楕円曲線上の通常高さ関数と標準高さ関数の差の評価とその応用について

京都大学大学院　理学研究科　数学・数理解析専攻
修士２回
学籍番号:0530-29-1950
橘由佑子

2019 年 1 月 24 日

目次

1　はじめに

この論文では，通常高さ関数と標準高さ関数の差の評価について論じている論文をいくつか紹介し，その後にそれを応用している例を紹介しようと思う．E を数体 K 上の楕円曲線とする．楕円曲線 E の高さ関数とは，Mordell-Weil 群 $E(K)$ 上の実数値関数である．楕円曲線 E の高さ関数には主に通常高さ関数と標準高さ関数がある．通常高さ関数は $E(K)$ の点の座標などを使い定義されており，よって実際に値を計算することができる．しかし，例えば中線定理において明示的に表すことのできない端数が出るなど論理面において扱いにくい側面がある．標準高さ関数は通常高さ関数の極限を使い定義されるため，実際に値を計算することは難しい．しかし通常高さ関数での理論的な扱いにくさが消えて，二次形式となる．よって，通常高さ関数と標準高さ関数の差の評価を得たり，さらに標準高さ関数の値の評価を得ることで，両者の利点を生かして楕円曲線の性質を調べることができる．例えば [4, 7 章] では，通常高さ関数と標準高さ関数の差の評価と標準高さ関数の近似値を使うことで $E(K)$ の生成元となり得る点の座標を絞り込んでいる．また，[8, Theorem1.3] では標準高さ関数の上下の評価と，$\hat{h}$ について $\hat{h}(mP) = m^2\hat{h}(P), (P \in E(\bar{K}), m \in \mathbb{Z})$ が成り立つことを使い，楕円曲線の quadratic twist 上のある有理点が原始的となる条件を与えている．

内田の [1] の論文では，以下の様に通常高さ関数と標準高さ関数の差の評価を与えている．

定理 1.1 (内田の主定理)**.**

$$S_v(m) = \frac{\log \delta_{m,v}}{m^2-1}, \quad T_v(m) = \frac{\log \epsilon_{m,v}}{m^2-1},$$

とおく．ただし $\delta_{m,v}, \epsilon_{m,v}$ を以下で定める．ϕ_m, ψ_m^2 を等分多項式，$v \in \mathrm{M}_K$ と正整数 m に対し，関数 $\Phi_{m,v} : E(K_v) \to \mathbb{R}$ を

$$\Phi_{m,v}(P) = \begin{cases} 1 & (P = O), \\ \dfrac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}} & (P \neq O), \end{cases}$$

と定め，

$$\epsilon_{m,v}^{-1} = \inf_{P \in E(K_v)} \Phi_{m,v}(P), \quad \delta_{m,v}^{-1} = \sup_{P \in E(K_v)} \Phi_{m,v}(P),$$

とおく．また，α_v を E の $v \in \mathrm{M}_K^0$ における小平型と玉河数 c_v によって定まる定数，q_v

を v における K の剰余体 k_v の元の個数とする．このとき任意の $P \in E(K)$ に対して

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^{\infty}} n_v S_v(m) \leqq h(P) - \hat{h}(P)$$
$$\leqq \frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^{\infty}} n_v\, T_v(m) + \frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^{0}} \left(\alpha_v + \frac{1}{6}\mathrm{ord}_v\left(\frac{\Delta}{\Delta_v^{\min}}\right)\right)\log q_v,$$

が成り立つ．

通常高さ関数と標準高さ関数の差を評価する際，標準高さ関数を K 上の素点 v ごとに局所高さ関数の和で表すことで評価を進めていく．このとき，v が非アルキメデス的な素点の場合はすでにその上限・下限が知られている ([6, Proposition8])．よって，v がアルキメデス的な素点である時にいかに良い評価を得るかということと，いかに速く評価を計算できるかということが重要となってくる．

この内田の論文での方法は J．E．Cremona，M．Prickett，S．Siksek の [6] をもとにしたものであり，理論上，アルキメデス的な素点での通常高さ関数と標準高さ関数の差の評価をその上限・下限に限りなく近づける事ができるものである．

アルキメデス的な素点での評価において内田のものより良い評価を出しているものでは，例えば以下の Múller，Corinna Stumpe の [10] での方法がある．

定理 1.2 (Múller，CorinnaStumpe **の主定理)．** $T_1, T_2, T_3 \in E$ を自明でない互いに異なる 2 捩れ点とする．まず，$i = 1, 2, 3$ に対し $a_{1,i}, a_{2,i}, b_{i,1}, b_{i,2}$ をそれぞれ

$$a_{1,i} = \frac{2x(T_j)x(T_k) - \frac{b_4}{2}}{2(x(T_i) - x(T_j))(x(T_i) - x(T_k))}, \quad a_{2,i} = \frac{-1}{2(x(T_i) - x(T_j))(x(T_i) - x(T_k))},$$
$$b_{i,1} = 1, \quad b_{i,2} = -x(T_i),$$

とする．ただし $j, k \in \{1, 2, 3\}, i, j, k$ は互いに異なる．$\varphi : \mathbb{R}^2_{\geqq 0} \to \mathbb{R}^2_{\geqq 0}$ を

$$(d_1, d_2) \mapsto (\varphi_1(d_1, d_2), \varphi_2(d_1, d_2)),$$
$$= \left(\sqrt{\sum_{j=1}^{3} |a_{1,j}|\sqrt{|b_{j,1}|d_1 + |b_{j,2}|d_2}}, \sqrt{\sum_{j=1}^{3} |a_{2,j}|\sqrt{|b_{j,1}|d_1 + |b_{j,2}|d_2}}\right),$$

で定める．$\|\cdot\|$ を，K 上の 2 次元ベクトル (x_1, x_2) に対し $\|(x_1, x_2)\| = \max\{|x_1|, |x_2|\}$ で定義して，

$$c_N := \frac{4^N}{4^N - 1}\log(\|\varphi^{\circ N}(1, 1)\|)$$

とおく．ただし $\varphi^{\circ N}(1,1)$ は $(1,1)$ を φ で N 回写したものである．

このとき，$\{c_N\}_{N\geqq 1}$ は単調減少列で，任意の $N \geqq 1$ に対し

$$\max_{P\in E(\mathbb{C})}\{\Psi_v(P)\} \leqq c_N,$$

が成り立つ．

この評価は以前のものよりも良い評価が得られるだけでなく，最初に $a_{i,j}, b_{j,k}$ の計算などの下準備が済めば後は比較的簡単に c_N が求められるので，評価の計算が速いという利点がある．

この論文ではまず 2 章で楕円曲線と高さ関数の基礎的な内容を紹介し，次に 3 章で内田の論文 [1] を紹介した後，3.7 節で J．S．Müller，Corinna Stumpe の論文 [10] について少し紹介する．その後，4.1 節，4.2 節ではそれぞれ前述した，標準高さ関数の下の評価を使用した例 [8, Theorem3]，通常高さ関数と標準高さ関数の差の評価を使用した例 [4, 7 章] をそれぞれ紹介しようと思う．

謝辞

本論文を書くにあたり，ご多忙の中ご指導いただいた雪江明彦先生に深く感謝致します．

2　楕円曲線と高さ関数

記号を定義しつつ楕円曲線などについて少し紹介する．詳細は [2]，[3] を参照せよ．

以下，特に断らない限り K を数体，$\mathcal{O}_K$ をその整数環，M_K，M_K^0，M_K^∞ をそれぞれ K の素点全体からなる集合，有限素点全体からなる集合，無限素点全体からなる集合とする．v を K の素点としたとき K_v を K の v における完備化，$\mathrm{n}_v = [K_v : \mathbb{Q}_v]$ を局所次数，$|\cdot|_v$ を v に関する標準的な絶対値，$v(x) = -\log|x|_v$ とする．

また $v \in \mathrm{M}_K^0$ の場合，k_v を v における K の剰余体，q_v を k_v の元の個数とする．

2.1　楕円曲線の基本

まず射影多様体の関数体と射影多様体間の有理写像について定義しておく．アフィン多様体，射影多様体，その関数体，有理写像についての詳細は [2, 1 章] を見よ．$K[X] = K[X_1, \cdots, X_n]$ を K 上の n 変数多項式環として，射影空間 $\mathbb{P}^n(\bar{K}), \mathbb{P}^n(K)$ の射影多様体について考える．V をアフィン多様体とすると，定義より V のイデア

ル $I(V) \in \bar{K}[X]$ は素イデアルとなる．特に，K 上の多様体 V について，イデアル $I(V/K) = \{f \in K[X] |$ 任意の $P \in V$ について $f(P) = 0\}$ は $K[X]$ の素イデアルとなる．

定義 2.1. V/K のアフィン座標環 $K[V]$ を $K[V] = K[X]/I(V/K)$ で定義する．このとき $K[V]$ は整域となる．$K[V]$ の商体を V/K の関数体といい，$K(V)$ で表す．$\bar{K}[V]$, $\bar{K}(V)$ も，K を $\bar{K}$ に置き換えることで同様に定義する．

任意の $f \in \bar{K}[V]$ に対し，well-defined な関数 $f : V \ni P \mapsto f(P) \in \bar{K}$ が導かれる事に注意せよ．

V を射影多様体とすると，[2, 1 章§ 2] での議論より，ある $i \in \{0, \cdots, n\}$ について集合と包含写像

$$U_i = \{P = [x_0, \cdots, x_n] \in \mathbb{P}^n : x_i \neq 0\},$$
$$\phi_i : \mathbb{A}^n \ni (y_1, \cdots, y_n) \mapsto [y_1, \cdots, y_{i-1}, 1, y_{i+1}, \cdots, y_n] \in \mathbb{P}^n,$$

で $\phi_i^{-1}(V \cap U_i) \neq \emptyset$ となるものが存在する．このとき $\phi_i^{-1}(V \cap U_i)$ はアフィン多様体となる．

定義 2.2. 射影多様体 V/K の関数体 $K(V)$ とは $\phi_i^{-1}(V \cap U_i)$ の関数体のことをいう．$\bar{K}(V)$ についても同様に定義する．

定義 2.3. V_1, V_2 を射影多様体とする．V_1 から V_2 への有理写像とは，写像

$$\phi : V_1 \to V_2, \phi = [f_0, \cdots, f_n],$$

である．ただし $f_i \in \bar{K}(V_1)$ で，$P \in V_1$ に対し $f(P) = [f_0(P), \cdots, f_n(P)] \in V_2$ となる点で定義されるものをいう．

定義 2.4. V_1, V_2 を射影多様体とする．有理写像 $\phi = [f_0, \cdots, f_n] : V_1 \to V_2$ が点 $P \in V_1$ で正則とは，ある関数 $g \in \bar{K}(V_1)$ で，以下を満たすものが存在する時のことをいう．

(i) それぞれの gf_i が P で正則．

(ii) ある i が存在し，$(gf_i)(P) \neq 0$.

また，全ての点で正則な有理写像を射という．

次に Weierstrass 方程式により与えられる曲線 E の性質を見ていく．Weierstrass 方程式により与えられる曲線の性質の詳細については [2, 3 章] を見よ．ただし，ここでの曲線とは 1 次元射影多様体のことを指す．

定義 2.5. K を完全体，$\bar{K}$ を K のある代数閉包とする．射影空間 $\mathbb{P}^2(K)$ 上の斉次方程式

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$
$$a_1, \cdots, a_6 \in \bar{K},$$

を Weierstrass 方程式といい，$O = [0,\ 1,\ 0]$ をその基点という．

$\mathrm{char}(K) = 2,\ 3$ の場合は別に証明が必要だが，そうでない場合は変数変換により Weierstrass 方程式を簡単な形にすることができる．この方程式の係数や方程式の微分から，判別式，j-不変量，不変微分を定義する．

定義 2.6. E を上の Weierstrass 方程式により与えられる曲線とする．このとき判別式 Δ，j-不変量 j，不変微分 ω を

$$b_2 = {a_1}^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = {a_3}^2 + 4a_6,$$
$$b_8 = {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2,$$
$$c_4 = {b_2}^2 - 24b_4, \quad c_6 = -{b_2}^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -{b_2}^2b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6, \quad j = {c_4}^3/\Delta,$$
$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

で定義する．

[2, 3 章 Proposition1.4] より判別式によりその曲線が滑らかかどうかがわかる．

なめらかでない Weierstrass 方程式で表わされる曲線について考える．$P = (x_0, y_0)$ を次の方程式

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

の零点で，$f(x, y) = 0$ の特異点であるものとする．このとき $f(x, y)$ の P でのテイラー展開より

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3,$$

と表わすことができる．これにより次を定義する．

定義 2.7. 上の状況で，$\alpha \neq \beta$ の時，特異点 P をノード，$\alpha = \beta$ の時，特異点 P をカスプという．

定義 2.8. 楕円曲線とは種数 1 のなめらかな曲線 E とその基点 $O \in E$ の対 (E, O) のことをいう．

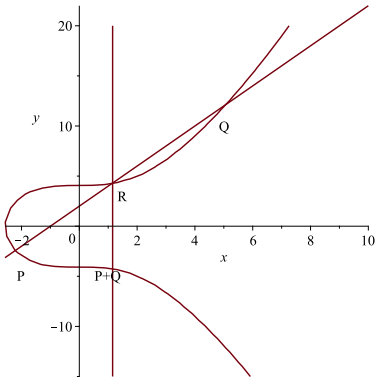
楕円曲線 (E,O) に対し，定義 2.5 で定義した $\mathbb{P}^2$ 上の Weierstrass 方程式で与えられる楕円曲線で (E,O) と同型となるものが存在する．[2, Exercise2.7] を使うことにより，なめらかな Weierstrass 方程式で与えられる曲線 E は種数 1 になるので，特に次が成り立つ．

命題 2.9. Weierstrass 方程式で与えられているなめらかな曲線で，基点 $O=[0,1,0]$ を持つものは楕円曲線である．

楕円曲線と直線が交わる時，重複を含め 3 点で交わることを利用し，楕円曲線の点集合に群の演算を定めることができる．

定義 2.10. E を楕円曲線，$P,Q\in E$ とする．L を P，Q で E と交わる直線（$P=Q$ のときは P で E に接する直線），R を L と E の 3 つ目の交点とする．L' を R，O と交わる直線とする．L' と E の 3 つ目の交点を $P\oplus Q$ として，E に群の演算を定義する．

この $\oplus$ により，E は O を単位元とするアーベル群となり自然に $\mathbb{Z}$ 加群となる．さらにこの演算を，点の座標と Weierstrass 方程式の係数で明示的に表すことができる ([2, 3 章 Group Law Algorithm2.3])．以下 $\oplus$ を $+$，P の $+$ に関する逆元を $-P$，$m\geqq 0$ のとき P を m 回足したものと $m<0$ のとき $-P$ を $-m$ 回足したものを $[m]P=mP$ で表記する．



定理 2.11. $P_0=(x_0,y_0)\in E$ とすると，

$$-P_0=(x_0,-y_0-a_1x_0-a_3),$$

となる．次に，

$$P_i=(x_i,y_i)\in E,\quad i=1,2,3,\quad P_1+P_2=P_3,$$

とする．このとき，もし $x_1=x_2$ かつ $y_1+y_2+a_1x_2+a_3=0$ ならば

$$P_1+P_2=O.$$

そうでなければ，λ，ν を以下で定義する．

このとき，$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2$，$y_3=-(\lambda+a_1)x_3-\nu-a_3$ と表わされる．

これにより，E が K 上定義されている場合は $E(K)$ が E の部分群となることがわかる．

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$	$\dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$

楕円曲線は特異点を持たない Weierstrass 方程式で与えられているが，特異点を持つ Weierstrass 方程式で与えられる曲線も，その非特異点の集合がアーベル群となっている ([2, 3 章§ 2　Singular Weierstrass Equations，特に Proposition2.5])．

楕円曲線の同型について，特に以下が [2, 3 章 Proposition3.1] で示される．

命題 2.12. $\mathbb{P}^2$ 上の Weierstrass 方程式で表される楕円曲線 E_1, E_2 が楕円曲線 (E, O) と同型とすると，変数変換

$$X = u^2 X' + r, \quad Y = u^3 Y' + s u^2 X' + t, \quad u \in K^*,\ r, s, t \in K,$$

で移りあうものとなる．また，逆に $\mathbb{P}^2$ 上のなめらかな Weierstrass 方程式で与えられる曲線は，基点を $[0, 1, 0]$ に持つ楕円曲線となる．

