数理解析研究所講究録
第1767巻 2011年 125-132

楕円曲線 $y^2 = x^3 + n$ のモーデル・ヴェイユ群について

東北大学大学院理学研究科　奈良　忠央　(Tadahisa Nara)
Mathematical Institute,
Tohoku University

1　導入

本稿ではある楕円曲線（有理数体上）の族を考える．それらは明示的なかたちの整数点をもっており、その整数点が楕円曲線のモーデル・ヴェイユ群の生成元として使えるものであるかを楕円曲線の canonical height を使ったアプローチで考える．よく知られているとおり、代数体上の楕円曲線のモーデル・ヴェイユ群は有限生成アーベル群であり、その free part の基底をモーデル・ヴェイユ基底と呼ぶことにする．

2　主結果と周辺の結果

Duquesne は simplest quartic field に付随する楕円曲線の考察を行い、その中の結果のひとつとして以下の定理を示した．

定理 2.1 ([2], 2007). $k \in \mathbb{Z}$, $n := 16 + (6k^2 + 2k - 1)^2$ とし E を楕円曲線

$$y^2 = x^3 - nx$$

とする．n は奇数の平方で割れないと仮定する．このとき2点 $(-4, 2(6k^2 + 2k - 1))$, $(-2k^2 + 2k + 1, 4(k + 1)(2k^2 - 2k + 1))$ は $E(\mathbb{Q})$ のモーデル・ヴェイユ基底の一部になることができる．

注 2.2. 特に、これはランク2以上の楕円曲線の族であり、ランクがちょうど2のものは上の2点とトーション点 $(0, 0)$ によってモーデル・ヴェイユ群が生成される．

これはいわゆる $y^2 = x^3 - nx$ というかたちの族のなかの部分族になっており、$y^2 = x^3 - x$ のツイストと見ることもできる．またこれについては Fujita, Terai により拡張も行われている．([3])

本稿では同様に多く研究されてきた $y^2 = x^3 + n$ のかたちの楕円曲線の族を考える. 具体的には a, b を互いに素な正の整数とし

$$E_{a,b} : y^2 = x^3 + a^6 + 16b^6$$

を $\mathbb{Q}$ 上の楕円曲線とし、その上の整数点を

$$P_1 = (-a^2, 4b^3),\ P_2 = (2ab, a^3 + 4b^3),\ P_3 = (-2ab, a^3 - 4b^3).$$

とする. これについて我々は以下を示すことができる.

定理 2.3. $a^6 + 16b^6$ が *square-free, ab* が奇数 でかつ $3||b$ を仮定する. このとき モーデル・ヴェイユ群 $E_{a,b}(\mathbb{Q})$ は少なくともランク 3 で、また $\{P_i, P_j\}$ $(i = 1, 2, 3,\ i \neq j)$ のうちのどの 2 点の組もモーデル・ヴェイユ基底の一部になることができる.

注 2.4. $y^2 = x^3 + n$ というかたちの楕円曲線のトーションは分類されており（例えば *[4, Theorem 5.3]*）、それによりこの $E_{a,b}(\mathbb{Q})$ はトーションを持たないことが容易にわかり、当然この 3 点はトーション点ではない.

一般に、有限生成アーベル群の free part の独立な点 Q_1, Q_2, ..., Q_s にたいし、$Q_1, Q_2, ..., Q_s \in \langle G_1 \rangle + \langle G_2 \rangle + \cdots + \langle G_s \rangle$ を満たすようにモーデル・ヴェイユ基底 $\{G_1, G_2, ..., G_r\}$ $(s \leq r)$ をとることができるが、このときの群指数 $[\langle G_1 \rangle + \langle G_2 \rangle + \cdots + \langle G_s \rangle : \langle Q_1 \rangle + \langle Q_2 \rangle + \cdots + \langle Q_s \rangle]$ を $\{Q_1, Q_2, ..., Q_s\}$ の格子指数と呼ぶことにする.

したがって上の定理の 2 つ目の主張は $\{P_i, P_j\}$ $(i = 1, 2, 3,\ i \neq j)$ のうちのどの 2 点の組も、その格子指数は 1 である、と言い換えることができる.

定理の証明の大枠は Duquesne のものと同様で、大きくは二つのパートからなっている. 一つは descent の議論で 3 点の独立性及び格子指数が 2, 3, 4 でないことを示し、もう一つは canonical height の議論により格子指数が 5 より小さいことを示す.

3 点の独立性

以下 $m_{a,b} := a^6 + 16b^6$ と置く.

上述の一つ目のパートは以下の命題の主張そのものである.

