^2 & x_{i+2}^2 \end{vmatrix} = 0, \qquad i = 1,\ 2,\ \ldots,\ n-2$$

と同値なのでこの行列式を第 4 行で展開すると (4) が得られる. □

よって W_n と X_n が関連付けられたので Vojta の結果である定理 4 の証明を W_n に用いることができるように拡張すると次が得られる.

定理 12 $n \geq 8$ のとき W_n の種数 0 または 1 の曲線は *trivial line* のみである.

次に W_n の点が与える楕円曲線に関する結果を述べる.

補題 13 $P = (Y_0,\ Y_1,\ \ldots,\ Y_n)$ を W_n 上の点で $Y_0 \neq 0$ であるとする. P によって与えられる楕円曲線 $E_{f(\alpha_0)}$ は

$$\tilde{E}_{f(\alpha_0)} : \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \end{vmatrix} y^2$$

$$= \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^4 - \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix} x^2 + \begin{vmatrix} \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 \\ Y_0^2 & Y_1^2 & Y_2^2 \end{vmatrix}$$

で定義される楕円曲線 $\tilde{E}_{f(\alpha_0)}$ と K 上同型である. またこの定義式は

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & x^2 \\ \alpha_0^4 & \alpha_1^4 & \alpha_2^4 & x^4 \\ Y_0^2 & Y_1^2 & Y_2^2 & y^2 \end{vmatrix} = 0$$

の行列式を第 4 列で展開したものである.

trivial line 上には K-有理点が無限個あるのでこれらがどのような楕円曲線を与えるかは問題である. しかし次のことが示される.

定理 14 W_n の *trivial line* の K-有理点から補題 13 のようにして作られる $\tilde{E}_{f(\alpha_0)}$ は有理曲線である.

一方 Lang 予想には次のものもある.

予想 15 k を有限生成体とし, X を k 上の一般型非特異射影部分多様体とするとき, k を含む任意の数体 K に対して $X(K)\backslash Z(K)$ が有限集合となるような X の *proper Zariski-closed subset* Z が存在する. (予想 *7* の k を有限生成体にしたもの)

この予想を仮定するとき, 次が成り立つ.

定理 16 n を 8 以上の整数とする. W_n に対し, 予想 *15* が成り立つものとする. このとき $y^2 = ax^4 + bx^2 + c$ $(a,\ b,\ c\ \in K)$ の形の K-上の楕円曲線で K-有理点の x-座標が α_i であるものは有限個しか存在しない. 特にこのような楕円曲線のランクは有界である.

このテーマにおいて特に述べたい点

- 今回取り上げたような楕円曲線は上に述べた捉え方をすることで W_n の K-有理点を調べればすべて分かる, という「入れ物」が作れることが面白いと思っています. 即ちこの入れ物に除外点ではないような良い有理点が存在すれば楕円曲線が構成できるし, そのような有理点が無い, ということが示せれば, このような性質を持つ楕円曲線は存在しない, ということを示すことができます. 実際, 今回の結果では Lang 予想が成り立てば楕円曲線が構成できない, という方向に用いていますが, 以前に得られた結果では E を $y^2 = ax^3 + bx^2 + cx + d$ としたときの (2) 式の楕円曲線の $k(V_\ell)$-有理点が generic に独立である, という結果 ([1]) を用いて n を 1 から 7 とするとき, ランクが少なくとも n である楕円曲線をすべて構成しています. ([5])

- 更に torsion part が指定された構造をもつもので, ランクの問題を考えるときなども今回考えた W_n に相当するものを考えることができます. これらははじめの内は有理的ですが, n を次第に大きくして有理点を調べるのが難しくなって来ると $K3$ 曲面や Kummer 曲面になっており, 楕円曲線の有理点の問題がこれらの曲面の有理点の問題に結びつく所が面白いと思っています.

- 今回述べた結果はかなりの計算を含んでいます. 時として計算を軽んじる批評を見かけることがありますが, 計算によって理論だけでは分からない所まで詳しく分かる時もあるので, 計算だから つまらない, ということも無いのでは無いかと思います. 例えば前項では Kummer 曲面が出てくる場合があると述べましたが, これは実は楕円曲線の直積に附随する Kummer 曲面で, ここに出てくる 2 つの楕円曲線の定義式は計算によって具体的に求められ, しかも求められた定義式によってはじめてこれらの楕円曲線がツイストになっていることや, どのような拡大体上で考えるとこれらが同型になるかもわかります. ([4])

最後に, 今回発表の機会を与えて下さいました伊原康隆先生, 御推薦下さいました硲文夫先生, 座長をして下さいました青木昇先生, そして沢山の質問を下さいました多くの方々, どうもありがとうございました. この場をお借りしてお礼申し上げます.

参考文献

[1] F. Hazama, Rational points on certain abelian varieties over function fields, *J. Number Theory* **50** (1995), no. 2, 278-285.

[2] S. Lang (ed.), "Number Theory III," Encyclopaedia of Mathematical Sciences vol. 60, Springer-Verlag, 1991.

[3] P. Vojta, Diagonal quadratic forms and Hilbert's tenth problem, *Contemp. Math.* **270** (2000), 261-274.

[4] H. Yamagishi, On the existence of families of elliptic curves of rank four with all two-torsion points, *Far East J. Math. Sci. (FJMS)* **3** (2001), no. 5, 803-823.

[5] H. Yamagishi, A unified method of construction of elliptic curves with high Mordell-Weil rank, *Pacific J. Math.* **191** (1999), 189-200.