height と canonical height の差について

伊藤　高志

平成 21 年 2 月 27 日

目 次

1 はじめに

この論文の主な目的は，任意の代数体 K 上で定義された楕円曲線 E に対する height と canonical height の差の評価を，乗法多項式を用いて定めることであり，内田氏の論文，[8] を中心にまとめた解説論文である．

一般に K 上で定義された楕円曲線は，次の Weierstrass 方程式と呼ばれる方程式で与えられる．

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K).$$

特に K の標数が 2 でも 3 でもない場合は，平方完成と変数変換を行うことにより，より簡単な次の形でかけることが知られている．

$$E : y^2 = x^3 + Ax + B \quad (A, B \in K).$$

どのように群の演算を定義するか等は後ほど述べることにするが，これらの楕円曲線の K-有理点からなる部分群,

$$E(K) = \{P = (x, y) \in E(\bar{K}) \mid x, y \in K\}$$

を求めることは興味深い問題である．この問題に関しては，Mordell と Weil により，次の定理が示されている．

定理 1.1 (**Mordell-Weil**)**.** $E(K)$ は有限生成可換群である．

Mordell はこの定理において $K = \mathbb{Q}$ の場合を示し，Weil は一般の代数体上のアーベル多様体についても同様の結果を示している．

この定理により $E(K)$ はそのねじれ部分群 $E(K)_{\mathrm{tors}}$ と，rank を r としたとき，$\mathbb{Z}^r$ の直和で次のように表されることがわかる．

$$E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r.$$

与えられた E に対して，$E(K)_{\mathrm{tors}}$ を完全に決定することは，一般的にはそれほど難しくはない．特に $K = \mathbb{Q}$ ならば，$E(\mathbb{Q})_{\mathrm{tors}}$ は，群として 15 種類の可能性しかないことが次の定理により知られている．

定理 1.2 (**Mazur** [2],[3])**.** $E(\mathbb{Q})_{\mathrm{tors}}$ は，次の 15 種類のいずれかと同型である．

1. $\mathbb{Z}/N\mathbb{Z}$ $\quad (1 \leq N \leq 10$ もしくは $N = 12)$,
2. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ $\quad (1 \leq N \leq 4)$.

しかし，r を完全に決定することは，はるかに難しく，どのような楕円曲線に対しても適用できるようなアルゴリズムはいまだに知られていない．

もし，幸運にも r が求められたとしたら，次に問題になるのはその基底を見つけることであるが，height と canonical height の差を用いることがその問題に対して有効である場合がある．後ほど述べるが，これらの定義は対数的なので，評価がより良くなれば，計算は飛躍的に楽になる．

この節の最後として，詳しい記号の定義は後ほど述べることにするが，内田氏による主定理の主張を述べておくことにする．

主定理 (内田 [8, Thm.1])．

m を 2 以上の整数とする．このとき，任意の $P \in E(K)$ に対して，

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

が成り立つ．

ただし，M_K^0 は有限素点全体の集合，M_K^∞ は無限素点全体の集合，T_v，S_v は楕円曲線の乗法多項式によって決まるある有界連続関数の上限と下限で表される値で，n_v は K の v における局所次数，q_v は v における K の剰余体の元の個数，$\Delta_v^{\min}$ は E の v における極小判別式，α_v は，E と v による小平タイプと玉河数と呼ばれるものにより一意的に定まる数である．

なお、この定理の $m = 2$ の場合は，2006 年に J. E. Cremona，M. Prickett，S. Siksek [1] の 3 氏により求められており，内田氏の主定理はその定理の一般化といえる．

謝辞

最後になりましたが，セミナー等で御世話になりました雪江明彦先生，中村哲男先生には心から感謝します．また，セミナーや授業で一緒だった田嶋和明君，田中修平君，五十嵐健太君にも感謝します．

2　楕円曲線の一般論

この節では，まず楕円曲線を定義し，それに対する一般的な事実を述べる．以下，特に断わらない限り，K を任意の代数体とする．

定義 2.1 (**楕円曲線**). 種数 1 の曲線 E と，E 上の固定された点 O との組 (E, O) を**楕円曲線**と言う．

任意の楕円曲線は，Weierstrass 標準形と呼ばれる以下の形の方程式，

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \tag{2.2}$$

で表される 3 次曲線のうち，非特異なものと同型であり，O は無限遠点に写ることが良く知られている ([5, pp.37–41] 参照)．以後，楕円曲線 (E, O) を単に E と書くことにする．

上の曲線において，K の標数が 2 でないと仮定すると，変数変換と平方完成を行うことにより，次の形に直すことができる．

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

ここで，$b_2 = a_1^2 + 4a_2$，$b_4 = 2a_4 + a_1a_3$，$b_6 = a_3^2 + 4a_6$ である．

また，標数が 3 でもないとき，変数変換により，x^2 の項を消去することができ，次の形に書ける．

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

ここで，$c_4 = b_2^2 - 24b_4$，$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ である．

後に必要となるので，次の値も定義しておく．

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta. \end{aligned}$$

Δ を E の **判別式**，j を E の ***j*-不変量**と呼ぶ．

命題 2.3. E が非特異であることと，$\Delta \neq 0$ であることは同値である．

証明. K の標数が 2 でないと仮定する．

$$\begin{aligned} f(x, y) &:= y^2 - (4x^3 + b_2x^2 + 2b_4x + b_6), \\ E &:= \{(x, y) \mid f(x, y) = 0\} \end{aligned}$$

とおく．$f(x, y)$ を斉次化すると次の方程式が得られる．

$$F(X, Y, Z) = Y^2Z - 4X^3 - b_2X^2Z - 2b_4XZ^2 - b_6Z^3.$$

また，無限遠点の斉次座標は，$[X, Y, Z] = [0, 1, 0]$ の 1 点で与えられることが知られている．

まず，無限遠点が非特異であることを示す．F を Z で偏微分し，O を代入すると，$\partial F/\partial Z(O) = 1 \neq 0$ となるので，無限遠点は非特異である．