命題 3.1. $m_{a,b}$ が *square-free, ab* が 奇数かつ $3||b$ と仮定する. このとき P_1, P_2, P_3, $P_1 + P_2$, $P_2 + P_3$, $P_1 + P_3$, $P_1 + P_2 + P_3 \notin 2E_{a,b}(\mathbb{Q})$ であり、また P_1, P_2, P_3, $P_1 \pm P_2$, $P_2 \pm P_3$, $P_1 \pm P_3$, $P_1 + P_2 \pm P_3$, $P_1 - P_2 \pm P_3 \notin 3E_{a,b}(\mathbb{Q})$ が成り立つ. 特に, P_1, P_2, P_3 は独立であり $\{P_1, P_2, P_3\}$, $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ の格子指数は 2 と 3 で割れない.

この命題の証明は P_1, P_2, P_3, $P_1 + P_2$, ... の各点において一つずつ具体的に計算し、以下の 2 つの補題を使って調べてゆけばよい.

補題 3.2. n を整数とし、$E/\mathbb{Q}$ を楕円曲線 $y^2 = x^3 + n$、$Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$ とする．ここで、$E(\mathbb{Q})_{\mathrm{tors}}$ は $E(\mathbb{Q})$ のトーション部分群とする．また Q の x 座標 $x(Q) = u/s^2$ $(\gcd(u,s) = 1)$ と書くとする．このとき以下のいずれの場合も $Q \notin 2E(\mathbb{Q})$ が成り立つ．

(1) n : 奇数, $u \not\equiv 0 \pmod 8$, s : 奇数,

(2) $n \equiv 1 \pmod 9$, $u \equiv 2 \pmod 3$, $s \not\equiv 0 \pmod 3$.

注 3.3. 実際には $\gcd(u,s) = 1$ という条件は必要ないことが、簡単なチェックによりわかる．

補題 3.4. n を整数とし、$E/\mathbb{Q}$ を楕円曲線 $y^2 = x^3 + n$、$Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$ とする．また $x(Q) = u/s^2$ $(\gcd(u,s) = 1)$ と書くとする．このとき以下のいずれの場合も $Q \notin 3E(\mathbb{Q})$ が成り立つ．

(1) n : 奇数, u : 偶数,

(2) $n \equiv 1 \pmod 9$, $u \equiv 1 \pmod 3$, $3 \| s$.

以下命題 3.1 の前半から後半の独立性が従う部分を補題として記す．

補題 3.5. A を有限生成アーベル群としトーションをもたないと仮定する．このとき A の元 P, Q, R が条件: P, Q, R, $P+Q$, $Q+R$, $P+R$, $P+Q+R \notin 2A$ を満たすならば P, Q, R は独立である．

証明. $kP+lQ+mR = 0$ のとき k,l,m のうち奇数のものがあると、条件に反する．よって k,l,m はすべて偶数．そこで $(k,l,m) = (2k', 2l', 2m')$ と書けば $k'P+l'Q+m'R = 0$ となり同じ議論を繰り返すことができるが、k,l,m のうち 0 でないものがあればあるところで止まり、そこで条件に反する．よって $(k,l,m) = (0,0,0)$. □

4 Canonical height

のこりのパートは canonical height をつかった議論になる．具体的には点 P_1, P_2, P_3 の canonical height の評価を求め、一方で $E_{a,b}(\mathbb{Q})$ のすべての点にわたる canonical height の下界を求める．そしてそれらを少し先で述べる Siksek による定理に適用することにより、格子指数が 5 より小さいことが言える．

ここで少し canonical height について復習する．楕円曲線上の点 $P = (x,y)$ $(x = n/d,$ $\gcd(n,d) = 1)$ にたいして naïve height を $h(P) = \max\{\log|n|, \log|d|\}$ で定義し、canonical height を

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

で定義する．さらに続けて Q_i, $Q_j \in E(\mathbb{Q})$ の height pairing を

$$\langle Q_i, Q_j \rangle = \frac{1}{2}\left(\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)\right)$$

で定義し、

$$R(Q_1, Q_2, ..., Q_s) = \det\left(\langle Q_i, Q_j\rangle\right)_{1\le i,j\le s}$$

と定義する. canonical height はモーデル・ヴェイユ群の free part 上の正値対称二次形式であり、モーデル・ヴェイユ基底 $\{G_1, G_2, ..., G_r\}$ を使って $P = x_1G_1 + x_2G_2 + \cdots + x_rG_r$ と表したとき $\hat{h}(P) = {}^t\mathbf{x}\left(\langle G_i, G_j\rangle\right)_{1\le i,j\le s}\mathbf{x}$ となる. ただし $\mathbf{x} = {}^t(x_1, x_2, ..., x_r)$ とする. 特に $\hat{h}(kP) = k^2\hat{h}(P)$ が成り立つ.