楕円曲線 E と $m \in \mathbb{Z}$ について，E の m 捩れ部分群を

$$E[m] = \{P \in E | [m]P = O\},$$

で定義する．このとき以下が成り立つ．証明は [2, 3 章 Corollary6.4] を見よ．

系 2.13. E を楕円曲線，$m \in \mathbb{Z} \setminus \{0\}$ とする．
(a) $\mathrm{char}(K) = 0$ 又は $0 < p = \mathrm{char}(K)$ が m を割り切らないとする．このとき

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

が成り立つ．
(b) $0 < p = \mathrm{char}(K)$，任意の $e = 1, 2, 3, \cdots$ のとき，次のうち一つが成り立つ．

$$\text{(i)} E[p^e] = \{O\}, \quad \text{(ii)} E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}.$$

2.2 最小 Weierstrass 方程式と還元

この節では K を離散付値 v に対し完備な局所体，$R = \{x \in K | v(x) \geqq 0\}$ を K の整数環，$R^* = \{x \in K | v(x) = 0\}$ を R の単元群，$\mathcal{M} = \{x \in K | v(x) > 0\}$ を R の極大イデアル，π を $\mathcal{M}$ の一意化変数 (つまり $\mathcal{M} = \pi R$ となる)，$k = R/\mathcal{M}$ を R の剰余体とする．

E/K を Weierstrass 方程式

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

で定義される楕円曲線とする．$u \in \bar{K} \setminus \{0\}$ に対し，変数変換 $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ を行うことによって，E は係数 a_i がそれぞれ $u^i a_i$ で置き換えられた方程式で与えられる楕円曲線に移される ([2, table3.1])．この新しい楕円曲線は E と同型である ([2, Proposition3.1])．よって，この変数変換により E/K を表す Weierstrass 方程式で $a_1, a_2, a_3, a_4, a_6 \in R$ となるように取ることができる．このとき $v(\Delta) \geqq 0$ となり，v は離散付値なので $v(\Delta)$ の値が最小となるような $a_i \in R$ たちを取ることができる．

定義 2.14. E/K を楕円曲線とする．v での E の最小 (Weierstrass) 方程式とは，E を表す Weierstrass 方程式で $a_1, a_2, a_3, a_4, a_6 \in R$ であり，$v(\Delta)$ の値が最小となるものの事をいう．このときの Δ を v での E の最小判別式という．

注意 2.15. 変数変換 $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ を行うと，その前の判別式を Δ，変換後の判別式を Δ' と置くと $\Delta' = u^{-12}\Delta$ となる ([2, table3.1]) ので，$v(\Delta)$ の値は変数変換によって 12 の倍数ずつ変化する．よって，

$$a_i \in R \text{ かつ } v(\Delta) < 12 \Rightarrow \text{このときの Weierstrass 方程式は最小},$$

となる．同様に考えて $c_4' = u^{-4}c_4$，$c_6' = u^{-6}c_6$ なので

$$a_i \in R \text{ かつ } v(c_4) < 4 \Rightarrow \text{このときの Weierstrass 方程式は最小},$$
$$a_i \in R \text{ かつ } v(c_6) < 6 \Rightarrow \text{このときの Weierstrass 方程式は最小},$$

が成り立つ．もし $\mathrm{char}(k) \neq 2, 3$ ならばこの逆も成り立つ．

任意の楕円曲線は最小方程式を持ち，それは変数変換

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t, \quad u \in R^*, \quad r, s, t \in R,$$

で移りあうものを除いて一意的に定まる ([2, 7 章 Proposition1.3])．

自然な写像 $R \ni t \mapsto \tilde{t} \in k = R/\pi R$ に対し，楕円曲線 E/K の最小 Weierstrass 方程式の係数を π の還元で考えたもの，つまり

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6},$$

で表わされるものを，π を法とした E の還元という．

次に $P \in E(K)$ について，P の斉次座標を $P = [x_0, y_0, z_0]$ とおく．このとき，斉次座標の定義より $x_0, y_0, z_0 \in R$ で x_0, y_0, z_0 の少なくとも 1 つが R^* の元になるように取れる．このとき，$[\tilde{0}, \tilde{0}, \tilde{0}] \neq \tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}] \in \tilde{E}(k)$ となる．よって還元写像

$$E(K) \ni P \mapsto \tilde{P} \in \tilde{E}(k),$$

が定義される．

$\tilde{E}/k$ はなめらかでなくなる場合もある．よって，$\tilde{E}_{ns}(k)$ を $\tilde{E}(k)$ の非特異な点全体の集合として，以下の集合を定める．

$$E_0(K) = \{P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k)\}, \quad E_1(K) = \{P \in E(K) | \tilde{P} = \tilde{O}\}.$$

このとき [2, 7 章 Proposition1.3(b)] よりこれら 2 つの集合は最小方程式の選び方によらずに定まる．

次が [2, 7 章 Propositionp2.1] で示される．

命題 2.16. 可換群の完全列

$$o \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0,$$

が存在する．ここで $E_0(K) \to \tilde{E}_{ns}(k)$ は π を法とした還元写像によるものである．

特に，$E_0(K)$ は $E(K)$ の指数有限な部分群となる ([2, 7 章 cor6．2])．よって，玉河数 $c_v := [E(K) : E_0(K)]$ を定義することができる．命題 2.16 を使うことで次が示される．証明は [2, 7 章 Proposition3.1] を見よ．

命題 2.17. E/K を楕円曲線，$m \geqq 1$ を $\mathrm{char}(k)$ と互いに素な整数とする．
(a) 部分群 $E_1(K)$ は位数 m の捩れ点を持たない．
(b) $\tilde{E}/k$ が非特異であるとする．このとき還元写像

$$E(K)[m] \to \tilde{E}/k,$$

は単射となる．ここで $E(K)[m]$ は $E(K)$ の点で位数が m であるもの全体の集合である．

命題 2.17 を使うことで，数体上定義された楕円曲線の捩れ部分群を見つけることができる．具体的な例は，[2, 7 章 Example3.3.1, 3.3.2 ,3.3.3] を見よ．

定義 2.18. E/K を楕円曲線，$\tilde{E}$ を，E の最小方程式の π を法とした還元とする．
(a) $\tilde{E}$ が非特異であるとき，E は良い還元を持つという．
(b) $\tilde{E}$ がノードを持つとき，E は乗法的な還元を持つという．
(c) $\tilde{E}$ がカスプを持つとき，E は加法的な還元を持つという．
(b)，(c) のとき，E は悪い還元を持つという．

[2, 3 章 Proposition1.4] を使うと次が従う．

命題 2.19. E/K を最小 Weierstrass 方程式

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

で与えられる楕円曲線，Δ をこの式の判別式，c_4 を定義 2.6 で定められる係数とすると次が成り立つ．
(a) E が良い還元を持つ事と $v(\Delta) = 0$ となる，つまり $\Delta \in R^*$ となる事は同値である．
(b) E が乗法的な還元を持つ事と $v(\Delta) > 0$ かつ $v(c_4) = 0$ となる，つまり $\Delta \in \mathcal{M}$ かつ $c_4 \in R^*$ となる事は同値である．
(c) E が加法的な還元を持つ事と $v(\Delta) > 0$ かつ $v(c_4) > 0$ となる，つまり $\Delta, c_4 \in \mathcal{M}$ となる事は同値である．

内田等の論文で使われている小平型とは，この還元の型の，特に悪い還元についてさらに細かく分類したものである．

2.3 Mordell-Weil 群

この節では Mordell-Weil 群と高さ関数について説明する．

定義 2.20. E/K を楕円曲線とする．E の Mordell-Weil 群とは，E の有理点全体のなす群 $E(K)$ のことをいう．

Mordell-Weil 群 $E(K)$ は有限生成，つまり

$$E(K) \cong E(K)_{\mathrm{tors}} \times \mathbb{Z}^r, r \in \mathbb{N},$$

となる (ここで $E(K)_{\mathrm{tors}}$ は $E(K)$ の捩れ点全体の有限集合で，$E(K)$ の捩れ部分群と言う．また，$\mathbb{Z}^r$ と同型な $E(K)$ の部分群を $E(K)$ の自由部分群，その基底を $E(K)$ の基

底，r を $E(K)$ のランクという)．これを Mordell-Weil の定理という．これは，まず弱 Mordell-Weil 定理により $m \geqq 2$ に対し $E(K)/mE(K)$ が有限群となる事を示し，さらに $E(K)$ に降下定理を使うことによって示される．弱 Mordell-Weil 定理と降下定理は以下の通り．証明はそれぞれ [2, 8 章§ 1]，[2, 8 章§ 3] を見よ．

定理 2.21. [弱 Mordell-Weil 定理] K を数体，E/K を楕円曲線，$m \geqq 2$ を整数とする．このとき $E(K)/mE(K)$ は有限群となる．

定理 2.22. [降下定理] A を可換群とする．次の 3 つの性質を満たす (高さ) 関数 $h : A \to \mathbb{R}$ が存在するとする．
(i) $Q \in A$ とする．このとき A と Q に依存する定数 C_1 で．任意の $P \in A$ に対し

$$h(P+Q) \leqq 2h(P) + C_1,$$

となるものが存在する．
(ii) A に依存する整数 $m \geqq 2$ と定数 C_2 で，任意の $P \in A$ に対し

$$h(mP) \geqq m^2 h(P) - C_2,$$

となるものが存在する．
(iii) 任意の定数 C_3 に対し，集合

$$\{P \in A | h(P) \leqq C_3\},$$

は有限集合となる．

さらに，(ii) の整数 m に対し商群 A/mA が有限であると仮定する．このとき A は有限生成となる．

したがって，降下定理を適用するためには，$E(K)$ 上で定理 2.22 の (i)〜(iii) を満たす高さ関数を定義する必要がある．

2.4 高さ関数

定理 2.22 の (i)〜(iii) を満たす高さ関数を作るために，まず次の高さについて考える．以下，$P \in \mathbb{P}^N(\bar{\mathbb{Q}})$ を斉次座標 $P = [x_0, \cdots, x_N]$ を持ち，ある数体 K について $x_0, \cdots, x_N \in K$ となるとする．

定義 2.23. P の (K による) 高さを，

$$H_K(P) = \prod_{v \in \mathrm{M}_K} \max\{|x_0|_v, \cdots, |x_N|_v\}^{n_v},$$

で定義する．

このとき次が成り立つ．

命題 2.24. K を固定して $P \in \mathbb{P}^N(K)$ とする．
(a) 高さ $H_K(P)$ は P の斉次座標の取り方によらず定まる．
(b) $H_K(P) \geqq 1$ が成り立つ．
(c) L/K を有限次拡大とする．このとき

$$H_L(P) = H_K(P)^{[L:K]},$$

が成り立つ．

証明. (a) 計算と積公式 [2, 8 章 product formula5.3] により示される．(b) 任意の点 P について，斉次座標の成分を少なくとも一つの成分が 1 になるように取れるので成り立つ．
(c) 計算と拡大公式 [2, 8 章 extension formula5.2] により示される．
詳しくは [2, 8 章 Proposition5.4] を見よ． □

$H_K(P)$ を使って，特定の数体によらない高さを定義する．

定義 2.25. P の (絶対) 高さ $H(P)$ を，

$$\begin{aligned} H(P) :&= H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}, \\ &= \left(\prod_{v \in \mathrm{M}_K} \max\left\{ |x_0|_v, \cdots, |x_N|_v \right\}^{n_v} \right)^{\frac{1}{[K:\mathbb{Q}]}}, \end{aligned}$$

で定義する．ただし，右辺は正の根を取るものとする．

このとき命題 2.24(c) より $H(P)$ は K の選び方によらない．
例えば，$P = [x_0, \cdots, x_N] \in \mathbb{P}^N(\mathbb{Q})$ の場合，$x_0, \cdots, x_N \in \mathbb{Z}, \gcd(x_0, \cdots, x_N) = 1$ と取れるので，このとき v が非アルキメデス的ならば $\max\{|x_0|_v, \cdots, |x_N|_v\} = 1$ となる．よってこの場合 $H(P) = \max\{|x_0|_\infty, \cdots, |x_N|_\infty\}$ が成り立つ．ただし，$|\cdot|_\infty$ は通常の絶対値である．
$H(P)$ に関して，特に次が成り立つ．証明は [2, 8 章 Theorem5.11] を見よ．

定理 2.26. C を定数とする．このとき，集合

$$\left\{ P \in \mathbb{P}^N(\bar{\mathbb{Q}}) | H(P) \leqq C \text{ かつ } [\mathbb{Q}(P) : \mathbb{Q}] \leqq d \right\},$$

は有限な点集合となる．ここで $\mathbb{Q}(P)$ は P の斉次座標の成分と $\mathbb{Q}$ を含む最小の体である．特に，任意の数体 K に対して集合

$$\left\{P \in \mathbb{P}^N(K) | H(P) \leqq C\right\},$$

は有限となる．

つまり $H(P)$ は定理 2.22 の (iii) を満たす．よってこの $H(P)$ を使いさらに (i)，(ii) を満たすような関数を構成していく．

E/K を楕円曲線としたとき，[2, 2 章 Example2.2] で定数でない関数 $f \in \bar{E}(K)$ に対し射 $f : E \to \mathbb{P}^1$ で，

$$P \mapsto \begin{cases} [1,0] & P \text{ は } f \text{ の極}, \\ [f(P),1] & \text{その他}, \end{cases}$$

となるものが定められる事を見た．これより $E(\bar{K})$ 上の高さ関数 $H_f(P) = H(f(P))$ を定義することができる．この H_f は対数を取ることにより，より良い性質を持つようになる事を紹介する．

定義 2.27. 射影空間上の (絶対対数) 高さ関数 $h : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{R}$ を，

$$\begin{aligned} h(P) &:= \log H(P), \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathrm{M}_K} n_v \log \max\left\{|x_0|_v, \cdots, |x_N|_v\right\}, \end{aligned}$$

で定義する．

このとき命題 2.24(b) より任意の P に対し $h(P) \geqq 0$ が成り立つ．

定義 2.28. E/K を楕円曲線，$f \in \bar{K}(E)$ を関数とする．E 上の (f による) 高さ関数 $h_f : E(\bar{K}) \to \mathbb{R}$ を

$$h_f(P) := h(f(P)),$$

で定義する．

このとき定理 2.26 より次が成り立つ．証明は [2, 8 章 Proposition6.1] を見よ．

命題 2.29. E/K を楕円曲線，$f \in \bar{K}(E)$ を定数でない関数とする．このとき任意の定数 C に対し，集合

$$\left\{P \in E(K) | h_f(P) \leqq C\right\},$$

は有限となる．

また，h_f と楕円曲線の加法には次の関係がある．証明は [2, 8 章 Theorem6.2] を見よ．

定理 2.30. E/K を楕円曲線，$f \in \bar{K}(E)$ を偶関数，つまり点の -1 倍写像 $[-1]$ に対し $f \circ [-1] = f$ が成り立つとする．このとき任意の $P, Q \in E(\bar{K})$ に対して

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1),$$

が成り立つ．ここで，$O(1)$ は E と f のみに依存する．

定理 2.30 を使うことで次が示される．証明は [2, 8 章 Corollary6.4] を見よ．

系 2.31. E/K を楕円曲線，$f \in K(E)$ を偶関数とする．
(a) $Q \in E(\bar{K})$ とする．このとき任意の $P \in E(\bar{K})$ に対し

$$h_f(P+Q) \leqq 2h_f(P) + O(1),$$

となる．ここで $O(1)$ は E と Q と f に依存する．
(b) $m \in \mathbb{Z}$ とする．このとき任意の $P \in E(\bar{K})$ に対し

$$h_f(mP) = m^2 h_f(P) + O(1),$$

となる．ここで $O(1)$ は E と f と m にのみ依存する．

よって，h_f が定理 2.22 の (i), (ii), (iii) を満たすことが，それぞれ系 2.31(a)，系 2.31(b) の $m = 2$ の場合，命題 2.29 から示される．以上から Mordell-Weil の定理が示される．

注意 2.32. [1]，[6]，[8]，[10] では，$x : E \to \mathbb{P}^1$ を

$$P \mapsto \begin{cases} [1,0] & P = O, \\ [x(P),1] & P \neq O, \text{ただし } x(P) \text{ は } P \text{ の } x \text{ 座標とする}, \end{cases}$$