次に E 上の無限遠点でない点，(x_0, y_0) が特異点であるとする．このとき，次が成り立つ．

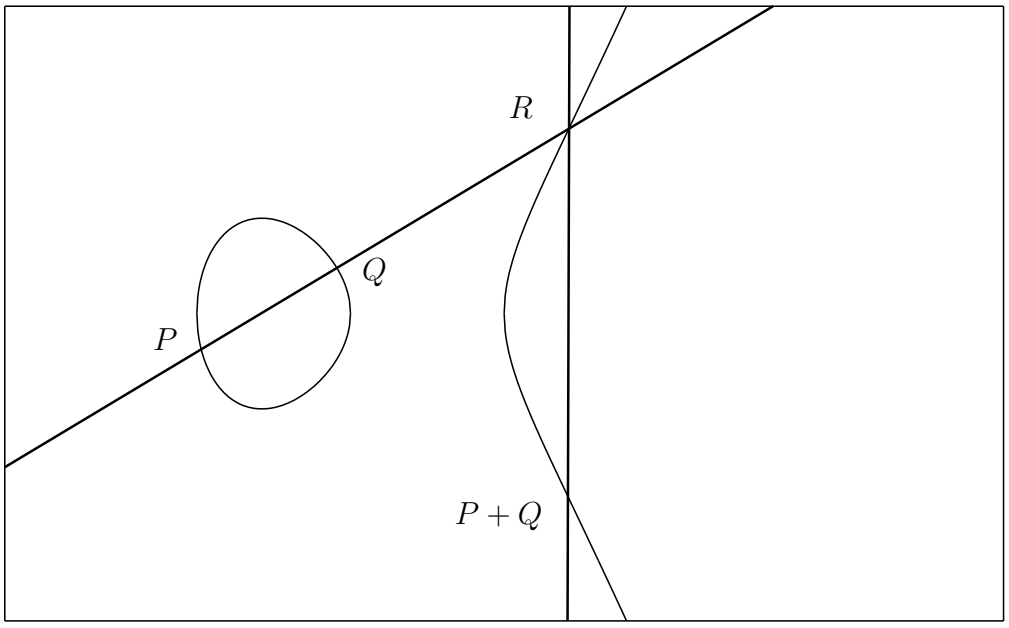
$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

これはつまり，$y_0 = 0$ であり，x_0 は $4x^3 + b_2x^2 + 2b_4x + b_6$ の重根であることを意味するが，3 次方程式が重根を持つのは判別式が 0 でないとき，また，そのときに限るので命題が示された (標数が 2 のときは，多少証明が複雑になるが，同様の結果が得られる)． □

例 2.4. (1) E を $\mathbb{Q}$ 上の曲線で，Weierstrass 方程式が $y^2 = x^3$ で与えられているものとすると，$\Delta = 0$ となり，E は (0,0) で特異点を持つので，これは楕円曲線ではない．
(2) E を $\mathbb{Q}$ 上の曲線で，Weierstrass 方程式が $y^2 = x^3 + 1$ で与えられているとすると，$\Delta = -27$ となり，E は特異点を持たないので，これは楕円曲線である．

次に，楕円曲線に演算を与える．

定義 2.5 (**楕円曲線の演算**)．E 上の点 P，Q に対して，P と Q を結んだ直線と第 3 の交点を R とする．このとき，O と R を結んだ直線の第 3 の交点を $P + Q$ と定義する．ただし，$P = Q$ の場合は R をその接線との交点する (下図参照)．



定理 2.6. [5, p.55]. この演算により E は O を単位元とする可換群となる.

結合法則のみ確認が必要だが，次に見る加法公式によりただちに導かれる.

命題 2.7. (**加法公式** [5, p.58]). E を (2.2) で与えられた楕円曲線とする．このとき，次が成り立つ.

1. $P_0 = (x_0, y_0) \in E$ とすると，
$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

2. $P_1 = (x_1, y_1)$，$P_2 = (x_2, y_2) \in E$ とするとき，
$$P_1 + P_2 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)).$$
ただし，
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \qquad (x_1 \neq x_2).$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},$$
$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \qquad (x_1 = x_2).$$
とする（つまり，$y = \lambda x + \nu$ は P_1, P_2 を通る直線とする（$P_1 = P_2$ の場合は接線)) .

3. $P = (x, y) \in E$ とするとき，
$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}.$$
これを楕円曲線 E の **2 倍公式**と呼ぶ.

例 2.8. $E : y^2 = x^3 - 43x + 166$, $P = (3, 8)$ として，加法公式により実際に計算してみる.
$$x(2P) = -5, \quad x(4P) = 11, \quad x(8P) = 3 = x(P)$$
となる．よって，P は位数が 7 か 9 の点であるが，y 座標を幾何学的に調べれば，$y(8P) = 8$ であることがわかり，$P = 8P$ となるので，P の位数は 7 であることがわかる.

注 2.9. 任意の整数 m に対する m 倍公式が主定理の証明で非常に重要になるが，それに関しては後ほど漸化式の形で定義し，性質を述べることにする.

次に，Mordell-Weil の定理を証明するために，楕円曲線 E における height function を定義する．そこで，もう一度定理を述べておく．

定理 2.10. (**Mordell-Weil** [5, p.189])．$E(K)$ は有限生成可換群である．

定理の証明は次の二つのステップで行われ，その後半で height function が必要になる．

1. 弱 Mordell-Weil の定理の証明.
2. height function による降下.

(1) に関しては詳しく述べないが，定理の主張のみ述べておくことにする．

定理 2.11. (**弱 Mordell-Weil** [5, p.190])．2 以上の整数 m に対して，
$E(K)/mE(K)$ は有限群である．

次に (2) に関してであるが，どのように降下するかを次の定理で述べる．

定理 2.12 (**降下定理**)．A を可換群とする．このとき，height function と呼ばれる A から $\mathbb{R}$ への関数 h があり，以下の性質を満たすとする．

1. 任意の $Q \in A$ に対して，A と Q のみに依存する定数 C_1 が存在して，任意の $P \in A$ に対して，
$$h(P+Q) \leq 2h(P) + C_1.$$
が成り立つ.
2. A にのみ依存する定数 C_2 が存在して，任意の $P \in A$ に対して，
$$h(2P) \geq 4h(P) - C_2.$$
が成り立つ.
3. 任意の定数 C_3 に対して，
$$\{P \in A : h(P) \leq C_3\}$$
は有限集合である．

このとき，$A/2A$ が有限集合ならば，A は有限生成である．

証明. 仮定より $A/2A$ は有限なので，その代表元の数を n として，ある一つの完全代表系を，$Q_1, Q_2, ..., Q_n$ とする．A の任意の元 P は，ある A の元 P_1 と，$A/2A$ の元 Q_{i_j} によって，
$$P - Q_{i_1} = 2P_1$$

と書くことができる．以下同様に繰り返すと，

$$\begin{aligned} P_1 &= 2P_2 + Q_{i_2}, \\ P_2 &= 2P_3 + Q_{i_3}, \\ &\vdots \\ P_{n-1} &= 2P_n + Q_{i_n} \end{aligned}$$

を得る．それぞれ代入していくと，次の式を得る．

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{n-1}Q_{i_n} + 2^n P_n.$$

仮定の 1. より，任意の $P \in A$ と $Q_i \in A/2A$ に対して，

$$h(P + Q_i) \leq 2h(P) + C_i$$

となる定数 C_i が存在する．その中で最大のものを C とすると，

$$h(P + Q_i) \leq 2h(P) + C$$

となる．

次に各 P_j に対して，2. の条件を使うと，A にのみ依存する C' が存在して，

$$4h(P_j) \leq h(2P_j) + C' = h(P_{j-1} - Q_{i_j}) + C' \leq 2h(P_{j-1}) + C + C'$$

