

種数 2 の超楕円曲線のヤコビ多様体の有理等分点

大阪大学 理学部 小川 裕之 (Hiroyuki OGAWA)

1. 序

代数体上で定義されたアーベル多様体の Mordell-Weil 群は、有限生成アーベル群であることが知られている。多様体の次元と定義体を固定したとき、Mordell-Weil 群の free-part の rank に上限は存在するのか。また、torsion 部分群として、どのようなものが現れるのであろうか。Mazur は、楕円曲線 E/\mathbb{Q} の torsion 部分群に関する次の決定的な結果を与えた。

定理 1.1 (B.Mazur, [12])

$$E_{tors}(\mathbb{Q}) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & (n = 1, 2, 3, \dots, 9, 10, 12) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & (n = 2, 3, 4) \end{cases}$$

これを高次元アーベル多様体へ拡張できないであろうか。2次元に限っても、まだ決定的な結果は出ておらず、適当な位数の有理等分点を持つ例が知られているに過ぎない。例えば、 $\mathbb{Q}(t)$ 上で、有理 11 等分点を持つもの (E.V.Flynn [6])、有理 13, 15, 17, 19, 21 等分点を持つもの (F.Leprévost [10], [11])、有理 23 等分点を持つもの (O-. [16])、が構成され、 t の \mathbb{Q} への特殊化により互いに同型でないものが \mathbb{Q} 上でそれぞれ無限個得られている。

2次元アーベル多様体は、ある種数 2 の超楕円曲線のヤコビ多様体に同型である。D.Grant [8] は、標数が 2 と異なる体 k 上で定義された種数 2 の超楕円曲線 C のヤコビ多様体 $J(C)$ の射影空間への埋め込みを与え、

定理 1.2 (D.Grant, [8])

$$\exists J(C) \hookrightarrow \mathbb{P}^8$$

加法公式をその射影空間の座標を用いて書き下した。ところが、 \mathbb{P}^8 において $J(C)$ は 13 個もの方程式で定義され、加法公式は複雑な式で与えられる。 $J(C)$ の 2 等分点ぐらひは計算できても、3 以上の等分点の計算のためには有用な形には思えない。また、E.V.Flynn [5]

は Grant とは独立に、 $J(C)$ の P^{15} への埋め込みを与えたが、Grant のものより更に複雑なものになっている。

ここでは、ヤコビ多様体の多様体としての構造よりも、アーベル群としての構造に注目するので、ヤコビ多様体を単に次数 0 の因子類群と捉える古典的な手法をとる。一部は Abel 以来既に知られていたことではあるが、ヤコビ多様体 (因子類群) 上での点 (因子群) の位数と、適当な関数の連分数の周期との関係が得られた。特に種数が 1 と 2 の場合には、ヤコビ多様体の全ての点が扱われる。また、Grant、Flynn のものでは見え難かった 3 等分点を容易に計算することが出来た。なおこれらは、山本芳彦氏 (阪大理) との共同研究である。

2. Continued Fractions and Orders on Jacobians.

k を代数閉体、 C/k を完備非特異代数曲線とするとき、次の完全列が知られている。

$$1 \longrightarrow k^\times \longrightarrow k(C)^\times \longrightarrow \text{Div}^0(C) \longrightarrow J(C) \longrightarrow 0$$

ここで、 $\text{Div}^0(C)$ は次数 0 の因子群、 $J(C) = \text{Div}^0(C)/\sim$ は次数 0 の因子類群 (以下、これをヤコビ多様体と呼ぶ)。この完全列と、代数体 K における基本的な完全列、

$$1 \longrightarrow (\text{単数群}) \longrightarrow K^\times \longrightarrow (\text{分数イデアル}) \longrightarrow (\text{イデアル類群}) \longrightarrow 1$$

の類似から、ヤコビ多様体とイデアル類群との類似が見えてくる。また、超楕円曲線は、その関数体が 1 変数有理関数体の 2 次拡大であることで特徴付けられる。つまり、超楕円曲線と 2 次体とが対応する。(多少大雑把ではあるが) これらの関係を通して、実 2 次体の整数論で大きな役割を担う "連分数の理論" の類似物を、超楕円曲線のヤコビ多様体 (因子類群) の上に構成することが可能であると思われる。