として，x による高さ関数 h_x を通常高さ関数としている．

命題 2.29 や系 2.31 より，通常高さ関数は $O(1)$ を除けば二次形式の性質を持つ．極限を使うことで h_f から定理 2.22 の (i)〜(iii) を満たす $E(\bar{K})$ 上の高さ関数で二次形式となるものが構成されることが Néron や Tate によって示されている．[2] では Tate によるものを紹介している．

定義 2.33. 楕円曲線 E/K 上の標準 (又は Néron-Tate) 高さ関数 $\hat{h}, \hat{h}_E : E(\bar{K}) \to \mathbb{R}$ とは，$f \in K(E)$ を任意の偶関数としたとき

$$\hat{h}(P) := \frac{1}{\deg(f)} \lim_{N \to \infty} 4^{-N} h_f(2^N P),$$

で定義される関数のことである．

$\frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f(2^N P)$ が存在し，f の選び方によらずに関数が定まることについては [2, 8 章 Proposition9.1] を見よ．

注意 2.34. [1]，[6]，[8]，[10] では標準高さ関数を $\lim_{N\to\infty} 4^{-N} h_x(2^N P)$ で定義している．つまり [2] での標準高さ関数を $\hat{h}$，$\hat{h}'$ を $\lim_{N\to\infty} 4^{-N} h_x(2^N P)$ とすると，$\deg x = 2$ より $2\hat{h} = \hat{h}'$ となる．

$\hat{h}$ は次を満たす．証明は [2, 8 章 Theorem9.3] を見よ．

定理 2.35. E/K を楕円曲線，$\hat{h}$ を E の標準高さ関数とする．
(a) 任意の $P, Q \in E(\bar{K})$ に対し

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q),$$

が成り立つ．
(b) 任意の $P \in E(\bar{K})$ と任意の $m \in \mathbb{Z}$ に対し

$$\hat{h}(mP) = m^2 \hat{h}(P),$$

が成り立つ．
(c) $\hat{h}$ は E 上の二次形式である．つまり，

$$\langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}, \quad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q),$$

が双線形形式となる．
(d) $P \in E(\bar{K})$ とする．このとき $\hat{h}(P) \geqq 0$ であり，$\hat{h}(P) = 0$ となる事と P が捩れ点であることは同値である．
(e) $f \in K(E)$ を偶関数とする．このとき

$$(\deg f)\hat{h} = h_f + O(1),$$

が成り立つ．ここで $O(1)$ は E と f に依存する．

定義からわかる通り，通常高さ関数は実際に値を求めることができるが標準高さ関数にはそれが難しい．しかし，標準高さ関数は通常高さ関数にくらべて理論面で扱いやすいという利点がある．例えば通常高さ関数は系 2.31 より $m \in \mathbb{Z}$, $P \in E(K)$ に対して $h(mP) = m^2 h(P) + O(1)$, となるが, 標準高さ関数だと定理 2.35 より $h(mP) = m^2 h(P)$,

が成り立っていた．よって，標準高さ関数や標準高さ関数と通常高さ関数の差の評価を利用する事で，その有用性を発揮することがある．例えば 4.1 節や 4.2 節ではそれぞれの点の取りうる値を絞り込んだり，さらにその値と高さ関数の先述したような性質を利用することで Mordel-Weil 群の生成元であるかどうか判定している．

一般に，Mordel-Weil 群の捩れ点はその座標になり得る整数が限られ ([2, 8 章§ 7])，特に $\mathbb{Q}$ 上の楕円曲線の Mordel-Weil 群の捩れ部分群は同型を除き 15 種類のみである ([2, 8 章 Theorem7.5])．よって，捩れ部分群は比較的簡単に計算することができる (詳細は [2, 8 章§ 7] を見よ)．しかし，一般の場合で Mordel-Weil 群のランクや基底を判定するような方法は見つかってなく，さらに，任意の大きさのランクを持つ楕円曲線が存在すると予想されている ([2, 8 章 Conjecture10.1])．よって，標準高さ関数や標準高さ関数と通常高さ関数の差のより良い評価を得ることが Mordel-Weil 群の性質を調べる上で重要となってくるのである．

3 内田の論文

内田の論文 [1] では，J．E．Cremona，M．Prickett，S．Siksek[6] でのアルキメデス的な素点での評価を改善することに成功している．内田の論文では 3.1 節で定義する $S_v(m), T_v(m), (m \in \mathbb{Z}, m \geqq 2)$ を使いアルキメデス的な素点での評価を得ている．$S_v(2), T_v(2)$ で評価したものが J．E．Cremona，M．Prickett，S．Siksek の論文での評価である．$h(P) - \hat{h}(P)$ は 3.3 節で定義する局所高さ関数 λ_v を使うと

$$h(P) - \hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathrm{M}_K} n_v \left(\log \max\{1, |x(P)|_v\} - \lambda_v(P) \right).$$

と表わされる．$S_v(m), T_v(m)$ は m を ∞ に飛ばすことで，$\log \max\{1, |x(P)|_v\} - \lambda_v(P)$ のそれぞれ下限，上限となる (系 3.32)．よって，少なくとも理論上は，m を 2 だけでなく十分大きい値にすることでアルキメデス的な素点において任意の精度で評価を得ることができるのである．実際の計算結果は [1, 9 章] を見よ．ここでの h，$\hat{h}$ はそれぞれ [1] での通常高さ関数，標準高さ関数を表すとする．

3.1 内田の論文の主定理

内田の論文では以下を主張している．

ϕ_m, ψ_m^2 を等分多項式とする．等分多項式についての詳細は 3.2 節を見よ．

$v \in \mathrm{M}_K, m$ を正整数とする．関数 $\Phi_{m,v} : E(K_v) \to \mathbb{R}$ を

$$\Phi_{m,v}(P) = \begin{cases} 1 & (P = O), \\ \dfrac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}} & (P \neq O), \end{cases} \tag{3.1}$$

と定める．このとき $\Phi_{m,v}$ は有界連続関数であり，下限が 0 よりも大きくなる．

$$\epsilon_{m,v}^{-1} = \inf_{P \in E(K_v)} \Phi_{m,v}(P), \quad \delta_{m,v}^{-1} = \sup_{P \in E(K_v)} \Phi_{m,v}(P), \tag{3.2}$$

とおいて，さらに

$$S_v(m) = \frac{\log \delta_{m,v}}{m^2 - 1}, \quad T_v(m) = \frac{\log \epsilon_{m,v}}{m^2 - 1}, \tag{3.3}$$

とおく．また，α_v を E の $v \in \mathrm{M}_K^0$ における小平型と玉河数 c_v によって定まる定数 (具体的な値は [1, Table1] を見よ)，q_v を v における K の剰余体 k_v の元の個数とする．

主定理は以下の通り．

定理 3.4. $m \geqq 2$ を整数とする．このとき任意の $P \in E(K)$ に対して

$$\begin{aligned} &\frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathrm{M}_K^\infty} n_v S_v(m) \leqq h(P) - \hat{h}(P) \\ &\leqq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathrm{M}_K^\infty} n_v \, T_v(m) + \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathrm{M}_K^0} \left(\alpha_v + \frac{1}{6} \mathrm{ord}_v \left(\frac{\Delta}{\Delta_v^{\min}} \right) \right) \log q_v, \end{aligned}$$

が成り立つ．

α_v については命題 3.20 や [6, Proposition6，Proposition8] を見よ．

3.2 等分多項式

等分多項式 $\phi_m, \psi_m \in K[X, Y]$ とは，$m = 0, 1, 2, 3, \cdots, P \in E(K)$ に対し mP の座標の分子，分母を表すことのできる多項式のことである．$P = (x, y) \in E(K)$ としたとき $\phi_m(x, y), \psi_m^2(x, y)$ は x のみで表すことができ (命題 3.7)，このとき互いに素な多項式となる (命題 3.10)．$\phi_m(x, y), \psi_m^2(x, y)$ を使うと P の x 座標を表すことができるが，y 座標を表すためにはもう一つの等分多項式を使わなければならない．詳しくは [7] を見よ．ここでは等分多項式の定義と性質について少し紹介する．

定義 3.5. $\phi_m, \psi_m \in K[X,Y]$ を以下で定める.
$\phi_1 = X, \quad \phi_2 = X^4 - b_4X^2 - 2b_6X - b_8,$
$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2Y + a_1X + a_3, \quad \psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,$
$\psi_4 = \psi_2 \cdot \left(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\right),$
$m \geqq 2$, について,
$\phi_m = X\psi_m^2 - \psi_{m-1} \cdot \psi_{m+1},$
$\psi_{2m+1} = \psi_{m+2} \cdot \psi_m^3 - \psi_{m-1} \cdot \psi_{m+1}^3, \quad \psi_2 \cdot \psi_{2m} = \psi_m \cdot \left(\psi_{m+2} \cdot \psi_{m-1}^2 - \psi_{m-2} \cdot \psi_{m+1}^2\right),$
この ϕ_m, ψ_m を等分多項式という.

等分多項式について次が成り立つ.

命題 3.6. $P = (x,y) \in E(K), m \geqq 0$ を整数とする. このとき, $mP = O$ であることと $\psi_m(x,y) = 0$ であることは同値であり, $mP \neq O$ のとき,

$$x(mP) = \frac{\phi_m(x,y)}{\psi_m(x,y)^2},$$

が成り立つ.

証明. $\mathbb{C}$ の格子 L と, Weierstrass $\wp$ 関数から導かれる関数 $\mathfrak{p}, \tilde{\mathfrak{p}} : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ で, $\mathbb{C}/L \ni z(\mod L) \mapsto (\mathfrak{p}, \tilde{\mathfrak{p}}) \in E$ が同型射となるものが存在する. この $\mathfrak{p}$ について, $\mathfrak{p}(nz) - \mathfrak{p}(mz) = -\frac{\psi_{n+m}(z)\psi_{n-m}(z)}{\psi_n(z)^2\psi_m(z)^2}, (m,n \in \mathbb{N}, n \neq m)$ が [7, Lemma2.19] で示される. この $m = 1$ の場合と $\phi_n = X\psi_n^2 - \psi_{n-1}\psi_{n+1}$ より導かれる. 詳しくは [7, 2 章,Theorem1.19] を見よ. □

命題 3.7. $P = (x,y) \in E(K)$ とすると, $\phi_m(x,y), \psi_m^2(x,y) \in \mathbb{Z}[b_2, b_4, b_6, b_8, x]$ であり, それぞれ x の多項式として考えたとき,
(a) ϕ_m は次数 m^2 で最高次の係数は 1,
(b) ψ_m^2 は次数 $m^2 - 1$ で最高次の係数は m^2,
となる.

命題 3.7 を示すために, まず次を示す.

命題 3.8. m が偶数のとき, $\psi_2^{-1}\psi_m \in \mathbb{Z}[b_2, b_4, b_6, b_8, x]$ であり, x の多項式として見たとき $\psi_2^{-1}\psi_m$ は次数が $\frac{m^2-4}{2}$, 最高次の係数が $\frac{m}{2}$ となる.

また, m が奇数のとき, $\psi_m \in \mathbb{Z}[b_2, b_4, b_6, b_8, x]$ であり, x の多項式として見たとき ψ_m は次数が $\frac{m^2-1}{2}$, 最高次の係数が m となる.

証明. m を偶数とする．まず $\psi_m \in \mathbb{Z}[b_2, b_4, b_6, b_8, x] = F$ となる事を示す．$F \ni \psi_1, \psi_3, \psi_2^{-1}\psi_0, \psi_2^{-1}\psi_2, \psi_2^{-1}\psi_4$ は明らかである．$m > 4$ として $m-1$ まで成り立つとする．この時 $m = 2k, (k > 2)$ と置ける．

$$\psi_2\psi_{2k} = \psi_k\left(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2\right),$$

より，

$$\psi_2^{-1}\psi_{2k} = \psi_2^{-2}\psi_k\left(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2\right).$$

k が奇数のとき，$k > 2$ から $m = 2k > k, k \pm 2, k \pm 1$ なので帰納法の仮定より $\psi_k, \psi_{k\pm2}, \psi_2^{-1}\psi_{k\pm1} \in F$ となるので，

$$\psi_2^{-1}\psi_{2k} = \psi_k\left(\psi_{k+2}\left(\psi_2^{-1}\psi_{k-1}\right)^2 - \psi_{k-2}\left(\psi_2^{-1}\psi_{k+1}\right)^2\right) \in F. \tag{3.9}$$

k が偶数の場合も同様にして示される．

次に $\psi_2^{-1}\psi_m$ の次数が $\frac{m^2-4}{2}$，最高次の係数が $\frac{m}{2}$ となる事を示す．$m = 0, 1, 2, 3, 4$ の時成り立つことは明らかである．$m > 4$ として $m-1$ まで成り立つとする．この時 $m = 2k, (k > 2)$ と置ける．k が奇数のとき (3.9) を使うと，$k > 2$ から $m = 2k > k, k \pm 2, k \pm 1$ なので帰納法の仮定を使うと

$$\begin{aligned}
\psi_2^{-1}\psi_{2k} =& \psi_k\left(\psi_{k+2}\left(\psi_2^{-1}\psi_{k-1}\right)^2 - \psi_{k-2}\left(\psi_2^{-1}\psi_{k+1}\right)^2\right), \\
=& \left(kx^{\frac{k^2-1}{2}} + \dots\right)\left\{\left((k+2)x^{\frac{(k+2)^2-1}{2}} + \dots\right)\left(\frac{k-1}{2}x^{\frac{(k-1)^2-4}{2}} + \dots\right)^2\right. \\
& \left. - \left((k-2)x^{\frac{(k-2)^2-1}{2}} + \dots\right)\left(\frac{k+1}{2}x^{\frac{(x+1)^2-4}{2}} + \dots\right)^2\right\}, \\
=& \left(kx^{\frac{k^2-1}{2}} + \dots\right)\left\{\frac{(k+2)(k-1)^2}{4}x^{\frac{3k^2-3}{2}} - \frac{(k-2)(k+1)^2}{4}x^{\frac{3k^2-3}{2}} + \dots\right\}, \\
=& \left(kx^{\frac{k^2-1}{2}} + \dots\right)(x^{\frac{3k^2-3}{2}} + \dots), \\
=& \frac{2k}{2}x^{\frac{(2k)^2-4}{2}} + \dots,
\end{aligned}$$

となり，k が奇数のときに成り立つ．k が偶数の時も同様にして示される．

m が奇数の時も同様にして示される． □

命題 3.7 の証明. 命題 3.8 を使い，命題 3.7 を示す．まず ψ_m^2 について命題 3.7 を示して

いく．m が奇数のときは明らかに命題 3.7(b) が成り立ち，m が偶数のときも，

$$\begin{aligned}\psi_2^2 =&(2y+a_1x+a_3)^2\\ =&4y^2+a_1^2x^2+a_3^2+2\left(2a_1xy+a_1a_3x+2a_3y\right)\\ =&4\left(x^3+a_2x^2+a_4x+a_6\right)+a_1^2x^2+a_3^2+2a_1a_3x\\ =&4x^3+b_2x^2+2b_4x+b_6\in F,\end{aligned}$$

と $\psi_m^2=\psi_2^2(\psi_2^{-1}\psi_m)^2$ から $\psi_m^2\in F$，次数が $3+\frac{m^2-4}{2}\cdot 2=m^2-1$，最高次の係数が $4\cdot\frac{m^2}{4}=m^2$ となり，以上から命題 3.7(b) が示された．

以上の結果を使って ϕ_m について (a) を示していく．$\phi_m=x\psi_m^2-\psi_{m-1}\psi_{m+1}$ より，m を奇数とすると

$$\begin{aligned}\phi_m =&x\psi_m^2-\psi_2^2\left(\psi_2^{-1}\psi_{m-1}\right)\left(\psi_2^{-1}\psi_{m+1}\right),\\ =&x\left(m^2x^{m^2-1}+\dots\right)-\left(4x^3+\dots\right)\left(\frac{m-1}{2}x^{\frac{(m-1)^2-4}{2}}+\dots\right)\left(\frac{m+1}{2}x^{\frac{(m+1)^2-4}{2}}+\dots\right),\\ =&m^2x^{m^2}-(m-1)(m+1)x^{m^2}+\dots,\\ =&x^{m^2}+\dots,\end{aligned}$$

となり，この場合に命題 3.7(a) が成り立つ．m が偶数のときも同様にして示されるので，以上から命題 3.7 が示された． □

命題 3.10. ϕ_m と ψ_m^2 は互いに素な多項式.