となる．よって，$h(P_{j-1}) \geq C + C'$ ならば，次の式を得る．

$$h(P_j) \leq \frac{3}{4} h(P_{j-1}).$$

したがって，十分大きな j に対しては，

$$h(P_j) \leq C + C'$$

が成り立つ．よって，十分大きな j に対して，P_j は

$$\{R \in A \mid h(R) \leq C + C'\}$$

で生成された部分群の元になる．

ゆえに A は，

$$\{Q_1, Q_2, ..., Q_n\} \cup \{R \in A \mid h(R) \leq C + C'\}$$

で生成される．この集合は，3. より有限集合なので定理が示された．

□

注 2.13. 定理 2.11，2.12 により，定理 2.12 の条件をみたすような height function $h : E(K) \to \mathbb{R}$ を見つけることができれば，定理 2.10 は直ちに示される．

定義 2.14 (**height function**)**.** 楕円曲線 E 上の height function $h : E(K) \to \mathbb{R}$ を次で定める.

$$h(P) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max\{1, |x(P)|_v\}$$

ただし，$n_v = [K_v : \mathbb{Q}_v]$ である.

実際，このように h を定義すれば，h は定理 2.12 の条件を満たすが，$K = \mathbb{Q}$ の場合のみ確認することにする.

$K = \mathbb{Q}$ の場合は，height function の定義は次と同値になる.

定義 2.15 ($\mathbb{Q}$ **上の楕円曲線の height function**)**.** $P = (x, y) \in E(\mathbb{Q})$ に対して，$x := m/n$ を既約分数とする．このとき，$h : E(\mathbb{Q}) \to \mathbb{R}$ を次で定める.

$$h(P) := \log \max\{|m|, |n|\}$$

注 2.16. $P = (x, y) \in E(\mathbb{Q})$ に対して，x を次のように素因数分解する.

$$x = p_1^{n_1} \times p_2^{n_1} \times \ldots \times p_i^{n_i}.$$

ただし，$n_j \leq 0$，$n_{j+1} \geq 0$ とする.

このとき，$i \leq j$ に対しては,

$$\max\{1, |x|_{p_i}\} = p_i^{n_i}$$

であり，$i \geq j + 1$ に対しては,

$$\max\{1, |x|_{p_i}\} = 1$$

である．よって，$|x| \leq 1$ に対しては,

$$\max\{1, |x|\} = 1$$

であるので,

$$\sum_{v \in M_K} \log \max\{1, |x(P)|_v\} = p_1^{n_1} \times p_2^{n_1} \times \ldots \times p_j^{n_j}$$

となる．$|x| \geq 1$ に対しては,

$$\max\{1, |x|\} = |x|$$

であるので,

$$\sum_{v \in M_K} \log \max\{1, |x(P)|_v\} = p_{j+1}^{n_{j+1}} \times p_{j+2}^{n_{j+2}} \times \ldots \times p_i^{n_i}$$

となる．よって，定義 2.14 と定義 2.15 は同値の定義である.

この h が，定理 2.12 の条件を満たすことを示す.

命題 2.17. E を $\mathbb{Q}$ 上の楕円曲線とし，Weierstrass 方程式が次で与えられているとする．

$$E : y^2 = x^3 + Ax + B \quad (A, B \in \mathbb{Z}).$$

1. P_0 を $E(\mathbb{Q})$ 上の任意の点とする．このとき，E と P_0 にのみ依存する定数 C_1 が存在して，任意の $E(\mathbb{Q})$ 上の点 P に対して，

$$h(P + P_0) \leq 2h(P) + C_1$$

が成り立つ．

2. 任意の $E(\mathbb{Q})$ 上の点 P に対して，E にのみ依存する定数 C_2 が存在して，

$$h(2P) \geq 4h(P) - C_2$$

が成り立つ．

3. 任意の定数 C_3 に対して，

$$\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$$

は有限集合である．

証明. 1. $P_0 = O$ のときは明らかであるので，$P_0 \neq O$ とする．

有限個の E 上の点 P は取り除いてもよいので，$P \neq O, \pm P_0$ としてよい．何故なら最後にそれらの P に対しても成り立つように定数 C_1 を取り直せば良いからである．

自明なことではないが，P, P_0 の各座標は既約分数により次のように書ける．

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right), \quad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right).$$

加法公式より次を得る．

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0.$$

また，P, P_0 はそれぞれ E 上の点なので，展開して式変形すると次を得る．

$$x(P + P_0) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

右辺は分子に a^2，ad^2，d^4，bd，分母に a^2，d^4 の項をそれぞれ持つ．

よって，A, B, a_0, b_0, d_0 の単項式の絶対値で表される C_1 により次の不等式が成り立つ．

$$h(P + P_0) \leq C_1 \log \max\{|a|^2, |ad^2|, |d|^4, |bd|\}.$$

$|a| \leq |d|^2$ と，$|d|^2 \leq |a|$ のように場合分けして考えれば，どちらの場合でも $|ad^2|$ を消去することができる．よって，$|bd|$ を消去できれば，求める結果が得られる．

ここで，P は E 上の点なので，

$$b^2 = a^3 + Aad^2 + Bd^6$$

となる．よって，$C_1' = 1 + |A| + |B|$ とすると，

$$|b| \leq C_1' \max\{|a|^{\frac{3}{2}}, |a|^{\frac{1}{2}}|d|, |d|^3\}$$

が成り立つ．ここで，再び $|a|^{1/2} \leq |d|$ と，$|d| \leq |a|^{1/2}$ のように場合分けして考えれば，$|a|^{1/2} \leq |d|$ の場合は，$|a|^{1/2}|d| \leq |d|^3$，$|d| \leq |a|^{1/2}$ の場合は，$|a|^{1/2}|d| \leq |a|^{3/2}$ となり，どちらの場合でも

$$|b| \leq C_1' \max\{|a|^{\frac{3}{2}}, |d|^3\}$$

となり，$|bd| \leq C_1'|a|^2$，もしくは，$|bd| \leq C_1'|d|^4$ を得る．よって，$|bd|$ を消去することができるように C を選び直せば求める結果が得られる．以上より 1. は示された．

2. 1. と同様に有限個の P を除いて考えてもよいので，$2P \neq O$ とする．

$P = (x, y)$，$2P = (s, t)$ とすると，加法公式より次が得られ，分子，分母を次のようにおく．

$$s = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} := \frac{\phi(x)}{\psi(x)}.$$

$f(x) = x^3 + Ax + B$ とすると，$\phi(x) = (f'(x^2)) - 8xf(x)$，$\psi(x) = 4f(x)$ となり，E は非特異なので，$\phi(x)$ と $\psi(x)$ は共通零点を持たない．