実際、Abel は、超楕円積分の研究 ([2]) の中で、次のことを示した。「 $C : y^2 = f(x)$ (ただし、 f は $2g + 2$ 次、重解を持たない) を超楕円曲線、 ∞, ∞' を C の異なる 2 つの無限遠点とするとき、 $\infty - \infty'$ の代表する類 $\overline{\infty - \infty'}$ が有限位数である必要十分条件は、 $\sqrt{f(x)}$ の $x = \infty$ における連分数 (定義は 2.3 で述べる) が周期的であることである」。この連分数のヤコビ多様体における役割は、Abel の研究に始まり E. Artin ([1]) 他、多くの人々による詳細な研究がある。ところが、関数の連分数の定義による制約のため、彼らの研究では $\overline{P - P'}$ で表されるヤコビ多様体の点しか扱われていなかった。

我々 ([15]) は、Abel 等のものも含めて、3 通りの連分数を定義し、それぞれ異なるタイプのヤコビ多様体の点との対応を与えた。その結果、種数が 1 と 2 の場合には、ヤコビ多様体のすべての点を、連分数の観点から扱うようになった。本報告では、その概略を記し、計算例と、種数 2 への簡単な応用を述べる。冗長になるので証明は [15] に譲る。

2.1. k を標数が 2 と異なる体、 $C : y^2 = f(x)$ を種数 g の超楕円曲線とする。ただし、 f は $2g + 1$ 次、重解を持たないとする。 C は、唯一の無限遠点を持ち、これを、 ∞ と書く。 $P = (x, y) \in C$ に対して、 $P' = (x, -y)$ とおく。以下、不分岐な ($P \neq P'$) C の点 P を固定する。関数体 $k(C) = k(x, y)$ の P での正規付値を ν_P で表す。 P での局所変数 $t_P = x - x(P)$ を用いて、任意の関数 $h \in k(C) = k(x, y)$ は、 P において次のように Laurent 展開される。

$$h = a_{-e} \frac{1}{t_P^e} + \cdots + a_{-1} \frac{1}{t_P} + a_0 + a_1 t_P + \cdots$$

この Laurent 展開の主要部と定数項をとり、

$$[h] = [h]_P := a_{-e} \frac{1}{t_P^e} + \cdots + a_{-1} \frac{1}{t_P} + a_0$$

と定義する。このとき、定義より、

$$h \equiv [h] \pmod{t_P k[[t_P]]} \quad \text{at } P$$

2.2. 次で帰納的に定義される関数列 $\{h_n\}_{n \geq 0}$ を $h = h_0$ の P における連分数と呼ぶ。

$$h_n = [h_n] + \frac{t_P}{h_{n+1}} \quad (n \geq 0)$$

このとき、 h は、

$$h = [h_0] + \frac{t_P}{[h_1] + \frac{t_P}{[h_2] + \cdots + \frac{t_P}{[h_{n-1}] + \frac{t_P}{h_n}}}}$$

と連分数に展開される。 h_{n_0+l}/h_{n_0} が定数関数となる $l > 0$ 、 $n_0 \geq 0$ が存在するとき、 $\{h_n\}$ は周期を持つと言い、これを満たす最小の l をその周期と呼ぶ。特に初項から循環するときは、純周期を持つと言う。この連分数と、ヤコビ多様体の点 $\overline{P - \infty}$ との間に、次の関係が成り立つ。

定理 2.1 $\overline{P - \infty}$ の位数が有限である必要十分条件は、 y/t_P^g の P での連分数 $\{y_n\}$ が周期を持つことである。更にその位数は、

$$l - 2 \sum_{n=1}^{\ell} \nu_P(y_n)$$

である。ただし、 l は周期とする。

(この定理の主張には、 $\{y_1, y_2, \dots, y_\ell\}$ が $\{y_n\}$ の 1 周期であることを含む。)

2.3. 次で帰納的に定義される関数列 $\{h_n\}_{n \geq 0}$ を $h = h_0$ の $2P$ における連分数と呼ぶ。

$$h_n = [h_n] + \frac{1}{h_{n+1}} \quad (n \geq 0)$$

このとき、 h は、

$$h = [h_0] + \frac{1}{[h_1] + \frac{1}{[h_2] + \dots + \frac{1}{[h_{n-1}] + \frac{1}{h_n}}}}$$

と連分数に展開される。Abel はこの連分数を用い、ヤコビ多様体の点 $\overline{P - P'} (= 2\overline{P} - \infty)$ との関係を示した。