証明. ある $m>1$ が存在し，ϕ_m と ψ_m^2 が共通の既約な多項式 $\theta(x)$ を持つ場合の最小の自然数であるとする.

(i) $m=2k$ の場合は ($k\geqq 1$)，[7, Proposition1.23] より

$$\Delta=\left(-48x^2-8b_2x+b_2^2-32b_4\right)\phi_2(x)+\left(12x^3-b_2x^2-10b_4x+b_2b_4-27b_6\right)\psi_2^2(x),$$

が成り立つので，$x=\frac{\phi_k}{\psi_k^2}$ を代入すると

$$\begin{aligned}\Delta=&\left(-48\frac{\phi_k^2}{\psi_k^4}-8b_2\frac{\phi_k}{\psi_k^2}+b_2^2-32b_4\right)\phi_2\left(\frac{\phi_k}{\psi_k^2}\right)\\ &+\left(12\frac{\phi_k^3}{\psi_k^6}-b_2\frac{\phi_k^2}{\psi_k^4}-10b_4\frac{\phi_k}{\psi_k^2}+b_2b_4-27b_6\right)\psi_2^2\left(\frac{\phi_k}{\psi_k^2}\right),\end{aligned}$$

ここで，[7, Exercise1.6.13] より $n,k\in\mathbb{Z}_{>0}$ に対し

$$\phi_{nk}(x)=\psi_k^{2n^2}(x)\phi_n\left(\frac{\phi_k(x)}{\psi_k^2(x)}\right),\quad \psi_{nk}^2(x)=\psi_k^{2n^2}(x)\psi_n^2\left(\frac{\phi_k(x)}{\psi_k^2(x)}\right), \tag{3.11}$$

が成り立つので，$n=2$ として上の等式に使うと，

$$\Delta = \left(-48\frac{\phi_k^2}{\psi_k^4} - 8b_2\frac{\phi_k}{\psi_k^2} + b_2^2 - 32b_4\right)\frac{\phi_{2k}}{\psi_k^8} + \left(12\frac{\phi_k^3}{\psi_k^6} - b_2\frac{\phi_k^2}{\psi_k^4} - 10b_4\frac{\phi_k}{\psi_k^2} + b_2b_4 - 27b_6\right)\frac{\psi_{2k}^2}{\psi_k^8},$$

となるので

$$\psi_k^{14}\Delta = \left\{-48\phi_k^2 - 8b_2\phi_k\psi_k^2 + (b_2^2 - 32b_4)\psi_k^4\right\}\phi_{2k}\psi_k^2 + \left\{12\phi_k^3 - b_2\phi_k^2\psi_k^2 - 10b_4\phi_k\psi_k^4 + (b_2b_4 - 27b_6)\psi_k^6\right\}\psi_{2k}^2,$$

θ は ϕ_{2k}, ψ_{2k}^2 を割り切るので ψ_k^{14} も割り切る．θ は既約なので θ は ψ_k^2 も割り切る．また，(3.11) より

$$\begin{aligned}\phi_{2k}(x) = \psi_k^8(x)\phi_2\left(\frac{\phi_k(x)}{\psi_k^2(x)}\right) &= \psi_k^8(x)\left(\frac{\phi_k^4(x)}{\psi_k^8(x)} - b_4\frac{\phi_k^2(x)}{\psi_k^4(x)} - 2b_6\frac{\phi_k(x)}{\psi_k^2(x)} - b_8\right),\\ &= \phi_k^4 - b_4\phi_k^2\psi_k^4 - 2b_6\phi_k\psi_k^6 - b_8\psi_k^8,\end{aligned}$$

よって θ は ϕ_k も割り切るが，これは m の取り方に矛盾する．

(ii) $m=2k+1$ の場合は ($k \geqq 0$)，等分多項式の定義より $\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$ より $\psi_{m-1}^2\psi_{m+1}^2 = (x\psi_m^2 - \phi_m)^2$ なので，θ は ψ_{m+1}^2 又は ψ_{m-1}^2 を割り切る．ψ_{m+1}^2 を割り切るとすると，

$$\phi_{m+1}^2 = \left(x\psi_{m+1}^2 - \psi_m\psi_{m+2}\right)^2 = x^2\psi_{m+1}^4 - 2x\psi_{m+1}^2\psi_m\psi_{m+2} + \psi_m^2\psi_{m+2}^2,$$

より θ は ϕ_{m+1} を割り切るので矛盾が導かれる．ψ_{m-1}^2 の場合も同様にして矛盾が導かれる． □

次の節で紹介する $v \in M_K$ ごとの局所高さ関数を使った和で通常高さ関数と標準高さ関数の差 (3.3 節でさらに関数 Ψ_v を定義し，その和で表される) を表すことができる．内田の論文では，任意の $m \geqq 2$ について $\Phi_{m,v}$ を定義し，この $\Phi_{m,v}$ を使って局所高さ関数を表している．そしてこの $\Phi_{m,v}$ の上限下限を使って Ψ_v の評価を表したのが $S_v(m), T_v(m)$ である．J.E. Cremona, M. Prickett, S. Siksek の [6] の論文で使われているのは $S_v(2), T_v(2)$ であるが，3.4 節で任意の $m \geqq 2$ に対し $S_v(m) \leqq \Psi_v(P) \leqq T_v(m)$ が，3.5 節で任意の $m \geqq 2, l \geqq 1$ に対し $S_v(m) \leqq S_v(m^l), \quad T_v(m^l) \leqq T_v(m)$ が示される．この様な性質は，v ごとの $\Phi_{m,v}$ と Ψ_v の m を変化させることから来る性質から導かれる．内田の論文では，これらの性質を利用することでより良い評価を得ているのである．

3.3 局所高さ関数

この節では局所高さ関数について述べる．局所高さ関数とは，Weierstrass 方程式と素点 v により定まる高さ関数であり，その素点がアルキメデス的である場合と非アルキメデス的である場合でそれぞれ具体的な形で表される．詳細は [3, 6 章] を見よ．局所高さ関数はその和で標準高さ関数を表すことができるので，標準高さ関数と通常高さ関数の差を表す際に重要な役割を果たす．

命題 3.12. $\Phi_{m,v}$ は $E(K_v)$ 上の有界連続関数で，

$$\inf_{P\in E(K_v)} \Phi_{m,v}(P) > 0,$$

が成り立つ．

証明. $\phi_m(x(P)), \psi_m^2(x(P)), x(P)$ は連続なので，$P \in E(K_v)\setminus\{O\}$ で $\Phi_{m,v}$ は連続．また，$P \to O$ とするとき $x(P) \to \infty$ となる事と命題 3.7 より，

$$\begin{aligned}\lim_{P\to O} \Phi_{m,v}(P) &= \lim_{P\to O} \frac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}},\\ &= \lim_{P\to O} \frac{|\phi_m(x(P))|_v}{|x(P)|_v^{m^2}},\\ &= 1 = \Phi_{m,v}(O).\end{aligned}$$

よって，$\Phi_{m,v}$ は $P = O$ でも連続となる．

また，$\mathbb{P}^2(K_v)$ はコンパクトで $E(K_v) \subset \mathbb{P}^2(K_v)$ は閉集合なので，$E(K_v)$ はコンパクトである．よって $\Phi_{m,v}$ は有界な関数となる．

明らかに $P \in E(K_v)$ で $\Phi_{m,v}(P) \geqq 0$ なので，後半を示すために $\inf_{P\in E(K_v)} \Phi_{m,v}(P) = 0$ と仮定する．$E(K_v)$ はコンパクトなので，ある $P \in E(K_v)$ で $\Phi_{m,v}(P) = 0$ を満たすものがある．このとき $P \neq O$ なので，定義より $\phi_m(x(P)) = \psi_m^2(x(P)) = 0$ となる．しかし，命題 3.10 より ϕ_m, ψ_m^2 は互いに素なので矛盾となる． □

定義 3.13. 局所高さ関数 $\lambda_v : E(K_v)\setminus\{O\} \to \mathbb{R}$ を，

$$\lambda_v(P) = \log \max\{1, |x(P)|_v\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_{2,v}(2^i P),$$

で定義する．

命題 3.14. (a) λ_v は $E(K_v)\setminus\{O\}$ 上で連続であり，O の任意の近傍の補集合上で有界である．

(b) 極限

$$\lim_{P\to O}\{\lambda_v(P)-\log|x(P)|_v\},$$

が存在する．

(c) $P,Q\in E(K_v)$ が $P\neq O, Q\neq O, P\pm Q\neq O$ ならば，

$$\lambda_v(P+Q)+\lambda_v(P-Q)=2\lambda_v(P)+2\lambda_v(Q)-2\log|x(P)-x(Q)|_v,$$

が成り立つ．

(d) 任意の整数 $m>0$ に対して $P\in E(K_v), mP\neq O$ ならば，

$$\lambda_v(mP)=m^2\lambda_v(P)-\log|\psi_m^2(x(P))|_v,$$

が成り立つ．

証明. (a) $P\in E(K_v)\setminus\{O\}$ の実数値関数 $\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP)$ は命題 3.12 と $E(K_v)\setminus\{O\}$ のコンパクト性より有界連続関数となる．よって Weierstrass の M 判定法より $\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP)$ は一様収束するので連続となり，よって $\lambda_v(P)$ は連続関数となる．また，O の任意の近傍の補集合は $E(K_v)$ の閉集合なので，$E(K_v)$ のコンパクト性よりこれもまたコンパクトとなる．よって $\lambda_v(P)$ は O の任意の近傍の補集合上で有界となる．

(b) $P\to O$ とすると $|x(P)|_v\to\infty$ となるので，O に十分近い P を取って来れば

$$\begin{aligned}\lambda_v(P)-\log|x(P)|_v&=\log|x(P)|_v+\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP)-\log|x(P)|_v,\\&=\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP).\end{aligned}$$

命題 3.12 より $\log\Phi_{2,v}(2^iP)$ は O でも定義されて連続なので，$\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP)$ は O でも連続関数となる．$\log\Phi_{2,v}(2^iP)$ は有界なので，$\lim_{P\to O}\{\lambda_v(P)-\log|x(P)|_v\}$ が存在する．

(c) まずアルキメデス的な素点での具体的な式を求めて，その式で (つまり $\mathbb{C}$ 上で)(c) が成り立つ事を示し，さらに $\mathbb{Q}_p$ の拡大体でも (c) が成り立つ事を示す．詳しくは [3, 6 章 § 3, Exercise6.3] を見よ．

(d) 命題 3.17 の証明と同様にして示される． □

命題 3.15. 関数 $\lambda_v : E(K_v)\setminus\{O\} \to \mathbb{R}$ がある整数 $m \geqq 2$ に対して命題 3.14 の (a), (b), (d) を満たせば一意的に定まる.

証明. ある $m \geqq 2$ に対して λ_v, λ_v' が命題 3.14 の (a), (b), (d) を満たすとする. $\Lambda : E(K_v) \to \mathbb{R}$ を,

$$\Lambda(P) = \begin{cases} \lim\limits_{Q\to O}(\lambda_v(Q) - \lambda_v'(Q)) & (P = O), \\ \lambda_v(P) - \lambda_v'(P) & (P \neq O), \end{cases}$$

と定義する.

(b) より $P = O$ で $\Lambda(P)$ は $P = O$ で well-defined. (a) より Λ は $E(K_v)$ 上で有界な連続関数となる.

したがって, ある $M > 0$ で, 任意の $P \in E(K_v)$ に対して $|\Lambda(P)| \leqq M$ を満たすものが存在する. (d) より, 任意の $mP \neq O$ となる $P \in E(K_v)$ に対して $\Lambda(mP) = m^2\Lambda(P)$ が成り立つ. しかし, $mP = O$ となる集合は Mordell-Weil の定理より $E(K_v)$ の離散部分集合であり Λ は連続関数なので, この等式は $mP = O$ の時も成立する. したがって,

$$|\Lambda(P)| = \left|\frac{\Lambda(m^iP)}{m^{2i}}\right| \leqq \frac{M}{m^{2i}},$$

となる. これより $\Lambda(P) = 0$ となるので, $\lambda_v = \lambda_v'$ が示された. □

注意 3.16. [3] では命題 3.14(a), (b) と $\lambda_v(2P) = 4\lambda_v(P) - \log|\psi_2^2(x(P))|_v + \frac{1}{4}\log|\Delta|_v$ が成り立つ関数 $\lambda_v : E(K_v)\setminus\{O\} \to \mathbb{R}$ を局所高さ関数と定義している.

命題 3.17. 整数 $m \geqq 2$ に対して,

$$\lambda_v(P) = \log\max\{1, |x(P)|_v\} + \sum_{i=0}^{\infty}\frac{1}{m^{2(i+1)}}\log\Phi_{m,v}(m^iP), \quad P \in E(K_v)\setminus\{O\},$$

が成り立つ.

証明. 上の式の右辺を $\lambda_v'(P)$ とおく. このとき,

$$\begin{aligned} |\lambda_v(P) - \lambda_v'(P)| &= \left|\sum_{i=0}^{\infty}\left(\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP) - \frac{1}{m^{2(i+1)}}\log\Phi_{m,v}(m^iP)\right)\right|, \\ &\leqq \left|\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\left(\log\Phi_{m,v}(m^iP) - \log\Phi_{2,v}(2^iP)\right)\right|, \end{aligned}$$

命題 3.12 より $\log \Phi_{m,v}(m^i P) - \log \Phi_{2,v}(2^i P)$ も連続で有界，$E(K_v)$ はコンパクトなので，この最大値を $M \in \mathbb{R}$ とおくと，

$$|\lambda_v(P) - \lambda'_v(P)| \leqq M \sum_{i=0}^{\infty} \frac{1}{4^{i+1}}.$$

λ_v は (a)，(b) を満たすので，これより λ'_v は命題 3.14 の (a)，(b) を満たす．

m について (d) を示す．

$$\begin{aligned}
\lambda'_v(mP) =& \log \max\{1, |x(mP)|_v\} + \sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^{i+1}P), \\
=& \log \max\left\{1, \left|\frac{\phi_m(x(P))}{\psi_m^2(x(P))}\right|_v\right\} + m^2 \sum_{i=1}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P), \quad (\text{命題 3.6 より}), \\
=& \log \max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\} - \log |\psi_m^2(x(P))|_v + \log \max\{1, |x(P)|_v\}^{m^2} \\
& - \log \max\{1, |x(P)|_v\}^{m^2} + m^2 \sum_{i=1}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P), \\
& \left(\log \max\left\{1, \left|\frac{\phi_m(x(P))}{\psi_m^2(x(P))}\right|_v\right\} \text{を分けて}, \log \max\{1, |x(P)|_v\}^{m^2} \text{を足して引いた}\right), \\
=& m^2 \log \max\{1, |x(P)|_v\} + m^2 \frac{1}{m^2} \log \Phi_{m,v}(P) + m^2 \sum_{i=1}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P) \\
& - \log |\psi_m^2(x(P))|_v, \quad (\Phi_{m,v} \text{の定義より}), \\
=& m^2 \lambda'_v(P) - \log |\psi_m^2(x(P))|_v, \quad (\lambda'_v \text{の定義より}).
\end{aligned}$$

よって λ'_v は m について (d) を満たすので，命題 3.15 より $\lambda_v = \lambda'_v$ が示された． □

標準高さ関数は局所高さ関数の和で表わされる．

命題 3.18. 任意の $P \in E(K_v) \setminus \{O\}$ に対して

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathrm{M}_K} n_v \lambda_v(P),$$

が成り立つ．

証明. このとき $\lambda_v(P) \neq 0$ となる項は有限個なので，この等式の右辺は well-defined となる．$L(P) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathrm{M}_K} n_v \lambda_v(P)$ とおく．この時, 積公式 [2, 8 章 product formula5.3] 等により，任意の $P \in E(\bar{K})$ について $L([2]P) = 4L(P), L(P) = \frac{1}{2} h(P) + O(1)$(この h は [1] の通常高さ関数である) が成り立つ．よって [2, 8 章 Theorem9.3] より $L = \hat{h}$ が示される．詳細は [3, 6 章§ 2] を見よ． □

命題 3.18 より通常高さ関数と標準高さ関数の差は以下で表わされる．

$$h(P)-\hat{h}(P)=\frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K} n_v\left(\log\max\{1,|x(P)|_v\}-\lambda_v(P)\right).$$