一般の二次形式の理論を canonical height に適用することによって次の定理が得られる.

定理 4.1. (Siksek, [5, Theorem 3.1]) E/K を代数体 K 上のランク r (≥ 2) の楕円曲線とし、$Q_1, Q_2, ..., Q_s$ $(s \le r)$ を独立な $E(K)$ の点、ν を $\{Q_1, Q_2, ..., Q_s\}$ の格子指数とする. ある実数 $\lambda > 0$ が存在して任意のトーションでない点 $P \in E(K)$ にたいし $\hat{h}(P) > \lambda$ が満たされていると仮定する. このとき

$$\nu \le R(Q_1, Q_2, ..., Q_s)^{1/2}(\gamma_s/\lambda)^{s/2}. \tag{4.2}$$

ただし、γ_s はエルミート定数と呼ばれるもので、たとえば

$$\gamma_1^1 = 1,\ \gamma_2^2 = 4/3,\ \gamma_3^3 = 2,\ \gamma_4^4 = 4,\ \ldots$$

であることが知られている.

5 Local height

canonical height の評価は、具体的な計算で通常行われている通り local height による分解をつかって行う.

定理 5.1. (Néron, Tate, [6]) K を代数体、v をその素点、K_v を $|\cdot|_v$ についての完備化とする. E を楕円曲線 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $(a_1, a_2, a_3, a_4, a_6 \in K)$ とする. このとき以下の3つの性質を満たす関数 $\hat{\lambda}_v : E(K_v) \setminus O \to \mathbb{R}$ が唯一つ存在する.

(1) $2P \ne O$ となるすべての $P \in E(K_v)$ にたいして等式

$$\hat{\lambda}_v(2P) = 4\hat{\lambda}_v(P) - 2\log|2y(P) + a_1x(P) + a_3|_v.$$

をみたす.

(2) 極限 $\lim_{\substack{P\to O\\ v\text{-}adic}}(\hat{\lambda}_v(P) - \log|x(P)|_v)$ が存在する.

(3) O の任意の近傍 *(v-adic)* の補集合上で $\hat{\lambda}_v$ は有界である.

注 5.2. この $\hat{\lambda}_v$ を *local height function* と呼ぶ．本稿では参照元の *canonical height* の2倍の値を *canonical height* の定義としていることに注意されたい．したがって *local height function* も2倍で定義している．また *local height function* には別の流儀もあって性質 *(1)* の右辺に $\frac{1}{2}\log|\Delta|_v$ を加えた形での定義もある．その場合、定義体上任意のワイエルシュトラスモデルの変換において値が保たれる．一方本稿での定義ではそうは言えないが、x 軸方向のずらしの変換においては値が保たれる．

canonical height は local height に分解できることが知られており、我々が考えている $K=\mathbb{Q}$ の場合

$$\hat{h}(P)=\sum_{p:\text{prime}}\hat{\lambda}_p(P)+\hat{\lambda}_\infty(P)$$

となる．

local height function の計算についてはいくつかの公式があり、それを使い分ける．素点が非アルキメディアンの場合、おおまかには還元のタイプによって決まり、Silverman によるアルゴリズム ([6, THEOREM 5.2]) がある．それをもとに $y^2=x^3+n$ についてまとめた結果が以下の補題である．

補題 5.3. n を *square-free* な整数とし、E を楕円曲線 $y^2=x^3+n$ とする．$P=(\alpha/\delta^2,\beta/\delta^3)$ $(\alpha,\beta,\delta\in\mathbb{Z},\ \delta>0,\ \gcd(\alpha,\delta)=\gcd(\beta,\delta)=1)$ を E の有理点とする．このとき

$$\sum_{p:prime}\hat{\lambda}_p(P)=2\log\delta+\lambda_2'(P)+\lambda_3'(P),$$

ここで、

$$\lambda_2'(P)=\begin{cases}0 & (\mathrm{ord}_2(\alpha)=0),\\ -\frac{2}{3}\log 2 & (\mathrm{ord}_2(\alpha)\neq 0),\end{cases}$$

$$\lambda_3'(P)=\begin{cases}0 & (\mathrm{ord}_3(\beta)=0),\\ -\frac{1}{2}\log 3 & (\mathrm{ord}_3(\beta)\neq 0).\end{cases}$$