定理 2.2 (N.H.Abel. [2]) $g' = [g/2]$ (Gauss 記号) とおく。 $\overline{P - P'}$ の位数が有限である必要十分条件は、 $y/t_P^{2g'+1}$ の $2P$ での連分数 $\{y_n\}$ が周期を持つことである。更にその位数は、

$$-\sum_{n=1}^{\ell} \nu_P(y_n)$$

である。ただし、 ℓ は周期とする。

(この定理の主張には、 $\{y_1, y_2, \dots, y_\ell\}$ が $\{y_n\}$ の 1 周期であることを含む。)

2.4. あと一つ連分数を定義する。 P と x -座標の異なる不分岐な点 $Q \in C$ をとり、

$$[h]_{P+Q} := t_P \left[\frac{h}{t_P} \right]_Q + t_Q \left[\frac{h}{t_Q} \right]_P$$

と定める。このとき、次が成立する。

補題 1

$$\begin{aligned} h &\equiv [h]_{P+Q} \pmod{t_P k[[t_P]]} && \text{at } P \\ h &\equiv [h]_{P+Q} \pmod{t_Q k[[t_Q]]} && \text{at } Q \end{aligned}$$

次で帰納的に定義される関数列 $\{h_n\}_{n \geq 0}$ を $h = h_0$ の $P + Q$ における連分数と呼ぶ。

$$\frac{h_n}{\psi_n} = \left[\frac{h_n}{\psi_n} \right]_{P+Q} + \frac{t_P t_Q}{h_{n+1}} \quad (n \geq 0)$$

ただし、

$$\psi_n := \left(\frac{t_P}{t_Q} \right)^{\nu_P(h) - \nu_Q(h)}$$

このとき、 h は、

$$h = \psi_0 \left[\frac{h_0}{\psi_0} \right]_{P+Q} + \frac{t_P t_Q \psi_0}{\psi_1 \left[\frac{h_1}{\psi_1} \right]_{P+Q} + \frac{t_P t_Q \psi_1}{\psi_2 \left[\frac{h_2}{\psi_2} \right]_{P+Q} + \dots + \frac{t_P t_Q \psi_{n-2}}{\psi_{n-1} \left[\frac{h_{n-1}}{\psi_{n-1}} \right]_{P+Q} + \frac{t_P t_Q \psi_{n-1}}{h_n}}$$

と連分数に展開される。この連分数は、ヤコビ多様体の点 $\overline{P-Q}$ ($= \overline{P+Q-2\infty}$) と、次のような関係を持つ。

定理 2.3 $\overline{P-Q}$ の位数が有限である必要十分条件は、 $y/t_P^{g'} t_Q^{g'}$ の $P+Q$ での連分数 $\{y_n\}$ が周期を持つことである。更にその位数は、

$$l - \sum_{n=1}^l (\nu_P(y_n) + \nu_Q(y_n))$$

である。ただし、 l は周期とする。

(この定理の主張には、 $\{y_1, y_2, \dots, y_l\}$ が $\{y_n\}$ の 1 周期であることを含む。)

2.5. 注意. 種数が 2 とする。このとき、Riemann-Roch の定理より、ヤコビ多様体の任意の点は、 C の適当な 2 点 P, Q を用いて、 $\overline{P+Q-2\infty} = \overline{P-Q}$ と書ける。先に述べたように、連分数の手法は、ヤコビ多様体の任意の点に適用される。

2.6. 上の 3 つの定理より、2 次元アーベル多様体の有理 3 等分点に関して、次の結果を得る。さらに、2 次元アーベル多様体の 3 等分方程式を求めることが出来る。(3 等分方程式の具体的な形は非常に繁雑なので、省略する。)

定理 2.4 k を標数が 2 と異なる体、 $J(C)$ を種数 2 の超楕円曲線 $C/k: y^2 = f(x)$ のヤコビ多様体で、位数 3 の有理点 $\overline{P-Q}$ を持つとする。 $k' = k(x(P))$ とするとき、

(I) $P=Q$ のとき、 $f(x) = ct_P^6 + A(t_P)^2$

(ただし、 $c \in k$ 、 A は高々 3 次の k -係数の多項式で、 $A(0) = y(P)$)

(II) $P \neq Q$ のとき、 $f(x) = ct_P^3 t_Q^3 + (A(t_P) t_Q^2 + B(t_Q) t_P^2)^2$

(ただし、 $c \in k$ 、 A, B は高々 1 次の k' -係数の多項式で、 $A(0) = y(P)$ 、 $B(0) = y(Q)$)