よって，$\Psi_v : E(K_v)\to\mathbb{R}$ を，

$$\Psi_v(P)=\begin{cases}0 & (P=O),\\ \log\max\{1,|x(P)|_v\}-\lambda_v(P) & (P\neq O),\end{cases}$$

と定義すれば，Ψ_v の評価から $h-\hat{h}$ の評価が得られる．

命題 3.19. Ψ_v は $E(K_v)$ 上の有界連続関数である．

証明. λ_v の定義より，任意の $P\in E(K_v)\diagdown\{O\}$ に対して

$$\Psi_v(P)=-\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP),$$

命題 3.14(a) の証明と同様にして $-\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log\Phi_{2,v}(2^iP)$ が一様収束することが示されるので，Ψ_v は $E(K_v)$ 上で連続となる．$E(K_v)$ はコンパクトなので Ψ_v は有界となり，命題が証明された． □

$v\in \mathrm{M}_K^0$ としたとき，以下の結果が知られている．

命題 3.20. $v\in \mathrm{M}_K^0$ とする．このとき，

$$\inf_{P\in E(K_v)}\Psi_v(P)=0,$$
$$\sup_{P\in E(K_v)}\Psi_v(P)=\left(\alpha_v+\frac{1}{6}\mathrm{ord}_v\left(\frac{\Delta}{\Delta_v^{\min}}\right)\right)\frac{\log q_v}{n_v},$$

が成り立つ．

証明. Ψ_v の定義より

$$\Psi_v(P)=\begin{cases}0 & (P=O),\\ \log\max\{1,|x(P)|_v\}-\lambda_v(P) & (P\neq O),\end{cases}$$

だったが，[6, Proposition8 の claim1] より

$$\Psi_v(P)=\begin{cases}0 & P\in E_0(E(K_v)),\\ -\lambda_v(P) & \text{その他},\end{cases}$$

が成り立つ．さらに [6, Proposition6] より $-\frac{n_v}{\log q_v}\lambda_v$ の値が E の v における小平型と玉河数により定まることが示されている．よってこれらの値から α_v が定められることで上限下限が得られる．詳しくは [6, Proposition8] を見よ． □

3.4 内田の主定理の証明

ここでは定理 3.4 を命題 3.20 と，以下の命題 3.21 から示す．

命題 3.21. $m \geqq 2$ を整数とする．このとき任意の $P \in E(K_v)$ に対して

$$S_v(m) \leqq \Psi_v(P) \leqq T_v(m),$$

が成り立つ．

証明. 命題 3.17 より，任意の $P \in E(K_v) \setminus \{O\}$ に対して

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P),$$

が成り立つ．命題 3.19 の証明と同様に考えるとこの等式は $P = O$ でも成立する．$\epsilon_{m,v}$ と $\delta_{m,v}$ の定義より

$$\log \delta_{m,v} \leqq -\log \Phi_{m,v}(m^i P) \leqq \log \epsilon_{m,v},$$

が成り立つ．また，$\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} = \frac{1}{m^2-1}$ なので，

$$\begin{aligned} S_v(m) = \frac{\log \delta_{m,v}}{m^2-1} &\leqq -\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P), \\ &\leqq \frac{\log \epsilon_{m,v}}{m^2-1} = T_v(m), \end{aligned}$$

が成立する． □

定理 3.4 の証明. 命題 3.20 より

$$0 \leqq \sum_{v \in \mathrm{M}_K^0} n_v \Psi_v(P) \leqq \sum_{v \in \mathrm{M}_K^0} \left(\alpha_v + \frac{1}{6} \mathrm{ord}_v \left(\frac{\Delta}{\Delta_v^{\min}} \right) \right) \log q_v.$$

これと命題 3.21 と $h(P)-\hat{h}(P)=\frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K} n_v\Psi_v(P)$ より，

$$\begin{aligned}\frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^\infty} n_v S_v(m) \leqq & h(P)-\hat{h}(P),\\ \leqq & \frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^\infty} n_v\, T_v(m)\\ & +\frac{1}{[K:\mathbb{Q}]}\sum_{v\in \mathrm{M}_K^0}\left(\alpha_v+\frac{1}{6}\mathrm{ord}_v\left(\frac{\Delta}{\Delta_v^{\min}}\right)\right)\log q_v,\end{aligned}$$

となり，定理 3.4 が証明される． □

3.5 $S_v(m)$ の m を変化させることによる評価への影響

ここでは，$S_v(m)$ の m を変化させる，特に $\{S_v(m^i)\}_{i=1}^\infty, \{T_v(m^i)\}_{i=1}^\infty$ がそれぞれ単調増加列，単調減少列となり，さらに m を ∞ に飛ばしたとき $S_v(m), T_v(m)$ がそれぞれ $\Psi_v(P)$ の下限，上限になることを見る．

命題 3.22. $m\geqq 2$, $l\geqq 1$ を整数とする．このとき

$$S_v(m)\leqq S_v(m^l),\quad T_v(m^l)\leqq T_v(m),$$

が成り立つ．

注意 3.23. $m'|m$ ならば $S_v(m)\leqq S_v(m'), T_v(m')\leqq T_v(m)$ は必ずしも真にはならない．詳しくは [1, 9 章] を見よ．

まず次の補題を示す．

補題 3.24. $m>0$ を整数とする．このとき任意の $P\in E(K_v)$ に対して

$$\Psi_v(mP)=\log\Phi_{m,v}(P)+m^2\Psi_v(P),$$

が成り立つ．

証明. $P=(x,y)$ とおく．$m=1$ のとき，$\phi_1(X,Y)=X, \psi_1(X,Y)=1$ より

$$\begin{aligned}\Phi_{1,v}(P) &= \begin{cases}1 & (P=O),\\ \dfrac{\max\{|x(P)|_v,1\}}{\max\{1,|x(P)|_v\}^{1^2}} & (P\neq O),\end{cases}\\ &=1,\end{aligned}\tag{3.25}$$

なので，このとき成立する．

$m \geqq 2$ とする．命題 3.17 より $\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P)$ だったので

$$\begin{aligned} m^2\Psi_v(P) &= -\sum_{i=0}^{\infty} \frac{1}{m^{2i}} \log \Phi_{m,v}(m^i P), \\ &= -\log \Phi_{m,v}(P) - \sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^{i+1} P), \\ &= -\log \Phi_{m,v}(P) + \Psi_v(mP). \end{aligned}$$

よって主張が成り立つ． □

補題 3.26. m, $m' > 0$ を整数とする．このとき任意の $P \in E(K_v)$ に対して

$$\log \Phi_{mm',v}(P) = m'^2 \log \Phi_{m,v}(P) + \log \Phi_{m',v}(mP),$$

が成り立つ．

証明. 補題 3.24 より，

$$\Psi_v(mP) = \log \Phi_{m,v}(P) + m^2\Psi_v(P), \tag{3.27}$$

$$\Psi_v(mm'P) = \log \Phi_{m',v}(mP) + m'^2\Psi_v(mP), \tag{3.28}$$

$$\Psi_v(mm'P) = \log \Phi_{mm',v}(P) + (mm')^2\Psi_v(P). \tag{3.29}$$

$m'^2 \cdot (3.27) + (3.28) - (3.29)$ より求める式が得られる． □

系 3.30. $m \geqq 2, l \geqq 1$ を整数とする．このとき任意の $P \in E(K_v)$ に対して

$$\frac{1}{m^{2l}} \log \Phi_{m^l,v}(P) = \sum_{i=0}^{l-1} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P),$$

が成り立つ．

証明. 補題 3.26 より，

$$\begin{aligned} \sum_{i=0}^{l-1} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}(m^i P) &= \sum_{i=0}^{l-1} \frac{1}{m^{2(i+1)}} \left(\log \Phi_{m^{i+1},v}(P) - m^2 \log \Phi_{m^i,v}(P) \right), \\ &= \sum_{i=0}^{l-1} \left(\frac{1}{m^{2(i+1)}} \log \Phi_{m^{i+1},v}(P) - \frac{1}{m^{2i}} \log \Phi_{m^i,v}(P) \right), \\ &= \frac{1}{m^{2l}} \log \Phi_{m^l,v}(P) - \log \Phi_{1,v}(P), \\ &= \frac{1}{m^{2l}} \log \Phi_{m^l,v}(P), \quad (\Phi_{1,v}(P) = 1 \text{ より}). \end{aligned}$$

□

補題 3.24 から補題 3.26 を，補題 3.26 から系 3.30 を示してきた．系 3.30 を使い命題 3.22 を示していく．

命題 3.22 の証明. 系 3.30,

$$\frac{1}{m^{2l}}\log\Phi_{m^l,v}(P)=\sum_{i=0}^{l-1}\frac{1}{m^{2(i+1)}}\log\Phi_{m,v}(m^iP),$$

の両辺の上限を取ると，

$$\begin{aligned}\frac{\log\delta_{m^l,v}^{-1}}{m^{2l}}=\sup_{P\in E(K_v)}\frac{1}{m^{2l}}\log\Phi_{m^l,v}(P)&=\sup_{P\in E(K_v)}\left(\sum_{i=0}^{l-1}\frac{1}{m^{2(i+1)}}\log\Phi_{m,v}(m^iP)\right),\\&\leqq\sum_{i=0}^{l-1}\sup_{P\in E(K_v)}\left(\frac{1}{m^{2(i+1)}}\log\Phi_{m,v}(m^iP)\right),\\&\leqq\sum_{i=0}^{l-1}\frac{\log\delta_{m,v}^{-1}}{m^{2(i+1)}},\\&=\frac{m^{2l}-1}{m^{2l}(m^2-1)}\log\delta_{m,v}^{-1}.\end{aligned}$$

よって

$$\begin{aligned}\frac{\log\delta_{m^l,v}^{-1}}{m^{2l}-1}&\leqq\frac{\log\delta_{m,v}^{-1}}{m^2-1},\\S_v(m)=\frac{\log\delta_{m,v}}{m^2-1}&\leqq\frac{\log\delta_{m^l,v}}{m^{2l}-1}=S_v(m^l),\end{aligned}$$

となり S_v について主張が成り立つ．T_v も同様にして示せばよい. □

命題 3.31. $m\geqq 2$ を整数とする．このとき，

$$\begin{aligned}0&\leqq\inf_{P\in E(K_v)}\Psi_v(P)-S_v(m)\leqq\frac{1}{m^2-1}\left(\sup_{P\in E(K_v)}\Psi_v(P)-\inf_{P\in E(K_v)}\Psi_v(P)\right),\\0&\leqq T_v(m)-\sup_{P\in E(K_v)}\Psi_v(P)\leqq\frac{1}{m^2-1}\left(\sup_{P\in E(K_v)}\Psi_v(P)-\inf_{P\in E(K_v)}\Psi_v(P)\right),\end{aligned}$$

が成り立つ.

証明. 命題 3.21 の $S_v(m) \leqq \Psi_v(P) \leqq T_v(m)$ より $0 \leqq \inf_{P\in E(K_v)} \Psi_v(P) - S_v(m)$ が成り立つ．また，補題 3.24　$\log \Phi_{m,v}(P) = \Psi_v(mP) - m^2\Psi_v(P)$ の両辺の上限を取ると，

$$\begin{aligned}\log \delta_{m,v}^{-1} = \sup_{P\in E(K_v)} \log \Phi_{m,v}(P) &= \sup_{P\in E(K_v)} (\Psi_v(mP) - m^2\Psi_v(P)),\\ &\leqq \sup_{P\in E(K_v)} \Psi_v(mP) - \inf_{P\in E(K_v)} m^2\Phi_{m,v}(P),\\ &\leqq \sup_{P\in E(K_v)} \Psi_v(P) - m^2 \inf_{P\in E(K_v)} \Phi_{m,v}(P),\end{aligned}$$

より，

$$\begin{aligned}-S_v(m) = \frac{\log \delta_{m,v}^{-1}}{m^2-1} &\leqq \frac{1}{m^2-1}\left(\sup_{P\in E(K_v)} \Psi_v(P) - m^2 \inf_{P\in E(K_v)} \Phi_{m,v}(P)\right),\\ &= \frac{1}{m^2-1}\left(\sup_{P\in E(K_v)} \Psi_v(P) - \inf_{P\in E(K_v)} \Phi_{m,v}(P)\right) - \inf_{P\in E(K_v)} \Psi_v(P),\end{aligned}$$

よって

$$\inf_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqq \frac{1}{m^2-1}\left(\sup_{P\in E(K_v)} \Psi_v(P) - \inf_{P\in E(K_v)} \Phi_{m,v}(P)\right),$$

が成り立ち，前半が示された．後半も同様にして示される． □

系 3.32.

$$\lim_{m\to\infty} S_v(m) = \inf_{P\in E(K_v)} \Psi_v(P), \quad \lim_{m\to\infty} T_v(m) = \sup_{P\in E(K_v)} \Psi_v(P),$$

が成り立つ．

証明. 命題 3.19 より Ψ_v は $E(K_v)$ で有界なので，命題 3.31 より従う． □

系 3.33. $m \geqq 2$ を整数とする．このとき，

$$\begin{aligned}0 &\leqq \inf_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqq \frac{1}{m^2}(T_v(m) - S_v(m)),\\ 0 &\leqq T_v(m) - \sup_{P\in E(K_v)} \Psi_v(P) \leqq \frac{1}{m^2}(T_v(m) - S_v(m)),\end{aligned}$$

が成り立つ．

証明. 命題 3.31 より

$$m^2 \inf_{P\in E(K_v)} \Psi_v(P) - (m^2-1)S_v(m) \leqq \sup_{P\in E(K_v)} \Psi_v(P),$$

したがって

$$m^2 \inf_{P\in E(K_v)} \Psi_v(P) - m^2 S_v(m) \leqq \sup_{P\in E(K_v)} \Psi_v(P) - S_v(m),$$

系 3.32 の $\lim_{m\to\infty} T_v(m) = \sup_{P\in E(K_v)} \Psi_v(P)$ と命題 3.21 の $S_v(m) \leqq \Psi_v(P) \leqq T_v(m)$ より $\sup_{P\in E(K_v)} \Psi_v(P) \leqq T_v(m)$ なので,

$$\sup_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqq T_v(m) - S_v(m),$$

となる．よって前半が示された．後半も同様にして示される． □

注意 3.34. 系 3.32 より，理論上は m を大きくすることで Ψ_v の上限，下限に T_v, S_v をいくらでも近づけられることがわかる．さらに系 3.33 より $S_v(m), T_v(m)$ と $\Psi_v(P)$ の上限下限の差がどれくらいになるのかを実際に計算することができる．

3.6 S_v, T_v の計算方について

$v \in \mathrm{M}_K^0$ の場合は Tate のアルゴリズムで E の v での小平型，玉河数 $c_v, \Delta_v^{\min}$ を求めれば表から α_v を求めることができる．詳しくは [3, 4 章§ 9] を見よ

$v \in \mathrm{M}_K^\infty$ とする．この時，$S_v(m), T_v(m)$ を計算することができればいい．v が複素素点の場合は [6, 8 章，9 章] の場合と同様にして計算する．v が実素点の場合について解説する．

$$S_v(m) = \frac{\log \delta_{m,v}}{m^2-1}, \quad T_v(m) = \frac{\log \epsilon_{m,v}}{m^2-1},$$

$$\delta_{m,v}^{-1} = \sup_{P\in E(K_v)} \Phi_{m,v}(P), \quad \epsilon_{m,v}^{-1} = \inf_{P\in E(K_v)} \Phi_{m,v}(P),$$

なので，$\Phi_{m,v}$ の像を考える．$P = (x, y) \neq O$ とすると $\Phi_{m,v} = \frac{\max\{|\phi_m(x)|_v, |\psi_m^2(x)|_v\}}{\max\{1, |x|_v\}^{m^2}}$ なので,

$$\Phi_{m,v}(P) = \begin{cases} \max\{|\phi_m(x)|_v, |\psi_m^2(x)|_v\} & (|x|_v \leqq 1), \\ \max\left\{ \left|\frac{\phi_m(x)}{x^{m^2}}\right|_v, \left|\frac{\psi_m^2(x)}{x^{m^2}}\right|_v \right\} & (|x|_v > 1), \end{cases} \tag{3.35}$$

と表わされる．さらに，$p(x) = 4x^3 + b_2x^2 + 2b_4x + b_6 = \psi_2^2(x)$，$P(x) = x^4 p(\frac{1}{x})$ として，$D = \{x \in [-1, 1] | p(x) \geqq 0\}, D' = \{x \in [-1, 1] | P(x) \geqq 0\}$ とおくと，以下が成り立つ．