証明のアイデアは与えられた有理式があまり約分できず，ある有理式によって評価できるということである．

まず，ϕ と ψ によってのみ決まる 1 以上の整数 R があって次が成り立つことを示す．任意の有理数 m/n に対して，$\gcd(n^4\phi(m/n), n^4\psi(m/n))$ は R を割り切る．

$$n^4\phi\left(\frac{m}{n}\right) := a_0m^3n + a_1m^2n^2 + a_2mn^3 + a_3n^4,$$

$$n^4\psi\left(\frac{m}{n}\right) := b_0m^4 + b_1m^3n^1 + a_2m^2n^2 + a_3mn^3 + b_4n^4$$

とする．$\phi(x)$，$\psi(x)$ は互いに素なので，ある $F(x)$，$G(x) \in \mathbb{Z}[x]$ によって，次のように表せる．

$$F(x)\phi(x) + G(x)\psi(x) = 1.$$

$D := \max\{\deg F, \deg G\}$ とすると，

$$n^DF\left(\frac{m}{n}\right)n^4\phi\left(\frac{m}{n}\right) + n^DG\left(\frac{m}{n}\right)n^4\psi\left(\frac{m}{n}\right) = n^{D+4}$$

を得る．よって，$u := \gcd(n^4\phi(m/n), n^4\psi(m/n))$ とすると，u は n^{D+4} を割り切ることがわかる．u は n に依存してしまうので，u が a_0^{D+4} を割り切ることを示す．

定義より u は $n^3n^4\phi(m/n)$ を割り切るので，u は $a_0m^4n^{D+3}$ を割り切る．ゆえに，u は $\gcd(n^{D+4}, a_0m^4n_{D+3})$ を割り切り，よって，u は a_0n^{D+3} を割り切る．同様に繰り返すと，u は a_0^{D+4} を割り切ることがわかる．

次に，ϕ と ψ によってのみ決まる定数 C_2 があって，任意の 0 でない有理数 m/n に対して，

$$4h\left(\frac{m}{n}\right) - C_2 \leq h\left(\frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})}\right)$$

が成り立つことを示す．既約な有理数 m/n に対して，$H(m/n) := \max\{|m|, |n|\}$ と定義すると，前に決めた R により，

$$\begin{aligned} H(2P) &\leq \frac{1}{R}\max\left\{\left|n^4\phi\left(\frac{m}{n}\right)\right|, \left|n^4\psi\left(\frac{m}{n}\right)\right|\right\}, \\ &\leq \frac{1}{2R}\left(\left|n^4\phi\left(\frac{m}{n}\right)\right| + \left|n^4\psi\left(\frac{m}{n}\right)\right|\right) \end{aligned}$$

となる．よって，

$$\begin{aligned} \frac{H(2P)}{H(\frac{m}{n})^4} &\leq \frac{1}{2R}\frac{|n^4\phi(\frac{m}{n})| + |n^4\psi(\frac{m}{n})|}{\max\{|m|^4, |n|^4\}}, \\ &= \frac{1}{2R}\frac{|\phi(\frac{m}{n})| + |\psi(\frac{m}{n})|}{\max\{|\frac{m}{n}|^4, 1\}} \end{aligned}$$

となる．この関数の次数を考えると，下極限は 0 より大きいことがわかる．よって，ある定数 $C_2 > 0$ があって，

$$\frac{H(2P)}{H(\frac{m}{n})^4} \leq C_2$$

となり，ゆえに C_2 を正しく取り直せば，求める結果が得られる．

3. $x(P) = m/n$ で，m/n は既約であるとすると，$\max\{|m|, |n|\} \leq e^{C_3}$ となる有理点の x 座標は高々有限個しかなく，その x 座標に対応する y 座標も高々2 つしかないため与えられた集合は有限集合である． □

多少証明は複雑になるが，この命題は一般の代数体に対しても成り立つ ([5, pp.215–220])．

上の命題より次の 2 つの系が得られる．

系 2.18. E を K 上の楕円曲線とする．このとき，E にのみ依存する定数 C', C'' が存在して，任意の P，$Q \in E$ に対して，

$$2h(P) + 2h(Q) - C' \leq h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + C''$$

が成り立つ．

系 2.19. E を K 上の楕円曲線とする．このとき，E にのみ依存する定数 C_m が存在して，任意の $P \in E$ と整数 m に対して，

$$-C_m \leq h(mP) - m^2h(P) \leq C_m$$

が成り立つ．

これらの 2 つの系は，$P=(x_1,y_1)$，$Q=(x_2,y_2)$ としたとき，
$x(P+Q)+x(P-Q)$，$x(P+Q)x(P-Q)$ を x_1,x_2 で表して，命題 2.17 を使えば導かれる．

これら 2 つの系において，定数がなくなり，不等号が等号になれば 2 次形式的な性質を持ち，非常に扱いやすいものになる．よって次に，それを実現するために canonical height を定義する．

定義 2.20 (**canonical height function**)**.** E を K 上の楕円曲線とする．このとき，E 上の canonical height function を次のように定義する．

$$\hat{h} : E(K) \to \mathbb{R}$$

$$\hat{h}(P) := \lim_{i\to\infty} \frac{1}{4^i} h(2^i P)$$

実際この極限が常に存在することを示す．

命題 2.21. 任意の $P \in E(K)$ に対して，極限

$$\lim_{i\to\infty} \frac{1}{4^i} h(2^i P)$$

は存在する．

証明. この点列が Cauchy 列であることを示せば良い．系 2.18 より，任意の $Q \in E(K)$ に対して，次が成り立つようなある定数 C が存在する．

$$|h(2Q) - 4h(Q)| \le C.$$

$N \ge M \ge 0$ をそれぞれ整数とする．このとき，

$$\begin{aligned}
&|4^{-N}h(2^N P) - 4^{-M}h(2^M P)| \\
&\qquad = \left| \sum_{n=M}^{N-1} 4^{-n-1} h(2^{n+1}P) - 4^{-n}h(2^n P) \right|, \\
&\qquad \le \sum_{n=M}^{N-1} 4^{-n-1} |h(2^{n+1}P) - 4^{-n}h(2^n P)|, \\
&\qquad \le \sum_{n=M}^{N-1} 4^{-n-1} C, \\
&\qquad \le \frac{C}{4^{M+1}}.
\end{aligned}$$

よって Cauchy 列であることがわかり，命題が示された． □

次に，前に述べた性質を，canonical height function が実際に満たすことを確かめる．

命題 2.22. $\hat{h}$ を E 上の canonical height function とする．このとき次が成り立つ．

1. 任意の $E(K)$ の元 P，Q に対して，次が成り立つ．

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

2. 任意の $E(K)$ の元 P と，任意の整数 m に対して，次が成り立つ．

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

証明. 1. 系 2.18 より，

$$h(P+Q)+h(P-Q)=2h(P)+2h(Q)+O(1).$$

P，Q をそれぞれ 2^NP，2^NQ に置き換え，全体に $\frac{1}{4^{-N}}$ を掛けて N を限りなく大きくすると，$O(1)$ の項は消すことができ次が得られる．