2.7. 例 1. $k = \mathbf{Q}$ 、 $C : y^2 = 1 + 4x + 6x^2 + 4x^3$ ($j(C) = 1728$)、 $P = (0, 1)$ とおく。 P での局所変数 $t_p = x$ による Laurent 展開を用いて、 y/t_p (C の種数は 1) の P での連分数 $\{y_n\}$ は、次のように計算される。

$$\begin{aligned} y_0 &= \frac{y}{x} = \frac{1}{x} + 2 + x + \cdots & [y_0] &= \frac{1}{x} + 2 \\ y_1 &= \frac{x}{y_0 - [y_0]} = \frac{x^2}{y - 1 - 2x} = \frac{x^2(y + 1 + 2x)}{y^2 - (1 + 2x)^2} = \frac{y + 1 + 2x}{2(1 + 2x)} \\ [y_1] &= \frac{1 + 1 + 0}{2(1 + 0)} = 1 \\ y_2 &= \frac{y + 1 + 2x}{x} & [y_2] &= \frac{2}{x} + 4 \\ y_3 &= \frac{y + 1 + 2x}{2(1 + 2x)} = y_1 \end{aligned}$$

定理 2.1 より、 $\overline{P - \infty}$ の位数は $2 - 2 \times (0 - 1) = 4$ である。

2.8. 例 2. $k = \mathbf{Q}$ 、 $C : y^2 = 1 - 4x^2 + 4x^3$ ($\text{cond}(C) = 11$)、 $P = (0, 1)$ とおく。 P での局所変数 $t_p = x$ による Laurent 展開を用いて、 y/t_p (C の種数は 1) の $2P$ での連分数 $\{y_n\}$ は、次のようになる。

$$\begin{aligned} y_1 &= \frac{y - 1}{4x(-1 + x)} & y_2 &= -\frac{y - 1 + 2x^2}{x^2} & y_3 &= \frac{y - 1 + 2x^2}{4x(-1 + x)} \\ y_4 &= \frac{y - 1}{x} & y_5 &= \frac{y - 1}{4x(-1 + x)} = y_1 \end{aligned}$$

定理 2.2 より、 $\overline{P - P'}$ の位数は $1 + 2 + 1 + 1 = 5$ である。

2.9. 例 3. $k = \mathbf{Q}$ 、 $C : y^2 = 1 + x(x - 1)(x + 1)$ 、 $P = (0, 1)$ 、 $Q = (1, 1)$ とおく。関数 y の $P + Q$ における連分数 $\{y_n\}$ を計算する。

$$\begin{aligned} y_1 &= \frac{y + 1}{1 + x} & y_2 &= \frac{y + 1 + x - x^2}{3 - x} \\ y_3 &= -9 \frac{y + 1 - 2/3x + 2/3x^2}{1 - 4x} & y_4 &= \frac{y + 1 - 10x + 10x^2}{9(19 - 25x)} \\ & \dots \end{aligned}$$

と、順に y_{12} まで計算したところ y_1 に定数倍を除いて等しい項は現れない。この連分数が周期を持ったとしても、それは 12 より大きい。定理 2.3 より、 $\overline{P - Q'}$ の位数が有限ならば、その位数は 12 より大きくなければならない。ところが、Mazur の定理 (1.1) より、 \mathbf{Q} -有理等分点の位数は 12 を越えないから、 $\overline{P - Q'}$ は等分点ではない。

2.10. 例 4. $k = \mathbf{Q}$ 、 $C : y^2 = 1 - 50x + 1849x^2 - 30600x^3 + 146448x^4 + 912384x^5$ 、 $P = (0, 1)$ とおく。定理 2.1 に従って、 $\overline{P - \infty}$ の位数を計算する。 y/x^2 の P での連分数

$\{y_n\}$ は、次のようになる。

$$\begin{aligned} y_1 &= \frac{y+1-25x+612x^2}{-228096x(1-4x)} & y_2 &= \frac{108(y+1-25x-444x^2)}{-1+21x+108x^2} \\ y_3 &= \frac{y+1-17x+228x^2}{1728-82944x+912384x^2} & y_4 &= \frac{16(y+1-79x+828x^2)}{1-8x+16x^2} \\ &\dots\dots & & \\ y_{15} &= \frac{y+1-25x+612x^2}{912384x^2} & y_{16} &= \frac{4(y+1-25x+612x^2)}{-x(1-4x)} = 912384y_1 \end{aligned}$$