とする．

素点がアルキメディアンの場合には2つの公式がある．ひとつは Tate による級数をつかったものである．$b_2, b_4, b_6, b_8\in\mathbb{Z}[a_i]$ $(i=1,2,3,4,6)$ を 通常使われる、E のワイエルシュトラス方程式によってきまる量とする．

定理 5.4. (Tate) ある $\epsilon>0$ が存在して 任意の $Q\in E(\mathbb{R})$ で $|x(Q)|>\epsilon$ を満たすとする．このとき

$$\hat{\lambda}_\infty(P)=\log|x(P)|+\frac{1}{4}\sum_{n=0}^{\infty}4^{-n}\log|z(2^nP)|,$$

ここで $z(P)=1-b_4/x(P)^2-2b_6/x(P)^3-b_8/x(P)^4$ とする．

注 5.5. ψ_2 を *division polynomial* としたとき $z(P)$ は $z(P)x(P)^4 = \psi_2(P)^2 x(2P)$ という関係式を満たす.

この定理は $|x(Q)| > \epsilon$ という条件があるためこのままでは $E_{a,b}$ に適用できないが、x 軸方向にずらしたワイエルシュトラスモデルで考えることにより解決できる. これを使って $\hat{h}(P_1), \hat{h}(P_2), \hat{h}(P_3)$ の評価を求める.

もう一つの公式はテータ関数を使ったものである.

定理 5.6 ([1], Algorithm 7.5.7).

$$\hat{\lambda}_\infty(P) = \frac{1}{16}\log\left|\frac{\Delta}{q}\right| + \frac{1}{4}\log\left(\frac{\omega_1 y(P)^2}{2\pi}\right) - \frac{1}{2}\log|\theta|,$$

ここで ω_1, ω_2 は E の周期で $\omega_1 > 0$, $\mathrm{Im}(\omega_2) > 0$, $\mathrm{Re}(\omega_2/\omega_1) = -1/2$ をみたすものとし、$q = \exp(2\pi i\omega_2/\omega_1)$, $\theta = \sum_{n=0}^{\infty}(-1)^n q^{\frac{n(n+1)}{2}} \sin\{2\pi(2n+1)\mathrm{Re}(z_P)/\omega_1\}$, Δ は E の *discriminant*, z_P は P の *elliptic logarithm* とする.

こちらは有理点全体（トーション除く）をわたるときの canonical height の下界を求めるのに使う.

6 Canonical height の評価

まず前節で述べたとおり $\hat{\lambda}_\infty(P_1), \hat{\lambda}_\infty(P_2), \hat{\lambda}_\infty(P_3)$ を定理 5.4 を使って考える. その際、x 軸方向に d ずらしたモデル $y^2 = (x-d)^3 + m_{a,b}$ で考える. つまり P_1, P_2, P_3 に対応する点を P_1', P_2', P_3' と書けば、$P_1' = (-a^2+d, 4b^3)$, $P_2' = (2ab+d, a^3+4b^3)$, $P_3' = (-2ab+d. a^3-4b^3)$ となる. ここでは例えば $d = 2a^2+4b^2$ とおいて $\hat{\lambda}_\infty(P_2')$ を計算すると、

$$\begin{aligned}
\hat{\lambda}_\infty(P_2') &= \log|x(P_2')| + \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n}\log|z(2^n P_2')| \\
&= \log(2ab+2a^2+4b^2) \\
&+ \frac{1}{4}\log\left(\frac{X^8-2X^7+2X^6+8X^5+2X^4+16X^3+16X^2-32X+32}{2X^8+8X^7+28X^6+56X^5+98X^4+112X^3+112X^2+64X+32}\right) \\
&+ \frac{1}{4^2}\log(\cdots) \\
&+ \cdots
\end{aligned}$$

となる. ただし $X = a/b$ と置いた. この各項は初等的な微分によって評価できる（コンピュータ使用）が、項は無限にあるので $1/4^3\log|z(2^2P_2')|$ のところまでのバウンドを求め、あとは寄与が小さいことから、粗いが一様なバウンド $0.062326 < z(P') < 120.351634$ (P' はずらしたモデルの点) を使う. こうして

$$\frac{1}{3}\log m_{a,b} - 0.295724 < \hat{\lambda}_\infty(P_2') < \frac{1}{3}\log m_{a,b} + 1.513566.$$

が求まる.

次に

$$\sum_{p:\text{prime}} \hat{\lambda}_p(P_2) = -\frac{2}{3}\log 2$$

であることは補題5.3から直ちにわかり、足し合わせることによって $\hat{h}(P_2)$ のバウンドが得られる. P_1, P_3 についても同様の考え方ができ、次の命題を得る.