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

2. 系 2.19 より，

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

を得る．以下，1. と同様である．

□

この命題により，canonical height function が求めていた性質を満たすことがわかった．

ここまで見てきたように，height function というのは一つ一つの計算は容易であり，また，ある一定の height function の値以下の楕円曲線上の有理点は高々有限個しかないことがわかった．

一方，canonical height function というのは，一つ一つの計算は容易ではないが，2 次形式的な性質を持つので，理論的には非常に扱いやすいといえる．差を評価することにより，これら 2 つの長所を組み合わせて，より有効に活用することができるようになる．

3　乗法多項式について

この節では，まず主定理の主張を述べるのに必要な乗法多項式というものを定義し，基本的な性質を述べる．

定義 3.1 (**乗法多項式**)．E を K 上の楕円曲線とする．ただし，K の標数は 2 ではないものとする．

このとき，乗法多項式を次のような漸化式で定義する．

$$\begin{aligned}
&\phi_1(X,Y) := X,\\
&\phi_2(X,Y) := X^4 - b_4X^2 - 2b_6X - b_8,\\
&\psi_0(X,Y) := 0,\\
&\psi_1(X,Y) := 1,\\
&\psi_2(X,Y) := 2Y + a_1X + a_3,\\
&\psi_3(X,Y) := 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,\\
&\psi_4(X,Y) := \psi_2(X,Y)(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2\\
&\qquad\qquad + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)).
\end{aligned}$$

2 以上の整数 m に対して，

$$\begin{aligned}
&\phi_m(X,Y) := X\psi_m(X,Y)^2 - \psi_{m-1}(X,Y)\psi_{m+1}(X,Y),\\
&\psi_{2m+1}(X,Y) := \psi_{m+2}(X,Y)\psi_m(X,Y)^3 - \psi_{m-1}(X,Y)\psi_{m+1}(X,Y)^3,\\
&\psi_2(X,Y)\psi_{2m}(X,Y) := \psi_m(X,Y)(\psi_{m+2}(X,Y)\psi_{m-1}(X,Y)^2\\
&\qquad\qquad -\psi_{m-2}(X,Y)\psi_{m+1}(X,Y)^2.
\end{aligned}$$

この定義の意味は次の命題によりわかる．

命題 3.2. ϕ_m，$\psi_m \in K[X,Y]$ であり，任意の $E(K)$ の元 $P = (x,y)$ と 2 以上の整数 m に対して，

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

と表せる．また，$\psi_m(x,y) = 0$ であることと，$mP = O$ であることは同値である．

(証明は [4, Thm 1.19.] 参照.)

例 3.3. 実際に乗法多項式が正しいことをみる．

$$E : y^2 = x^3 + 1, \quad P = (2,3)$$

とする．このとき，

$$\begin{aligned}
&a_1 = a_2 = a_3 = a_4 = 0, \quad a_6 = 1,\\
&b_2 = b_4 = b_8 = 0, \quad b_6 = 4
\end{aligned}$$

である．命題 2.7 により，$x(2P)$，$x(3P)$，$x(4P)$ を計算すると，

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

となる．

また，ϕ_m，ψ_m をそれぞれ計算すると，

$$\begin{aligned}
&\phi_1(2,3) = 2,\\
&\phi_2(2,3) = 0,\\
&\psi_0(2,3) = 0,\\
&\psi_1(2,3) = 1,\\
&\psi_2(2,3) = 2 \times 3,\\
&\psi_3(2,3) = 3 \times 16 + 3 \times 4 \times 2 = 72,\\
&\psi_4(2,3) = 6(2 \times 2^6 + 10 \times 4 \times 2^3 - 16) = 2592,\\
&\psi_5(2,3) = 2592 \times 6^3 - 1 \times 72^3 = 186624,\\
&\phi_3(2,3) = 2 \times 72^2 - 6 \times 2592 = -5184,\\
&\phi_4(2,3) = 2 \times 2592^2 - 72 \times 186624 = 0
\end{aligned}$$

となる．よって，

$$\begin{aligned}
x(2P) &= \frac{0}{6^2} = 0,\\
x(3P) &= \frac{-5184}{72^2} = -1,\\
x(4P) &= \frac{0}{2592^2} = 0
\end{aligned}$$

となり，この場合乗法多項式が正しいことがわかる．

次に，乗法多項式の基本的な性質をいくつか述べるが，$P = (x, y) \in E(K)$ とすると，$\phi_m(x, y)$ と $\psi_m(x, y)^2$ は，x と前に定義した b_2, b_4, b_6, b_8 によって整数係数多項式とみなせるので，$\phi_m(x, y)$，$\psi_m(x, y)^2$ をそれぞれ x 変数の多項式とみることにする．

(**乗法多項式の基本的性質**)

1. ϕ_m は最高次係数 1 で次数は m^2 である．
2. ψ_m は最高次係数 m^2 で次数は $m^2 - 1$ である．
3. ϕ_m，ψ_m^2 は互いに素である．

(証明は [4] 参照) 1. と 2. の証明は主に計算によるので，3. のみ証明を与える．

3. **の証明**. m を ϕ_m と ψ_m^2 が既約因子 $\theta(X)$ を持つ最小の自然数と仮定する.
$m = 2k$ を偶数とする.
計算により次がわかる.

$$\Delta = \left(-48\frac{\phi_k^2(X)}{\psi_k^4(X)} - 8b_2\frac{\phi_k(X)}{\psi_k^2(X)} + b_2^2 - 32b_4\right)\psi_2\left(\frac{\phi_k(X)}{\psi_k^2(X)}\right) + \left(12\frac{\phi_k^3(X)}{\psi_k^6(X)} - b_2\frac{\phi_k^2(X)}{\psi_k^4(X)} - 10b_4\frac{\phi_k(X)}{\psi_k^2(X)} + b_2b_4 - 27b_6\psi_2^2\left(\frac{\phi_k(X)}{\psi_k^2(X)}\right)\right).$$

また，n，k を正の整数とすると，

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

となる．ここで $n = 2$ とすると，

$$\Delta = \left(-48\frac{\phi_k^2(X)}{\psi_k^4(X)} - 8b_2\frac{\phi_k(X)}{\psi_k^2(X)} + b_2^2 - 32b_4\right)\psi_2\left(\frac{\phi_k(X)}{\psi_k^2(X)}\right) + \left(12\frac{\phi_k^3(X)}{\psi_k^6(X)} - b_2\frac{\phi_k^2(X)}{\psi_k^4(X)} - 10b_4\frac{\phi_k(X)}{\psi_k^2(X)} + b_2b_4 - 27b_6\left(\frac{\phi_{2k}^2(X)}{\psi_k^8(X)}\right)\right)$$

となるので，$\theta(X)$ は $\phi_m(X)$，$\psi_m^2(X)$ の両方を割り切ることがわかる．よって，m が奇数の場合は 3. が示された.
m が奇数の場合もほぼ同様である.