$\{y_n\}$ は周期 16 を持つので、 $\overline{P-\infty}$ は $J(C)$ の \mathbf{Q} -有理等分点である。また、

$$\nu_P(y_1) = \nu_P(y_{14}) = -1, \quad \nu_P(y_{15}) = -2, \quad \nu_P(y_2) = \dots = \nu_P(y_{13}) = 0$$

より、 $\overline{P-\infty}$ の位数は、 $15 - 2(-1 - 1 - 2) = 23$ である。(参考、O-. [16])

2.11. 例 5. $k = \mathbf{Q}(t)$ 、

$$\begin{aligned} C/k : y^2 &= (t(1+x)(1-x)^2 + (4t - (\frac{4t}{3} + \frac{3}{4t})x)x^2)^2 + 2x^3(1-x)^3 \\ &= (t(1-3x)(1+x)^2 + (8t + (\frac{8t}{3} + \frac{3}{4t})x)x^2)^2 - x^3(1+x)^3 \end{aligned}$$

とおく。 $P_0 = (0, t)$ 、 $P_1 = (1, \frac{8t}{3} - \frac{3}{4t})$ 、 $P_{-1} = (-1, \frac{16t}{3} - \frac{3}{4t})$ とするとき、定理 2.4 より、 $\overline{P_1 - P'_0}$ 、 $\overline{P_{-1} - P'_0}$ は、位数 3 の $\mathbf{Q}(t)$ -有理点である。さらに、 $\overline{P_1 - P'_0} \neq \pm \overline{P_{-1} - P'_0}$ だから、 $J(C)(\mathbf{Q}(t))$ の 3-part の rank は、2 以上である。

References

- [1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, in "The Collected Papers of Emil Artin", pp. 1-94, Addison-Wesley, Reading, MA, 1965.
- [2] N. H. Abel, *Sur l'intégration de la formule différentielle $\rho dx/\sqrt{R}$, R and ρ étant des fonctions entières*, J. Reine Angew. Math., 1, (1826), pp.185-221
- [3] J. W. S. Casselles, *Arithmetic of curves of genus 2*, in "Number Theory and Applications", Proceedings of a NATO conference in Banff, 1988, ed. R. A. Mollin, D. Reidel Publishing Co.
- [4] J. W. S. Casselles, *The Mordell-Weil group of curves of genus 2*, in "Arithmetic and Geometry Papers Dedicated to I. R. Shafarevich on Occasion of this Sixtieth Birthday" Vol.1. Arithmetic, Prog. in Math. 35, Birkhäuser, Boston, 1983

- [5] E. V. Flynn, *The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Camb. Phil. Soc. (1990), 107, pp.425-441
- [6] E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number T. 36, (1990), pp. 257-265
- [7] R. Fricke, "Lehrbuch der Algebra, Volume III", F. Vieweg & Sohn, Braunschweig, 1928
- [8] D. Grant, *Formal groups in genus 2*, J.reine angew. Math., 411, (1990), pp. 96-121
- [9] J. Igusa, *Arithmetic variety of moduli for curves of genus 2*, Ann. of Math., 72, (1960), pp. 612-649
- [10] F. Leprévost, *Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13*, C. R. Acad. Sci. Paris, t. 313, Série I, (1991), pp. 451-454
- [11] F. Leprévost, *Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15,17,19 ou 21*, C. R. Acad. Sci. Paris, t. 313, Série I, (1991), pp. 771-774
- [12] B. Mazur, *Rational points of modular curves*, in "Modular Functions of One Variable, V", pp. 107-148, Lecture Notes in Mathematics, Vol. 601, Springer-Verlag, Berlin/New York, 1977
- [13] J.-P. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, in "Effective Methods in Algebraic Geometry", Progress in Math., 94, Birkhäuser, 1991
- [14] D. Mumford, "Curves and Their Jacobians", University of Michigan Press, Ann Arbor, 1975
- [15] H. Ogawa-Y. Yamamoto, *Continued fractions and orders on jacobians*, preprint
- [16] H. Ogawa, *Curves of genus 2 with a rational divisor class of order 23*, preprint
- [17] J. H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, Berlin/New York, 1986