命題 3.36. $P=(x,y)\in E(K_v)$ ならば $x\in D$ 又は $\frac{1}{x}\in D'$ が成り立つ．逆に $x\in D$ 又は $\frac{1}{x}\in D'$ ならばある y が存在して

$$E(K_v)\ni\begin{cases}(x,y) & (x\in D\text{ の場合}),\\ \left(\dfrac{1}{x},y\right) & \left(\dfrac{1}{x}\in D'\text{の場合}\right),\end{cases}$$

となる．

証明. $(x,\ y)\in E(K_v)$ とすると，

$$\begin{aligned}p(x)&=4x^3+b_2x^2+2b_4x+b_6,\\&=4x^3+(a_1^2+4a_2)x^2+2(2a_4+a_1a_3)x+(a_3^2+4a_6),\\&=4(x^3+a_2x^2+a_4x+a_6)+a_1^2x^2+a_3^2+2a_1a_3x,\\&=4(y^2+a_1xy+a_3y)+a_1^2x^2+a_3^2+2a_1a_3x,\\&=(2y+a_1x+a_3)^2.\end{aligned}$$

よって，

$$(x,y)\in E(K_v)\Rightarrow p(x)\geqq 0, \tag{3.37}$$

となり，また，

$$p(x)\geqq 0\Rightarrow\text{ある }y\text{ が存在して }(x,y)\in E(K_v) \tag{3.38}$$

が成り立つ．

$P=(x,y)\in E(K_v)$ とする．まず $|x|_v\leqq 1$ とすると，(3.37) より $x\in D$ となる．$|x|_v>1$ のとき，$\frac{1}{x}\leqq 1$ で，(3.37) より

$$P\left(\frac{1}{x}\right)=\left(\frac{1}{x}\right)^4 p(x)\geqq 0.$$

よって $\frac{1}{x}\in D'$ となり， 前半が示された．

$x\in D$ とすると (3.38) よりある y が存在して $(x,y)\in E(K_v)$ となる．$\frac{1}{x}\in D'$ とすると，

$$0\leqq P(x)=x^4p\left(\frac{1}{x}\right),$$

より $0\leqq p(\frac{1}{x})$ となるので，$x'=\frac{1}{x}$ と置けば (3.38) よりある y' が存在して $(x',y')\in E(K_v)$ が成り立つ．以上から命題が示された． □

よって (3.35)，命題 3.36 より

$$\begin{aligned}
\delta_{m,v}^{-1} &= \sup_{P\in E(K_v)} \Phi_{m,v}(P), \\
&= \max\left\{ \sup_{x\in D} \max\left\{|\phi_m(x)|_v, |\psi_m^2(x)|_v\right\}, \sup_{x\in D'} \max\left\{ \left| x^{m^2}\phi_m\left(\frac{1}{x}\right)\right|_v, \left| x^{m^2}\psi_m^2\left(\frac{1}{x}\right)\right|_v \right\}\right\}, \\
\epsilon_{m,v}^{-1} &= \inf_{P\in E(K_v)} \Phi_{m,v}(P), \\
&= \min\left\{ \inf_{x\in D} \max\left\{|\phi_m(x)|_v, |\psi_m^2(x)|_v\right\}, \inf_{x\in D'} \max\left\{ \left| x^{m^2}\phi_m\left(\frac{1}{x}\right)\right|_v, \left| x^{m^2}\psi_m^2\left(\frac{1}{x}\right)\right|_v \right\}\right\},
\end{aligned}$$

と書ける．ここで定義より D, D' は有限個の閉区間の和集合なので $\delta_{m,v}, \epsilon_{m,v}$ を計算することができる．

3.7 アルキメデス的な素点について考察している論文

v が非アルキメデス的な場合は命題 3.20 よりすでに上限下限がわかっているので，関連の論文で v がアルキメデス的な場合を考察しているものを少し紹介する．ここでは E を $\mathbb{C}$ 上の楕円曲線で，

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

で与えられるものとする．

J．S．Müller，Corinna Stumpe の論文 [10] では次の方法を紹介している．ここでの h，$\hat{h}$ はそれぞれ [10] での通常高さ関数，標準高さ関数を表すとする．

E を楕円曲線とし，$T_1, T_2, T_3 \in E$ を自明でない互いに異なる 2 捩れ点とする．まず，$i = 1, 2, 3$ に対し $a_{1,i}, a_{2,i}, b_{i,1}, b_{i,2}$ をそれぞれ

$$a_{1,i} = \frac{2x(T_j)x(T_k) - \frac{b_4}{2}}{2(x(T_i) - x(T_j))(x(T_i) - x(T_k))}, \quad a_{2,i} = \frac{-1}{2(x(T_i) - x(T_j))(x(T_i) - x(T_k))},$$

$$b_{i,1} = 1, \quad b_{i,2} = -x(T_i),$$

とする．ただし $j, k \in \{1, 2, 3\}$ で，i, j, k は互いに異なるとする．系 2.13 より上のような

T_1, T_2, T_3 が取れることに注意せよ．次に $\varphi : \mathbb{R}^2_{\geqq 0} \to \mathbb{R}^2_{\geqq 0}$ を

$$(d_1, d_2) \mapsto (\varphi_1(d_1, d_2), \varphi_2(d_1, d_2)) = \left(\sqrt{\sum_{j=1}^{3} |a_{i,j}| \sqrt{|b_{j,1}| d_1 + |b_{j,2}| d_2}} \right)_{i=1,2},$$
$$= \left(\sqrt{\sum_{j=1}^{3} |a_{1,j}| \sqrt{|b_{j,1}| d_1 + |b_{j,2}| d_2}}, \sqrt{\sum_{j=1}^{3} |a_{2,j}| \sqrt{|b_{j,1}| d_1 + |b_{j,2}| d_2}} \right),$$

で定める．ただし $P \in K^2$ に対し，P_i は P の第 i 成分 $(i = 1, 2)$ とする．$\| \cdot \|$ を，K 上の 2 次元ベクトル (x_1, x_2) に対し $\|(x_1, x_2)\| = \max\{|x_1|, |x_2|\}$ で定義して，

$$c_N := \frac{4^N}{4^N - 1} \log(\|\varphi^{\circ N}(1, 1)\|)$$

とおく．ただし $\varphi^{\circ N}(1, 1)$ は $(1, 1)$ を φ で N 回写したものとする．次が [10] の主定理である．

定理 3.39. $\{c_N\}_{N \geqq 1}$ は単調減少列で，任意の $N \geqq 1$ に対し，

$$\max_{P \in E(\mathbb{C})} \{\Psi_v(P)\} \leqq c_N,$$

が成り立つ．

次の命題を使い定理 3.39 を示す．

命題 3.40. $\kappa : E \to \mathbb{P}^1$ を

$$P \mapsto \begin{cases} (1, 0) & P = O, \\ (x(P), 1) & P \neq O, \text{ただし } x(P) \text{ は } P \text{ の } x \text{ 座標とする}, \end{cases}$$

とし，$P \in E$，$\kappa(P) = (x_1, x_2)$ としたとき $\kappa(2P) = \delta(x_1, x_2) = (\delta_1(x_1, x_2), \delta_2(x_1, x_2))$ を，

$$\delta_1(x_1, x_2) = x_1^4 - b_4 x_1^2 x_2^2 - 2b_6 x_1 x_2^3 - b_8 x_2^4,$$
$$\delta_2(x_1, x_2) = 4x_1^3 x_2 + b_2 x_1^2 x_2^2 + 2b_4 x_1 x_2^3 + b_6 x_2^4,$$

とする．このとき E にのみ依存する二次形式 $y_1, y_2, y_3 \in K[x_1, x_2]$ と $i = 1, 2, j = 1, 2, 3, k = 1, 2$ に対し上で定めた定数 $a_{i,j}, b_{j,k} \in K$ について，

$$x_i^2 = \sum_{j=1}^{3} a_{i,j} y_j(x_1, x_2), \quad y_j(x_1, x_2)^2 = \sum_{k=1}^{2} b_{j,k} \delta_k(x_1, x_2) \in K[x_1, x_2],$$

が成り立つ．

証明. $T \in E[2] \setminus \{O\}$ に対し行列 M_T を

$$M_T := \begin{pmatrix} x(T) & f'(x(T)) - x(T)^2 \\ 1 & -x(T) \end{pmatrix},$$

$M_O := E_2$ とおく．ただし $f = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$ とする．このとき M_T で表される写像 $m_T : \mathbb{P}^1 \to \mathbb{P}^1$ は，$T \in E[2]$ を足すことで得られる E の平行移動 $+_T : E \ni P \mapsto P + T \in E$ に対し，

$$\kappa \circ +_T = m_T \circ \kappa$$

が成り立つということが [10] で述べられている．この M_T に対し，$\gamma_T \in K^*$ を $\gamma_T^2 = \det(M_T)^{-1}$ とおいて $\tilde{M}_T := \gamma_T M_T$ とする．

$$G_E := \left\{ \pm \tilde{M}_T | T \in E[2] \right\}$$

とおくと，$G_E \subset SL_2(K)$ が $SL_2(K)$ の部分群となる事が [10, Lemma2.2, Lemma2.3] で示されている．

V を，x_1, x_2 における K 線形形式全体からなるベクトル空間とする．ρ を，G_E の元を $\mathbb{P}^1$ 上の線形写像として見た時の，V の元との合成による作用での表現とする．ρ^2 を，$T \in G_E$ に対し $\rho(T)$ から導かれる $\mathrm{Sym}(V)$ での写像，つまり $T \in G_E, f, g \in V, fg \in \mathrm{Sym}^2(V)$ に対して $\rho^2(T)(fg) := (\rho(T)f)(\rho(T)g) \in \mathrm{Sym}^2(V)$ となる表現とすれば，ρ^2 は $E[2]$ の $\mathrm{Sym}^2(V)$ 上の表現としてみなせて

$$\rho^2 = \bigoplus_{T \in E[2] \setminus \{O\}} e_2(\cdot, T),$$

が成り立つ．ここで，$e_2 : E[2] \times E[2] \to \{\pm 1\}$ は Weil pairing，つまり $T, T' \in E[2] \setminus \{O\}$ に対し

$$e_2(T, T') = \begin{cases} 1 & (T = T'), \\ -1 & (T \neq T'), \end{cases}$$

となり，$T = O$ 又は $T' = O$ の場合 $e_2(T, T') = 1$ となるものとする．$i = 1, 2, 3$ に対し，$E[2] \setminus \{O\}$ の点に番号を付ける．y_i を $T_i \in E[2] \setminus \{O\}$ の $e_2(\cdot, T_i)$ の部分に対応する部分空間を生成する斉次式とすると y_1, y_2, y_3 が $\mathrm{Sym}^2(V)$ の基底となるので，$x_1^2, x_2^2 \in \mathrm{Sym}^2(V)$ を y_1, y_2, y_3 で表すことができ，よって $a_{i,j}$ が定まる．

また，ρ^2 と同様に ρ^4 を作ると，$\delta(\tilde{M}_T(x_1, x_2)) = \delta(\gamma_T M_T(x_1, x_2)) = \delta(x_1, x_2) \in \mathbb{P}^1$ なので，斉次式 δ_1, δ_2 は ρ^4 で $E[2]$ 不変である．さらに，δ_1, δ_2 は線形独立で，$E[2]$ 不変な 4 次斉次式の空間が 2 次元なので，δ_1, δ_2 がその基底となる．よって y_j を δ_1, δ_2 で表すことができ，$b_{j,k}$ が定まる．詳細は [10] を見よ． □

等分多項式の形と命題 3.6，命題 3.7 より δ を上のように x_1, x_2 を使って表される事に注意せよ．

定理 3.39 の証明. まず任意の $N \geqq 1$ に対し $\max_{P\in E(\mathbb{C})}\{\Psi_v(P)\} \leqq c_N$ を示す．$P \in E(\mathbb{C}), \kappa(P) = (x_1, x_2) = x$ とおき，$N \geqq 1$ とする．まず，

$$|x_i| \leqq \varphi^{\circ N}(|\delta_1^{\circ N}(x)|, |\delta_2^{\circ N}(x)|)_i, \tag{3.41}$$

を示す．$N = 1$ のとき，命題 3.40 より

$$|x_i| \leqq \sqrt{\sum_{j=1}^{3} |a_{ij}||y_j|} \leqq \sqrt{\sum_{j=1}^{3} |a_{ij}|\sqrt{|b_{j1}||\delta_1| + |b_{j2}||\delta_2|}} = \varphi(|\delta_1(x)|, |\delta_2(x)|)_i.$$

また，$N \geqq 2$ に対し $(\delta_1^{\circ N-1}(x), \delta_2^{\circ N-1}(x)) = \kappa(2^{N-1}P)$ より，$\delta_i^{\circ N-1}(x)$ に上を適用すると $|\delta_i^{\circ N-1}(x)| \leqq \varphi(|\delta_1^{\circ N}(x)|, |\delta_2^{\circ N}(x)|)_i$ となる．φ は斉次式からなり，φ の係数・φ に代入する数がいずれも非負であることから，

$\varphi^{\circ N-1}(|\delta_1^{\circ N-1}(x)|, |\delta_2^{\circ N-1}(x)|)_i \leqq \varphi^{\circ N}(|\delta_1^{\circ N}(x)|, |\delta_2^{\circ N}(x)|)_i$, となる．よって任意の $N \geqq 1$ に対し (3.41) が成り立つ．次に

$$|\delta^{\circ N}(x_1, x_2)_i| \leqq \varphi(1,1)_i \left\|\delta^{\circ N+1}(x_1, x_2)\right\|^{\frac{1}{4}}, \tag{3.42}$$

を示す．$\alpha = (\alpha_1, \alpha_2)$ をある点 $Q \in E$ に対し $\kappa(Q) = (\alpha_1, \alpha_2)$ となるものとすると命題 3.40 より

$$\begin{aligned} |\alpha_i| &\leqq \sqrt{\sum_{j=1}^{3} |a_{i,j}|\sqrt{|b_{j,1}|\delta_1 + |b_{j,2}|\delta_2}}, \\ &\leqq \sqrt{\sum_{j=1}^{3} |a_{i,j}|\sqrt{(|b_{j,1}| + |b_{j,2}|)\|\delta(\alpha)\|}}, \\ &= \sqrt{\sum_{j=1}^{3} |a_{i,j}|\sqrt{|b_{j,1}| + |b_{j,2}|}\|\delta(\alpha)\|^{\frac{1}{4}}} = \varphi(1,1)_i \left\|\delta(\alpha)\right\|^{\frac{1}{4}}. \end{aligned} \tag{3.43}$$

よって，$\alpha = \delta^{\circ N}(x_1, x_2)$ とおけば (3.42) が示される．(3.41)，(3.42)，前述した φ の性質より，

$$|x_i| \leqq \varphi^{\circ N}(|\delta_1^{\circ N}(x)|, |\delta_2^{\circ N}(x)|)_i \leqq \varphi^{\circ N}(\|\delta^{\circ (N+1)}(x)\|^{\frac{1}{4}}\varphi(1,1))_i,$$

が導かれる．φ は $\frac{1}{4}$ 次の斉次式からなるので，定数を前に出して $N+1$ を N と書くと

$$|x_i| \leqq \|\delta^{\circ N}(x)\|^{\frac{1}{4^N}} \varphi^{\circ N}(1,1)_i, \tag{3.44}$$

が得られる．この時 (3.43) より (3.44) は $N=1$ でも成り立つ．ここで x を改めて $x = k(2^{Nn}P) = \delta^{\circ Nn}(x_1, x_2)$ と置き，これを (3.44) に代入すると

$$\|\delta^{\circ Nn}(x_1,x_2)\| \leqq \|\delta^{\circ N(n+1)}(x_1,x_2)\|^{\frac{1}{4^N}} \|\varphi^{\circ N}(1,1)\|,$$

となり，これより

$$\frac{\|\delta^{\circ Nn}(x_1,x_2)\|}{\|\delta^{\circ N(n+1)}(x_1,x_2)\|^{\frac{1}{4^N}}} \leqq \|\varphi^{\circ N}(1,1)\|, \tag{3.45}$$

が得られる．最後に

$$\Psi_v(P) = \sum_{n=0}^{\infty} \frac{1}{4^{Nn}} \log \frac{\|\delta^{\circ Nn}(x_1,x_2)\|}{\|\delta^{\circ N(n+1)}(x_1,x_2)\|^{\frac{1}{4^N}}}, \tag{3.46}$$