□

以上により述べた乗法多項式は，主定理を述べるにあたって，非常に重要である.

4　準備

この節では，主定理の主張に必要な記号を準備する．

M_K を K の素点全体，M_K^0 を K の有限素点全体，M_K^∞ を K の無限素点全体として，$n_v = [K_v : \mathbb{Q}]$ とする．

$v \in M_K^\infty$ のとき，0 でない任意の K の元 x に対して，

$$|x|_v := q_v^{-\mathrm{ord}_v(x)/n_v},$$

$v \in M_K^\infty$ のときは，v に対応する埋め込み $\sigma : K_v \to \mathbb{C}$ に対して，

$$|x|_v := |\sigma(x)|$$

とする (ただし，右辺の絶対値は，通常の絶対値である)．

また，無限遠点を除けば $E(K_v)$ は，

$$\{(x, y) \in K_v \mid y^2 = x^3 + Ax + B\} \subset K_v^2$$

となるので，その部分位相を $E(K_v)$ の位相とする．また，O の近傍も同様に定義する．

まず始めに次の関数を定義する．

定義 4.1.

$$\Phi_{m,v} : E(K_v) \longrightarrow \mathbb{R},$$

$$\Phi_{m,v}(P) := \frac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}}.$$

ただし，$\Phi_{m,v}(O) := 1$ とする．

この関数について，次の命題を述べる．

命題 4.2. $\Phi_{m,v}$ は，$E(K_v)$ 上の有界連続関数であり，

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

である．

証明. まず連続性を示す．$\Phi_{m,v}$ は連続関数の絶対値と max による有理式なので，$P \neq O$ では連続である．$P = O$ で連続であることを示す．

前節で述べたように，ϕ_m は最高次係数 1 で次数は m^2 であり，ψ_m は最高次係数 m^2 で次数は $m^2 - 1$ であるので，

$$\lim_{P \to O} \Phi_{m,v}(P) = 1$$

が成り立つ．よって，$P = O$ でも連続である．

有界性は，任意の v に対して，$E(K_v)$ がコンパクトであることより得られる．

最後に後半部分を背理法によって示す．

$\inf_{v\in E(K_v)} \Phi_{m,v}(P) = 0$ とする．$E(K_v)$ のコンパクト性より，ある $P \in E(K_v)$ が存在して，$\Phi_{m,v}(P) = 0$ が成り立つ．$P = O$ であるので定義より，$\phi_m(x(P)) = \psi_m^2(x(P)) = 0$ を得るが，前節でみた乗法多項式の性質より，ϕ_m，ψ_m^2 は互いに素なので，これは矛盾である．よって，後半部分が示された． □

height function は局所的な値の和で定義されているので，canonical height function も同様に局所的なものの和で表したい．そのために次に，local height function を定義する．

定義 4.3 (**local height function**)**.** 楕円曲線 E 上の local height function を次のように定義する．

$$\lambda_v : E(K_v) \setminus \{O\} \longrightarrow \mathbb{R},$$

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

一般的には、$m = 2$ の場合に local height function と言われるが，m が 3 以上の場合に一般化したというのが重要なアイデアである．

次にこの関数を用いて，canonical height function が局所的なものの和で表されることを示す．

命題 4.4. 任意の $P \in E(K) \setminus \{O\}$ に対して，

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

と表せる．ここで，$n_v = [K_v : \mathbb{Q}_v]$ である．

$m = 2$ の場合を示すが，m が 3 以上の場合も実は $m = 2$ の場合と同様の結果が得られる．

証明. 関数 L を次のように定義する．

$$L : E(K) \setminus \{O\} \to \mathbb{R}, \quad L(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v\in M_K} n_v \lambda_v(P).$$

また，S を次のように定義する．$v(\cdot) = -\log |\cdot|_v$ とするとき，$S \subset M_K$ で，任意の $v \in S$ に対して，次が成り立つ．

$$\lambda_v(P) = \frac{1}{2} \max\{v(x(P)^{-1}), 0\}.$$

このようにすると，任意の $P \in E(K) \setminus \{O\}$ に対して，もし $v \notin S$ かつ $v(x(P)) \geq 0$ ならば，$\lambda_v(P) = 0$ が成り立つ．

次に $L(P)$ と $h(x(P))$ の差を評価する．任意の $v \in M_K$ に対して，次を満たすある定数 C_v が存在する．

$$-c_v \leq \lambda_v(P)\frac{1}{2}\max\{v(x(P)^{-1}), 0\} \leq c_v.$$

よって，次が成り立つ．

$$-c \leq L(P) - \frac{1}{2}h(x(P)) \leq c.$$

ここで，$c = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S} n_v c_v$ である．よって，

$$L(P) = \frac{1}{2}h(x(P)) + O(1)$$

を得る．また，

$$\begin{aligned} L(2P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S} n_v\lambda_v(2P) &= \frac{4}{[K:\mathbb{Q}]}\sum_{v\in S} n_v\lambda_v(P), \\ &= 4L(P) \end{aligned}$$

が得られる．よって $F = L - \hat{h}$ とすると，これは有界であり，$F(2P) = 4F(P)$ が成り立つ．ゆえに，

$$F(P) = \frac{1}{4^N}F(2^N P) \to 0 \quad (N \to \infty).$$

よって，$L = \hat{h}$ が得られた． □

この命題によって，height と canonical height の差が次のように表されることがわかる．

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

よって，次の関数を定義することにする．

定義 4.5.

$$\Psi_v : E(K_v) \longrightarrow \mathbb{R}$$

$$\Psi_v(P) := \log\max\{1, |x(P)|_v\} - \lambda_v(P)$$

とする．ただし，$\Psi_v(O) := 0$ とする．

この関数が全ての素点で有界連続ならば，全ての素点での評価を足しあわせれば，差の評価が得られることがわかる．

命題 4.6. 任意の $v \in M_K$ に対して，Ψ_v は $E(K_v)$ 上の有界連続関数である．

証明. まず，連続性を示す.

定義より，任意の $P \in E(K_v)$ に対して，

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

が成り立つ．$\Phi_{2,v}$ は連続有界だったので，$\log \Phi_{2,v}$ も連続有界である．よって右辺は一様収束するので，Ψ_v は $E(K_v)$ 上の連続関数であることがわかる.