命題 6.1. 定理 *2.3* と同じ状況のもとで

$$\frac{1}{3}\log m_{a,b} - 0.7441 < \hat{h}(P_1) < \frac{1}{3}\log m_{a,b} + 0.5409,$$
$$\frac{1}{3}\log m_{a,b} - 0.7579 < \hat{h}(P_2) < \frac{1}{3}\log m_{a,b} + 1.0515,$$
$$\frac{1}{3}\log m_{a,b} - 0.5113 < \hat{h}(P_3) < \frac{1}{3}\log m_{a,b} + 0.5665.$$

この後は $E_{a,b}(\mathbb{Q})$ の点全体（トーション除く）をわたるときの canonical height の下界を考えるのだが、結論は以下の命題である.

命題 6.2. n を正の *square-free* な整数とし E を楕円曲線 $y^2 = x^3 + n$、$P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\text{tors}}$ とする. このとき

$$\hat{h}(P) > \frac{1}{12}\log n - 0.147152.$$

注 6.3. これの証明では $y^2 = x^3 + m_{a,b}$ のかたちであることは必要ないので $y^2 = x^3 + n$ のかたちで与えた.

証明の概要としては、まずトーションでない点を $P = (\alpha/\delta^2, \beta/\delta^3)$ と置いて定理5.6をつかって $\hat{\lambda}_\infty$ を計算すると、

$$\hat{\lambda}_\infty(P) > \frac{1}{12}\log n + \frac{1}{2}\log\left|\frac{\beta}{\delta^3}\right| + 0.3149468597\cdots$$

という評価が得られる. この計算では、q は $\mathbb{R}$ 上の同型で一定であること、$\omega_1 = n^{-\frac{1}{6}}\cdot\omega_1'$ (ω_1' は $y^2 = x^3 + 1$ の周期とする) であること、$|\theta| < 1 + |q| + |q|^3 + |q|^6 + |q|^{10}\cdot\frac{1}{1-|q|^5}$ であることに着目し数値計算している. 次に、これに補題5.3をあわせるとうまく β, δ によらない下界が求められて命題6.2を得る.

7 Siksek の定理と主定理の証明

ここまでで Siksek の定理 (定理 4.1) 使うための準備ができた.

定理 *2.3* の証明. まず命題 3.1 により 3 点は独立でまた格子指数は 2、3 で割れない. 次に (4.2) の右辺を $\{P_2, P_3\}$ について考えると、$\lambda = \frac{1}{12}\log m_{a,b} - 0.147152$ ととってよいので、

$$\begin{aligned}\nu &\leq \sqrt{\frac{4}{3}\frac{\hat{h}(P_2)\hat{h}(P_3) - \frac{1}{4}\left\{\hat{h}(P_2+P_3) - \hat{h}(P_2) - \hat{h}(P_3)\right\}^2}{(\frac{1}{12}\log m_{a,b} - 0.147152)^2}} \\ &< \sqrt{\frac{4}{3}\frac{\hat{h}(P_2)\hat{h}(P_3)}{(\frac{1}{12}\log m_{a,b} - 0.147152)^2}} \\ &< \sqrt{\frac{4}{3}\frac{(\frac{1}{3}\log m_{a,b} + 1.0515)(\frac{1}{3}\log m_{a,b} + 0.5665)}{(\frac{1}{12}\log m_{a,b} - 0.147152)^2}}\end{aligned}$$

となる. 最後の右辺は $a > 6321$ または $b > 3982$ ならば 5 より小さいことが計算できる. そうでない有限個の場合についてはコンピュータによる総当りで確かめることにより、$\{P_2, P_3\}$ がモーデル・ヴェイユ基底の一部に使えることがわかる. 組 $\{P_3, P_1\}, \{P_1, P_2\}$ の場合もまったく同様のことができ証明が終了する.

□

References

[1] H. Cohen. *A Course in computational algebraic number theory.* Springer-Verlag, 1993.

[2] S. Duquesne. Elliptic curves associated with simplest quartic fields. *J. Theor. Nombres Bordeaux*, Vol. 19, pp. 81–100, 2007.

[3] Y. Fujita and N. Terai. Generators for the elliptic curve $y^2 = x^3 - nx$. *to appear in J. Theor. Nombres Bordeaux.*

[4] A. Knapp. *Elliptic curves.* Princeton Univ. Press, 1992.

[5] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, Vol. 25, pp. 1501–1538, 1995.

[6] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, Vol. 51, pp. 339–358, 1988.