を示せば，(3.45) より

$$\Psi_v(P) \leqq \sum_{n=0}^{\infty} \frac{1}{4^{Nn}} \log \|\varphi^{\circ N}(1,1)\| = \frac{4^N}{4^N-1} \log \|\varphi^{\circ N}(1,1)\|,$$

となり定理 3.39 の後半が示される．

$P \neq O$ のとき ϕ_2, ψ_2, δ の定義と $x_1 = x(P), x_2 = 1$ より，

$$\Phi_{2,v}(P) = \frac{\max\{|\phi_2(x(P))|_v, |\psi_2^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^4} = \frac{\max\{|\delta_1(x_1,x_2)|, |\delta_2(x_1,x_2)|\}}{\max\{x_1,x_2\}^4} = \frac{\|\delta(x_1,x_2)\|}{\|\kappa(P)\|^4},$$

$P = O$ のとき $x_1 = 1, x_2 = 0$ より $\frac{\|\delta(x_1,x_2)\|}{\|\kappa(P)\|^4} = \frac{\delta_1(1,0)}{x_1^4} = 1 = \Phi_{2,v}(O)$ より任意の $P \in E$ に対し $\Phi_{2,v}(P) = \frac{\|\delta(x_1,x_2)\|}{\|\kappa(P)\|^4}$ と表わされる．特に，計算すると $\Phi_{2,v}(2^nP) = \frac{\|\delta^{\circ n+1}(P)\|}{\|\delta^{\circ n}(P)\|^4}$ となるので，

$$\begin{aligned}
\Psi_v(P) &= -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_{2,v}(2^nP), \\
&= -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \frac{\|\delta^{\circ n+1}(P)\|}{\|\delta^{\circ n}(P)\|^4}, \\
&= \sum_{n=0}^{\infty} \frac{1}{4^n} \log \frac{\|\delta^{\circ n}(P)\|}{\|\delta^{\circ n+1}(P)\|^{\frac{1}{4}}}, \quad \left(-\frac{1}{4}\text{を log の中に入れた}\right).
\end{aligned}$$

が成り立つ．よって，$l=0,1,2,\cdots$ とすると

$$\begin{aligned}\Psi_v(P)=&\cdots+\frac{1}{4^{Nl}}\log\frac{\|\delta^{\circ Nl}(P)\|}{\|\delta^{\circ Nl+1}(P)\|^{\frac{1}{4}}}+\frac{1}{4^{Nl+1}}\log\frac{\|\delta^{\circ Nl+1}(P)\|}{\|\delta^{\circ Nl+2}(P)\|^{\frac{1}{4}}}+\cdots\\&\qquad+\frac{1}{4^{N(l+1)-1}}\log\frac{\|\delta^{\circ N(l+1)-1}(P)\|}{\|\delta^{\circ N(l+1)}(P)\|^{\frac{1}{4}}}+\cdots,\\=&\cdots+\frac{1}{4^{Nl}}\left\{\log\frac{\|\delta^{\circ Nl}(P)\|}{\|\delta^{\circ Nl+1}(P)\|^{\frac{1}{4}}}+\log\frac{\|\delta^{\circ Nl+1}(P)\|^{\frac{1}{4}}}{\|\delta^{\circ Nl+2}(P)\|^{\frac{1}{4^2}}}+\cdots\right.\\&\qquad\left.+\log\frac{\|\delta^{\circ N(l+1)-1}(P)\|^{\frac{1}{4^{N-1}}}}{\|\delta^{\circ N(l+1)}(P)\|^{\frac{1}{4^N}}}\right\}+\cdots,\\=&\cdots+\frac{1}{4^{Nl}}\log\frac{\|\delta^{\circ Nl}(P)\|}{\|\delta^{\circ N(l+1)}(P)\|^{\frac{1}{4^N}}}+\cdots,\end{aligned}$$

よって，(3.46) が示され，定理 3.39 の後半が示された．

次に $\{c_N\}_{N\geqq 1}$ が単調減少列となる事を示していく．$\vartheta:\mathbb{R}^2\to\mathbb{R}^2$ を

$$\begin{aligned}\alpha=(\alpha_1,\alpha_2)\mapsto&(\vartheta_1(\alpha),\vartheta_2(\alpha))=(\log(\varphi(\exp\alpha_1,\exp\alpha_2)_i))_{i=1,2},\\&=\left(\log\sqrt{\sum_{j=1}^{3}|a_{i,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}}\right)_{i=1,2},\end{aligned}$$

で定義する．このとき，ϑ の Jacobi 行列の成分を計算すると，$k,l\in\{1,2\}$ について，

$$\begin{aligned}&\frac{\partial\vartheta_k}{\partial\alpha_l}\\&=\frac{1}{4\left(\sum_{j=1}^{3}|a_{k,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}\right)}\cdot\left(\sum_{j=1}^{3}\frac{|a_{k,j}||b_{j,l}|\exp\alpha_l}{\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}}\right),\\&\geqq 0.\end{aligned}$$

よって，計算すると

$$\begin{aligned}&\frac{\partial\vartheta_k}{\partial\alpha_1}+\frac{\partial\vartheta_k}{\partial\alpha_2}\\&=\frac{1}{4\left(\sum_{j=1}^{3}|a_{k,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}\right)}\\&\cdot\left(\sum_{j=1}^{3}\frac{|a_{k,j}||b_{j,1}|\exp\alpha_1}{\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}}+\sum_{j=1}^{3}\frac{|a_{k,j}||b_{j,2}|\exp\alpha_2}{\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}}\right),\end{aligned}$$

$$= \frac{1}{4\left(\sum_{j=1}^{3}|a_{k,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}\right)}\cdot\left(\sum_{j=1}^{3}\frac{|a_{k,j}|(|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2)}{\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}}\right),$$
$$= \frac{1}{4\left(\sum_{j=1}^{3}|a_{k,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}\right)}\cdot\left(\sum_{j=1}^{3}|a_{k,j}|\sqrt{|b_{j,1}|\exp\alpha_1+|b_{j,2}|\exp\alpha_2}\right),$$
$$= \frac{1}{4},$$

となる．よって ϑ を $\alpha,\beta\in\mathbb{R}^2$ に対しテーラー展開することで，

$$\begin{aligned}\vartheta_k(\alpha) &= \vartheta_k(\beta)+(\alpha_1-\beta_1)\frac{\partial\vartheta_k}{\partial\alpha_1}(\beta)+(\alpha_2-\beta_2)\frac{\partial\vartheta_k}{\partial\alpha_2}(\beta)\\ &\qquad+\sum_{n=2}^{\infty}\frac{1}{n!}\left\{(\alpha_1-\beta_1)\frac{\partial}{\partial\alpha_1}+(\alpha_2-\beta_2)\frac{\partial}{\partial\alpha_2}\right\}^n\vartheta_k(\beta),\\ |\vartheta_k(\alpha)-\vartheta_k(\beta)| &\leqq |\alpha_1-\beta_1|\left|\frac{\partial\vartheta_k}{\partial\alpha_1}(\beta)\right|+|\alpha_2-\beta_2|\left|\frac{\partial\vartheta_k}{\partial\alpha_2}(\beta)\right|\\ &\qquad+\sum_{n=2}^{\infty}\frac{1}{n!}\left|\left\{|\alpha_1-\beta_1|\frac{\partial}{\partial\alpha_1}+|\alpha_2-\beta_2|\frac{\partial}{\partial\alpha_2}\right\}^n\vartheta_k(\beta)\right|,\end{aligned}$$

$\frac{\partial\vartheta_k}{\partial\alpha_l}\geqq 0, \frac{\partial\vartheta_k}{\partial\alpha_1}+\frac{\partial\vartheta_k}{\partial\alpha_2}=\frac{1}{4}$ となる事と，$n\geqq 2$ に対し $(\frac{\partial}{\partial\alpha_1}+\frac{\partial}{\partial\alpha_2})^n\vartheta_k=0$ となる事から，

$$\begin{aligned}|\vartheta_k(\alpha)+\vartheta_k(\beta)| &\leqq |\alpha_1-\beta_1|\frac{\partial\vartheta_k}{\partial\alpha_1}(\beta)+|\alpha_2-\beta_2|\frac{\partial\vartheta_k}{\partial\alpha_2}(\beta)\\ &\qquad+\sum_{n=2}^{\infty}\frac{1}{n!}\left|\left\{|\alpha_1-\beta_1|\frac{\partial}{\partial\alpha_1}+|\alpha_2-\beta_2|\frac{\partial}{\partial\alpha_2}\right\}^n\vartheta_k(\beta)\right|,\\ &\leqq \|\alpha-\beta\|\left(\frac{\partial\vartheta_k}{\partial\alpha_1}(\beta)+\frac{\partial\vartheta_k}{\partial\alpha_2}(\beta)\right)+\sum_{n=2}^{\infty}\frac{1}{n!}\|\alpha-\beta\|\left|\left(\frac{\partial}{\partial\alpha_1}+\frac{\partial}{\partial\alpha_2}\right)^n\vartheta_k(\beta)\right|,\\ &= \|\alpha-\beta\|\frac{1}{4}.\end{aligned}$$

これより

$$\|\vartheta(\alpha)-\vartheta(\beta)\|\leqq\frac{1}{4}\|\alpha-\beta\|, \tag{3.47}$$

が得られる．ϑ の定義より任意の $N\geqq 1$ に対し $c_N=\frac{4^N}{4^N-1}\|\vartheta^{\circ N}(0,0)\|$ が成り立つ $(\vartheta_i(0,0)=\log\varphi_i(\exp 0,\exp 0)=\log\varphi_i(1,1)$ より $c_1=\frac{4}{3}\log\|\varphi(1,1)\|=\frac{4}{3}\|\vartheta(0,0)\|$ が成り立つ．$N\geqq 1$ について $\vartheta_i^{\circ N}(0,0)=\log\varphi_i^{\circ N}(1,1)$ が成り立つとすると，$\vartheta_i^{\circ N+1}(0,0) = \vartheta_i(\vartheta^{\circ N}(0,0)) = \log\varphi_i(\exp\log\varphi_1^{\circ N}(1,1),\exp\log\varphi_2^{\circ N}(1,1)) =$

$\log\varphi_i(\varphi_1^{\circ N}(1,1),\varphi_2^{\circ N}(1,1)) = \log\varphi_i^{\circ N+1}(1,1)$ となる．よって数学的帰納法より任意の $N \geqq 1$ に対し $c_N = \frac{4^N}{4^N-1}\|\vartheta^{\circ N}(0,0)\|$ が成り立つ).

$e_N := \|\vartheta^{\circ N}(0,0)\|$ とおく．$N \geqq 1$ に関する帰納法で $\{c_N\}_{N\geqq 1}$ が単調減少列となる事を示していく．(3.47) より

$$e_2 - e_1 \leqq \|\vartheta^{\circ 2}(0,0) - \vartheta(0,0)\| \leqq \frac{1}{4}\|\vartheta(0,0)\| = \frac{1}{4}e_1,$$

なので $c_2 \leqq c_1$ が成り立つ．$N \geqq 2$ として，$c_N \leqq c_{N-1}$ が成り立つとする．

この時，$e_{N+1} \leqq e_N$ ならば $\frac{4^{N+1}}{4^{N+1}-1} \leqq \frac{4^N}{4^N-1}$ より $c_{N+1} \leqq c_N$ が成り立つので $e_{N+1} \geqq e_N$ とする．

(3.47) を $\alpha = \vartheta^{\circ N}(0,0), \beta = \vartheta^{\circ N-1}(0,0)$ で適用すると，

$$\|\vartheta^{\circ N+1}(0,0) - \vartheta^{\circ N}(0,0)\| \leqq \frac{1}{4}\|\vartheta^{\circ N}(0,0) - \vartheta^{\circ N-1}(0,0)\|,$$

ここで，$F(\alpha_1,\alpha_2) = \vartheta_1(\alpha_1,\alpha_2) - \vartheta_2(\alpha_1,\alpha_2)$ とおいて，(3.47) と同様に計算すると，$\frac{\partial F}{\partial\alpha_1} + \frac{\partial F}{\partial\alpha_2} = 0$ なので，任意の $\alpha,\beta \in \mathbb{R}^2$ に対し $|F(\alpha) - F(\beta)| \leqq 0$ が成り立つ．F は明らかに連続な実数値関数なので，F は定数関数となる．よって，任意の $N \geqq 1$ に対し $\vartheta_1^{\circ N}(0,0) \leqq \vartheta_2^{\circ N}(0,0)$ 又は $\vartheta_1^{\circ N}(0,0) \geqq \vartheta_2^{\circ N}(0,0)$ のどちらか一方が成り立ち (つまり $\{e_N\} = \{\vartheta_2^{\circ N}(0,0)\}_N$ 又は $\{e_N\} = \{\vartheta_1^{\circ N}(0,0)\}_N$ が成り立つ)，さらに $\vartheta_1^{\circ N+1}(0,0) - \vartheta_1^{\circ N}(0,0) = \vartheta_2^{\circ N+1}(0,0) - \vartheta_2^{\circ N}(0,0)$ なので $\|\vartheta^{N+1}(0,0) - \vartheta^N(0,0)\| = |e_{N+1} - e_N|$ が成り立つ．以上から

$$e_{N+1} - e_N \leqq \frac{1}{4}|e_N - e_{N-1}|,$$

が成り立つ．まず $e_N \geqq e_{N-1}$ の時を示す．帰納法の仮定より $\frac{4^N}{4^N-1}e_N = c_N \leqq c_{N-1} = \frac{4^{N-1}}{4^{N-1}-1}e_{N-1}$ が成り立つので，これより $-\frac{1}{4}e_{N-1} \leqq -\frac{4^{N-1}-1}{4^N-1}e_N$ が導かれる．これを上の式に使って，

$$\begin{aligned}
e_{N+1} - e_N &\leqq \frac{1}{4}e_N - \frac{1}{4}e_{N-1} \leqq \frac{1}{4}e_N - \frac{4^{N-1}-1}{4^N-1}e_N,\\
e_{N+1} &\leqq \frac{5}{4}e_N - \frac{4^{N-1}-1}{4^N-1}e_N = \frac{4^{N+1}-1}{4^{N+1}-4}e_N,\\
\frac{1}{4^{N+1}-1}e_{N+1} &\leqq \frac{1}{4^{N+1}-4}e_N,\\
c_{N+1} = \frac{4^{N+1}}{4^{N+1}-1}e_{N+1} &\leqq \frac{4^N}{4^N-1}e_N = c_N,
\end{aligned}$$

$e_N \leqq e_{N-1}$ の時も同様にして示される．以上から $\{c_N\}$ が単調減少であることが示された．□

注意 3.48. [10, Theorem4.2] における $\{c_N\}_{N\geqq 1}$ が単調減少列となる事についての証明では，$e_N \leqq e_{N-1}$ の場合も同様にして示されるとあるが，きちんと示すことができなかった．

ここで，$l=1,2$ について $\frac{\partial \vartheta_k}{\partial \alpha_l} \geqq 0$ であったので，もし $i=1,2$ に対し $\varphi_i(0,0) \geqq 0$ であったら $\vartheta_i^{\circ 2}(0,0) \geqq \vartheta_i(0,0) \geqq 0$ となり，同様の操作を繰り返すことで任意の $N \geqq 1$ に対して $\vartheta_i^{\circ N+1}(0,0) \geqq \vartheta_i^{\circ N}(0,0) \geqq 0, (i=1,2)$ が示される．この時 $i=1,2$ について $\vartheta_i^{\circ N}(0,0) \geqq 0$ であり $\{\vartheta_i^{\circ N}(0,0)\}_N$ が単調増加列となる．よって $\{e_N\}_N$ が単調増加列となるので，この時 $\{c_N\}_N$ が単調減少であることが示される．