有界性は $E(K_v)$ のコンパクト性より得られる． □

5　主定理の証明

前節の命題により，Ψ_v を全ての素点で評価すればよいことがわかったので，実際に有限素点と無限素点に分けて評価するのだが，有限素点に関しては，2006 年に J. E. Cremona，M. Prickett，S. Siksek の 3 氏により，次のようなもっとも良い結果 (つまり，イコールの形) が得られているので次に述べる．

命題 5.1. (**J. E. Cremona, M. Prickett, S. Siksek** [1, 2006]).
v を K の任意の有限素点とする．このとき，

$$\inf_{P\in E(K_v)} \Psi_v(P) = 0$$

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

である．

ただし，$\Delta_v^{\min}$ は E の v における極小判別式であり，α_v は小平タイプと玉河数により決まる値で，詳細は次の表の通りである．

E の v による小平型	E の v による玉河数	α_v
任意	1	0
I_m,m は偶数	2 または m	$m/4$
I_m,m は奇数	m	$m(m^2-1)/4m$
III	2	1/2
IV	3	2/3
I_0^*	2 または 4	1
I_0^*	2	1
I_0^*	4	$(m+4)/4$
I_0^*	3	4/3
III^*	2	3/2

有限素点に関してはこのような最良の評価が得られているので，次に無限素点に関する評価を与えるために，次の値を定義する．

定義 5.2. $\epsilon_{m,v}$，$\delta_{m,v}$ をそれぞれ次のように定義する．

$$\epsilon_{m,v}^{-1} := \inf_{P\in E(K_v)} \Phi_v(P),$$

$$\delta_{m,v}^{-1} := \sup_{P\in E(K_v)} \Phi_v(P).$$

前にみた命題 4.2 により，常にこの 2 つの値は存在することがわかる．
さらに，次の値も定義する．

定義 5.3. $S_v(m)$，$T_v(m)$ をそれぞれ次のように定義する．

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

以上を用いて実際に無限素点を評価する．

命題 5.4. $m \in \mathbb{Z}_{\geq 2}$，$v \in M_K$(特に M_K^∞) とする．このとき，

$$S_v(m) \leq \Psi_v(P) \leq T_v(m)$$

が成り立つ．

証明. $P = O$ のときは明らかに成り立つ．
$P \neq O$ とする．λ_v の定義より，

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

を得る．また，ϵ，δ の定義より，

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

となり，さらに，等比数列の無限和の公式より，

$$\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} = \frac{1}{m^2-1}$$

が得られるので，以上を組み合わせればよい． □

以上により示された 2 つの命題によって，無限素点，有限素点をそれぞれ評価して和をとれば，主定理は示される．

定理 5.5. (**主定理**, **Y. Uchida** [8, 2008]). m を 2 以上の整数とする．このとき，任意の $P \in E(K)$ に対して，

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

ただし，記号は前に述べたとおりである．

6 mについて

この節では，m による評価の値の変化をみることにする．

命題 6.1. $m \geq 2$，$l \geq 1$ をそれぞれ整数とする．このとき，

$$S_v(m) \leq S_v(m^l),$$

$$T_v(m^l) \leq T_v(m)$$

が成り立つ．

この命題により，m を m^l に変えれば評価は少なくとも悪くはならないことがわかる．

この命題の証明には，以下の 3 つの補題を必要とする．

補題 6.2. $v \in M_K$，m を正の整数とする．このとき，任意の $P \in E(K_v)$ に対して，

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

が成り立つ．

証明. $m = 1$ のときは明らかであるので，$m \geq 2$ とする．

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

が成り立つので求める結果が得られた． □

補題 6.3. $v \in M_K$， m, m' を正の整数とする
このとき，任意の $P \in E(K_v)$ に対して，

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

が成り立つ．

証明. 補題 6.2 より，次の 3 つの式が得られる．

$$\Psi_v(mP) = \log \Psi_{m,v}(P) + m^2 \Psi_v(P), \tag{6.4}$$

$$\Psi_v(mm'P) = \log \Psi_{m',v}(P) + m'^2 \Psi_v(mP), \tag{6.5}$$

$$\Psi_v(mm'P) = \log \Psi_{mm',v}(P) + mm'^2 \Psi_v(P). \tag{6.6}$$

$m'^2 \times (6.4) + (6.5) - (6.6)$ を計算すると，次の求める結果が得られる．

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

□

補題 6.7. $v \in M_K$ とし，$m \geq 2$，$l \geq 1$ をともに整数とする．
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 6.3 と $\Phi_{1,v}(P) = 1$ より，

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

となり示された． □

命題 6.1 の証明. 補題 6.7 の式の両辺から下極限をとると，

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

が得られる．よって，

$$\frac{\log \epsilon_{m,v}}{m^2-1} \geq \frac{\log \epsilon_{m^l,v}}{m^{2l-1}}$$

となるので，

$$T_v(m^l) \leq T_v(m)$$

が得られる．S_v についても同様である． □

注 6.8. $m' \leq m$ であっても，必ずしも

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

となるとは限らない (後に反例を挙げる)．

次に，m を限りなく大きくしたとき，評価がどのようになるのかをみる．

命題 6.9. $v \in M_K$，$m \geq 2$ とする．このとき次が成り立つ．

$$0 \leq \inf_{P \in E(K_v)} \Psi_v(P) - S_v(m) \leq \frac{1}{m^2-1} \left(\sup_{P \in E(K_v)} \Psi_v(P) - \inf_{P \in E(K_v)} \Psi_v(P) \right),$$

$$0 \leq T_v(m) - \inf_{P \in E(K_v)} \Psi_v(P) \leq \frac{1}{m^2-1} \left(\sup_{P \in E(K_v)} \Psi_v(P) - \inf_{P \in E(K_v)} \Psi_v(P) \right).$$

証明. 命題 5.4 より，

$$0 \leq T_v(m) - \inf_{P \in E(K_v)} \Psi_v(P)$$

が得られる．また，補題 6.2 より，

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

となるので，両辺から下極限をとって，計算すると，

$$T_v(m) - \inf_{P \in E(K_v)} \Psi_v(P) \leq \frac{1}{m^2-1} \left(\sup_{P \in E(K_v)} \Psi_v(P) - \inf_{P \in E(K_v)} \Psi_v(P) \right).$$

$S_v(m)$ についてもほぼ同様である．

□

よって，Ψ_v の有界性より直ちに次の系が得られる．

系 6.10.

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

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

が成り立つ．

この命題により，この評価はある意味最も良い評価といえる．

7　別の評価の紹介と比較

height と canonical height の差の評価に関しては，Silverman と Zimmer によってそれぞれ与えられているので，まず始めにそれらの結果を紹介する．

定理 7.1. (**Silverman** [6, 1990]). 任意の $x \in K$ に対して，

$$h(x) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max\{1, |x|_v\},$$

$$h_\infty(x) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} n_v \log \max\{1, |x|_v\},$$

$$2^* := 2 \qquad b_2 \neq 0,$$

$$2^* := 1 \qquad b_2 = 0$$

と定義する．さらに，

$$\nu(E) := \frac{1}{12} h(\Delta) + \frac{1}{12} h_\infty(j) + \frac{1}{2} h\infty \left(\frac{b_2}{12}\right) + \frac{1}{2} \log 2^*$$

と定義すると，
任意の $P \in E(\bar{K})$ に対して，

$$-2\nu(E) - 2.14 \leq h(P) - \hat{h}(P) \leq \frac{1}{12} h(j) + 2\nu(E) + 1.946$$

が成り立つ．

定理 7.2. (**Zimmer** [9, 1976]). $x \in K, v \in M_K$ に対して，$v(x) := -\log |x|_v$ として，

$$\mu := \min \left\{ v(b_2), \frac{v(b_4)}{2}, \frac{v(b_6)}{3}, \frac{v(b_8)}{4} \right\}$$

と定義する．さらに，

$$\mu_l := -\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \min\{0, \mu_v\},$$

$$\mu_h := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \min\{0, \mu_v\},$$

$$\mu := -\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \mu_v = \mu_l - \mu_h,$$

と定義すると，
任意の $P \in E(\bar{K})$ に対して，

$$-\mu_l - \log 2 \leq h(P) - \hat{h}(P) \leq 2\mu + \mu_h + \frac{8}{3} \log 2$$

が成り立つ．

まず，これらの定理の評価と主定理の評価の比較を内田氏の例によってみて，続いて差を評価することが実際にどのようなことに役に立つのかをみてみる．

例 7.3. [8, Ex 27]

$$E : y^2 = x^3 - 459x^2 - 3478x + 169057$$

を考えることにする．

この楕円曲線は rank が 4 であり，

$$P_1 = (16, -1),\ P_2 = (-4, -419),\ P_3 = (-22, -113),\ P_4 = (566, -5699)$$

の 4 つを基底に持つ．

主定理によれば次の評価が得られる．

$$\begin{aligned}
&-6.531924724 \leq h - \hat{h} \leq 0.4620981204 && (m = 2),\\
&-5.228881425 \leq h - \hat{h} \leq 0.4620981204 && (m = 3),\\
&-5.227187136 \leq h - \hat{h} \leq 0.4620981204 && (m = 4),\\
&-5.006931796 \leq h - \hat{h} \leq 0.4620981204 && (m = 5).
\end{aligned}$$

Silverman の定理によれば，

$$-15.40309857 \leq h - \hat{h} \leq 18.74780624,$$

Zimmer の定理によれば，

$$-8,208491752 \leq h - \hat{h} \leq 1641698351$$

がそれぞれ得られる．

よって，この場合には主定理が他の 2 つの定理よりもかなり優れていることがわかる．

実際，$P = 2P_1$ とすれば，

$$h(P) - \hat{h}(P) = 0.462098788.....,$$

$P = P_1 - 3P_2 + P_3 + 3P_4$ とすれば，

$$h(P) - \hat{h}(P) = -4.900153342.....,$$

という値が得られるので，この場合は主定理の評価が上からも，下から優れている．

次に，主定理の $m = 5$ の場合を用いて，P_1 が原始的であることを示す．$P_1 = (16, -1)$ なので，

$$h(P_1) = \log 16 = 2.77....$$

また，$\hat{h}(P_1)$ を計算すると，$\hat{h}(P_1) = 4.41....$ を得る．

主定理より，$-5.01 \leq h - \hat{h} \leq 0.47$ なので，$E(\mathbb{Q})$ の元 R と, 絶対値が 2 以上の整数 n に対して，$nR = P_1$ と表せたとする．

canonical height function の性質より，

$$\hat{h}(R) = \frac{1}{n^2}\hat{h}(P) \leq \frac{1}{4}\hat{h}(P) = 0.69...$$

を得る．よって，主定理の結果より

$$h(R) \leq \hat{h}(R) + 0.47 \leq 1.2$$

となり，$e^{1.2} < 4$ なので，$x(R)$ が $\{\pm\frac{m}{n} \mid 0 \leq m \leq 4,\ 1 \leq n \leq 4,\ m, n \in \mathbb{Z}\}$ の範囲の高々19 個の点を調べればよいが，実際に

$$f(x) := x^3 - 459x^2 - 3478x + 169057$$

として計算してみると，

$$\begin{aligned}
&f(1) = 165121 = 11 \times 17 \times 883, \quad f(2) = 160273 = 83 \times 1931,\\
&f(3) = 154519 = 191 \times 809, \quad f(-1) = 172075 = 5^2 \times 6883,\\
&f(-2) = 174169, \quad f(-3) = 175333, \cdots\cdots,
\end{aligned}$$

となるので，どの値を代入しても有理数の平方にはならないので，上で仮定したような $E(\mathbb{Q})$ の元はないことがわかるので，$n = \pm 1$ であり，よって P_1 は原始的であることがわかる．

最後に前にみた注 6.5 で述べておいた反例をみてみる．

例 7.4. [8, Ex 29]

$$E : y^2 + y = x^3 - x$$

とする．

このとき，主定理によれば,

$$-0.48648 \leq h - \hat{h} \leq 0.12298 \qquad (m = 3),$$

$$-0.46933 \leq h - \hat{h} \leq 0.12650 \qquad (m = 6)$$

が得られる．

よって．$m = 3$ のほうが上からの評価がよいことがわかる．

例 7.5. [8, Ex 30]

$$E : y^2 = x^3 - 52x + 100$$

とする．

このとき，主定理によれば，

$$-2.1041 \leq h - \hat{h} \leq 1.8394 \qquad (m = 5),$$

$$-2.1193 \leq h - \hat{h} \leq 1.8394 \qquad (m = 10)$$

が得られる．

よって，$m = 5$ のほうが下からの評価がよいことがわかる．

参考文献

[1] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, Vol. 116, No. 1, pp. 42–68, 2006.

[2] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, No. 47, pp. 33–186 (1978), 1977.

[3] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, Vol. 44, No. 2, pp. 129–162, 1978.

[4] Susanne Schmitt and Horst G. Zimmer. *Elliptic curves*, Vol. 31 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, 2003. A computational approach, With an appendix by Attila Pethö.

[5] Joseph H. Silverman. *The arithmetic of elliptic curves*, Vol. 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[6] Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, Vol. 55, No. 192, pp. 723–743, 1990.

[7] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, Vol. 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[8] Yukihiro Uchida. The difference between the ordinary height and the canonical height on elliptic curves. *J. Number Theory*, Vol. 128, No. 2, pp. 263–279, 2008.

[9] Horst Günter Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, Vol. 147, No. 1, pp. 35–51, 1976.