(3.42) より任意の $(x_1,x_2)=\kappa(P), P\in E$ に対し $\frac{|x_i|}{\|\delta(x_1,x_2)\|^{\frac{1}{4}}} \leqq \varphi(1,1)_i$ が成り立つので，$P=O$ とおくと $\kappa(O)=(1,0), \|\delta(1,0)\|=1$ より $\frac{|x_1|}{\|\delta(x_1,x_2)_1\|^{\frac{1}{4}}}=1 \leqq \varphi_1(1,1)$ となる．よって，$\vartheta_1(0,0)=\log\varphi_1(1,1)\geqq 0$ となる．$\vartheta_1(0,0)\geqq 0$ は容易に示されるが，この方法での評価では $\vartheta_2(0,0)\geqq 0$ の場合は簡単には示されない．$P=O$ とすると，同様にして $\frac{|x_2|}{\|\delta(x_1,x_2)\|^{\frac{1}{4}}}=0 \leqq \varphi(1,1)_2$ となり，また，$P\neq O$ とすると，$\kappa(P)=(x(P),1)$ であり，この時 $\frac{|x_2|}{\|\delta(x_1,x_2)\|^{\frac{1}{4}}}=\frac{1}{\|\delta(x(P),1)\|^{\frac{1}{4}}} \leqq \varphi_2(1,1)$ となる．よって，$1\leqq \frac{1}{\|\delta(x(P),1)\|^{\frac{1}{4}}}$，つまり $\max\{|\delta_1(x(P),1)|, |\delta_2(x(P),1)|\} \leqq 1$ となる $P\neq O$ を取ってくることができれば $\vartheta_2(0,0)=\log\varphi(1,1)\geqq 1$ が示される．

以上をまとめると，楕円曲線 $E/\mathbb{C}$ が $\max\{|\delta_1(x(P),1)|, |\delta_2(x(P),1)|\} \leqq 1$ となる点 $P\in E\setminus\{O\}$ を持てば $\{c_N\}_N$ は単調減少列となる．

ただ，$c_2 \leqq c_1$ は示されており，さらに例 3.49 を見ると J．E．Cremona，M．Prickett，S．Siksek[6] の評価と比較してかなり良い結果が実際に得られている．よって，たとえ $\{c_N\}$ が単調減少でなくともこの方法で以前のものより良い評価が得られることがわかる．

[10] の方法は，計算時間が短いという利点がある．例えば，この評価と同様に数列になっている内田 [1] の評価と比較すると，[10] の方法では，最初に捩れ点を見つけて $a_{i,j}, b_{j,k}$ などを計算するなどの準備が必要だが，その後はほとんど実数値関数に値を代入するだけで評価が得られる．しかし，内田の方法では N ごとの評価を得るためには毎回閉区間での多項式の上限・下限を求めなければならない (詳細は 3.6 節を見よ)．よって [10] の方法の方が計算時間が短くなると思われる．また，評価の精度においても [10] の方法を使うことで以前の方法から得られる評価より良いものが得られる場合が多い．例えば [10, Example6.1] では J．E．Cremona，M．Prickett，S．Siksek[6] の上の評価 (つまり内田の評価の数列の初項にあたるもの) とこの方法での評価を比較している．次の例

がそれにあたるものである．

例 3.49. 楕円曲線 $E/\mathbb{Q}$ を，

$y^2+xy+y=x^3-x^2+31368015812338065133318565292206590792820353345x$
$+30203880269856608733564318842954349862452204168387449355518606256815984 7,$

で表されるものとする．この場合，J．E．Cremona，M．Prickett，S．Siksek での評価が 18.018，この方法での評価が 0.147 となっており，よって注意 3.48 で述べたように，[10] の方法によりかなり良い評価を得られることがわかる．

ただ，実素点においては J．E．Cremona，M．Prickett，S．Siksek や内田の方法もかなり良い結果を出していて，さらに複素素点においては，係数が大きくなると計算時間がかかるという欠点もあるが P．Bruin[11] の方法を使うことでも良い結果が得られている．よって，これらの方法を場合によって使い分けることが望ましいと主張している．詳しくは [10] を見よ．

4 応用例

ここでは，通常高さ関数と標準高さ関数の差の評価や標準高さ関数の評価を利用している例を紹介する．

4.1 奈良の [8, Theorem1.3] について

奈良の論文 [8] では [8, Theorem1.1] で楕円曲線の quadratic twist の有理点での標準高さ関数の値の下からの評価を与えている．それを利用して得られるのが次の定理である．ただし，ここでの h，$\hat{h}$ はそれぞれ [8] での通常高さ関数，標準高さ関数を表すとする．

定理 4.1. $t\in\mathbb{Z}, D(t)=t^6+4t^4+30t^3+5t^2+54t+245,$
$\mathbb{Q}$ 上の楕円曲線 E_D を

$$y^2=x^3+2D(t)x^2+163D(t)^2x+2205D(t)^3,$$

で定め，$P=(D(t)(t^4+2t^2+12t),\ D(t)^2(t^3+t+3))\in E_D(\mathbb{Q})$ とおき，$D(t)$ が無平方とする．このとき，$|t|\geqq 2216$ ならば P は原始的である．

ここで，E_D は $\mathbb{Q}$ 上の楕円曲線 $E: y^2=x^3+2x^2+163x+2205$ の $D(t)$ による quadratic twist である．以下で quadratic twist について少し紹介する．

定義 4.2. K 上の曲線 C に対し，C/K の twist とは滑らかな K 上の曲線 C'/K で C と $\bar{K}$ 上同型なものの，K 同型類のことを言う．

quadratic twist とは twist の一つで，$d \in \bar{\mathbb{Q}}$ に対し，$(x, y) \mapsto (x, \sqrt{d}y)$ により楕円曲線 E から移されるものである．奈良の論文 [8] では 3 章で，この quadratic twist を実際に作る方法を紹介している．具体的には，3 次のモニックな既約多項式 $f \in \mathbb{Z}[t]$，ある $m \in \mathbb{Z}$ に対し $F' = mf$ となる多項式 $F \in \mathbb{Z}[t]$，f の根 α，$F(\alpha)$ の $\mathbb{Q}$ 上の最小多項式 f_1 に対し，多項式 $D(t)$ が存在して $D(t)f(t)^2 = f_1(F(t))$ となることが示されている．これより楕円曲線 $y^2 = f_1(x)$ の quadratic twist$D(t)y^2 = f_1(x)$ が得られ，さらにこの曲線は有理点 $(F(t), f(t))$ を持つことが示される (詳細は [8, 3 章] を見よ)．f, F を次のように限定すると，この場合における f_1, D の明示的な式が得られる．

補題 4.3. $A, B \in \mathbb{Z}, f = t^3 + At + B, F = t^4 + 2At^2 + 4Bt$ とする．このとき，上の f_1, D は，

$$f_1(t) = t^3 + 2A^2t^2 + A(A^3 + 18B^2)t + B^2(2A^3 + 27B^2),$$
$$D(t) = t^6 + 4At^4 + 10Bt^3 + 5A^2t^2 + 18ABt + 2A^3 + 27B^2,$$

となる．特に f, f_1 の判別式を $\mathrm{disc}(f), \mathrm{disc}(f_1)$ とおくと，$\mathrm{disc}(f_1) = B^2\mathrm{disc}(f)^3$ が成り立つ．

証明. $D(t)f(t)^2 = f_1(F(t))$ より，$f(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$ とおくと $i = 1, 2, 3$ について $f_1(F(\alpha_i)) = 0$ となる．$f_1(t)$ は 3 次のモニック多項式であったので，$f_1(t) = (t - F(\alpha_1))(t - F(\alpha_2))(t - F(\alpha_3))$ と書ける．よって，$f(t)$ における解と係数の関係と $F(t)$ の形から $f_1(t)$ の係数が導かれ，あとは計算から $D(t)$ の形が得られる． □

$y^2 = f_1$ で表わされる楕円曲線を E' とおくと，補題 4.3 より

$$\Delta_{E'} = 16\mathrm{disc}(f_1) = 16B^2\mathrm{disc}(f)^3 = 16B^2(-4A^3 - 27B^2)^3,$$

となる．よって例えば B が奇数で $\gcd(A, B) = 1$，$\mathrm{disc}(f)$ が無平方ならば，$\Delta_{E'}$ は 6 乗因子を持たないので [8, Theorem1.1] を適用することができる，ということが [8, Remark3.2] で言及されている．

定理 4.1 は補題 4.3 で $A = 1, B = 3$ としたものである．このとき B は奇数で $\gcd(A, B) = 1, \mathrm{disc}(f) = -4A^3 - 27B^2 = -247 = 13 \cdot 19$ となる．よってこの時 [8, Theorem1.1] を適用することができるので，それを使い定理 4.1 が導かれるのである．定理 4.1 を示すためには直接的には以下のふたつが必要となる．

系 4.4. $E_D, D(t)$ を定理 4.1 のものとする．$Q \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$ に対し

$$\hat{h}(Q) > \frac{1}{4}\log D(t) - 3.5472,$$

が成り立つ．

証明. [8, Definition4.14] で E_D の有限素点を 6 つの集合に分けて，[8, Lemma4.16] から [8, Lemma4.20] でそれぞれ点ごとの局所高さ関数の下の評価を与えている．特に [8, Lemma4.21, Lemma4.22] ではそれぞれ $p = 2, 3$ の場合の評価を与えている．それらの結果より [8, Theorem1.1] が示され，その結果と PARI/GP v.2.3.4 により $E : y^2 = x^3 + 2x^2 + 163x + 2205$ の Δ, ω_1, q の値を計算する事により導かれる．詳しくは [8, Corollary4.23] を見よ． □

命題 4.5. $E_D, D(t), P$ を定理 4.1 のものとする．このとき

$$\hat{h}(P) < \frac{2}{3}\log D(t) + 1.2177,$$

が成り立つ．

証明. [8, Lemma5.1] で無限素点での上の評価，[8, Lemma5.2] で有限素点での上の評価を与えている．これらを合わせることで導かれる．詳しくは [8, 5 章] を見よ． □

定理 4.1 の証明. $y(P) = D(t)^2(t^3+t+3) \neq 0$ ならば $2y(P)+a_1x(P)+a_3 = 2y(P) \neq 0$ なので，この時 [2, 3 章 2.3(b)] より P は 2-捩れ点ではない．この時系 4.4 より計算すると $|t| \geqq 11$ となる．

また P に命題 4.5，任意の $Q \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$ に系 4.4 を適用すると，$|t| \geqq 2216$ の時

$$\frac{\hat{h}(P)}{\hat{h}(Q)} < \frac{\frac{2}{3}\log D(t) + 1.2177}{\frac{1}{4}\log D(t) - 3.5472} < 4, \tag{4.6}$$

となる．ここで，ある $R \in E_D(\mathbb{Q})$ が存在して $P = mR, m \geqq 3$ と仮定する．このとき $2P \neq O$ なので $2R \neq O$ となる．よって (4.6) を R に適用すると定理 2.35(b) より，

$$\begin{aligned}\hat{h}(P) < 4\hat{h}(R) &< m^2\hat{h}(R),\\ &= \hat{h}(mR) = \hat{h}(P),\end{aligned}$$

となりこれは矛盾である．よってこの様な R は存在しないので P は原始的である． □

4.2　J．H．Silverman の [4, Example7．1] について

[4, Theorem1.1] では $P \in E(K)$ につて $\hat{h}(P) - \frac{1}{2}h(x(P))$ を評価している．[4, Theorem1.1] の特別な場合が [4, Theorem1.3] である．これより導かれるのが [4, Example2.4] で，楕円曲線 $E : y^2 = x^3 - x + 1, P \in E(\mathbb{Q})$ について，

$$\frac{1}{2}h(x(P)) \leqq \hat{h}(P) + \frac{1}{8}\log\frac{6912}{23} + 1.205 \leqq \hat{h}(P) + 1.92, \tag{4.7}$$

が示されている．[4, 7 章] では，この $\hat{h}(P) - \frac{1}{2}h(x(P))$ の評価と [5] で計算した $\hat{h}(P)$ の近似値を使うことで Mordel-Weil 群の生成元の x 座標を絞り込んでいる．これについて以下で紹介する．

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 - x + 1$ について，Mordel-Weil 群の生成元を考える．E の判別式 Δ を計算すると $\Delta = -368 = -2^4 \cdot 23$ なので，[2, 7 章 Remark1.1] より E は任意の素数を法とした剰余で非特異となる．$\#E(\mathbb{F}_3) = 7, \#E(\mathbb{F}_5) = 8$ より [2, 7 章 Proposition3.1] を使うと，$E(\mathbb{Q})$ は捩れ部分を持たない．[9] より，$E(\mathbb{Q})$ のランクは大きくて 1 となる．少し探すと E の有理点

$$(-1, 1), \quad (0, 1), \quad (1, 1), \quad (3, 5), \quad (5, 11), \tag{4.8}$$

が見つかる．よって $E(\mathbb{Q})$ のランクは 1 である．

E の Mordel-Weil 群 $E(\mathbb{Q})$ の生成元を見つける．[5] のアルゴリズムを使うとこれら 5 つの点の標準高さ関数の値の近似値を計算することができる ([5] の論文では，局所高さ関数を急速に収束する数列の和で表し，さらに初項から第 N 項まで足した値と実際の値との誤差について論じている)．最も値が小さかったのは $P = (1,\ 1)$ で $\hat{h}(P) = 0.\ 0249\cdots$ である．さらに計算すると，

$$(-1, 1) = 2P, \quad (0, 1) = -3P, \quad (3, 5) = -4P, \quad (5, 11) = 5P,$$

となることがわかる．

P が $E(\mathbb{Q})$ の生成元となる事を示す．

P が生成元でないと仮定すると，ある $R \in E(\mathbb{Q}), m \geqq 2$ で $P = mR$ となるものがある．さらに $x(P) \in \mathbb{Z}$ なので $x(R) \in \mathbb{Z}$ となる (もし $x(R) = \frac{p}{q}, q \neq \pm 1, \gcd(p, q) = 1$ とすると，命題 3.6, 命題 3.7 より $1 = x(P) = \frac{\phi_m(x(R))}{\psi_m^2(x(R))} = \frac{x(R)^{m^2}+\cdots}{m^2 x(R)^{m^2-1}+\cdots} = \frac{\frac{p^{m^2}}{q^{m^2}}+\cdots}{m^2\frac{p^{m^2-1}}{q^{m^2-1}}+\cdots} = \frac{p^{m^2}+\cdots}{m^2 q p^{m^2-1}+\cdots}$，よってこの分子を p'，分母を q' とおくと，q' は q で割り切れるが p' は割

り切れない．よって p' は q' で割り切れないので矛盾となる)．もしこの様な R が存在すれば標準高さ関数の性質より

$$\hat{h}(R) = \frac{1}{m^2}\hat{h}(P) \leqq \frac{1}{4}\hat{h}(P) = 0.0061\cdots,$$

となる．(4.7) より

$$h(x(R)) \leqq 2\hat{h}(R) + 3.84 \leqq 3.86,$$

より，もしこの様な R が存在すれば $x(R) \in \mathbb{Z}, |x(R)| \leqq e^{3.86} < 48$ を満たす．$x \leqq -2$ ならば $x^3 - x + 1 < 0$ となるので，以上から $x(R)$ は -1 から 48 の間の整数となる．それらを全て確かめると，この様な点は (4.8) ですべてであることがわかる．したがってこの様な R は存在しないので，P が生成元であることが示された．

参考文献

[1] . Y. Uchida, The difference between the ordinary height and the canonical height on elliptic curves. Journal of Number Theory, 128 (2008), 263279.

[2] . J. H. Silverman , The Arithmetic of Elliptic Curves(2nd Edition). Springer-Verlag,

[3] . J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag, (1994)

[4] . J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves. Math. Comp. 55 (1990) 723743.

[5] J. H. Silverman, Computing heights on elliptic curves. Math. Comp. 51(1988), no. 183, 339-358.

[6] . J. E. Cremona, M. Prickett, S. Siksek, Height difference bounds for elliptic curves over number fields. J. Number Theory, 116(2006), pp. 42-68

[7] . S. Schmitt, H. G. Zimmer, Elliptic Curves: A Computational Approach. de Gruyter Stud. Math, vol. 31, Walter de Gruyter (2003)

[8] . T. Nara, Lower bounds of the canonical height on quadratic twists of elliptic curves. Rocky Mountain J. Math. Volume forthcoming, Number forthcoming (2013).

[9] A. Brumer, K. Kramer, The rank of elliptic curves, . Duke Math. J. 44 (1977), no. 4, 715743.

[10] J. S. Múller, Corinna Stumpe, Archimedean local height differences on elliptic curves. (2018), https://arxiv. org/pdf/1807. 04153. pdf

[11] P. Bruin, Bornes optimales pour la diff ´ erence entre la hauteur de Weil et la hauteur de N ´ eronTate sur les courbes elliptiques sur Q, Acta Arith. 160 (2013), 385-397. ↑