実二次体上の楕円曲線の整数点の計算, および自明な導手を持つ楕円曲線の決定

早稲田大学理工学部* 加川 貴章 (Takaaki KAGAWA)

1 結果

次の問題を考える: 実二次体 k 上自明な導手を持つ楕円曲線 (の k-同型類) を決定せよ.

この問題に対し, 次の結果が過去に得られていた ([4], [5], [6], [7], [9], [10], [11]; いくつかの m については準備中):

定理 1. (1) $m = 2$, 3, 5, 10, 13, 15, 17, 21, 30, 34, 39, 42, 47, 57, 58, 66, 69, 70, 73, 74, 82, 85, 93, 94, 97, 113, 149, 173, 181, 191 の時, $\mathbb{Q}(\sqrt{m})$ 上自明な導手を持つ楕円曲線は存在しない.

(2) $m = 6, 7, 14, 29, 33, 37, 41, 65$ の時, $\mathbb{Q}(\sqrt{m})$ 上自明な導手を持つ楕円曲線が存在し, しかも決定されている.

ここでは定理 1 に現われていない m を扱い, 次の定理を証明する:

定理 2. (1) $m = 11, 19, 23, 31, 53, 61, 89, 101, 197$ の時, $\mathbb{Q}(\sqrt{m})$ 上自明な導手を持つ楕円曲線は存在しない.

(2) $\mathbb{Q}(\sqrt{m})$ ($m = 22, 77, 133, 157$) 上自明な導手を持つ楕円曲線は表 1 にある $m\mathrm{A}i$, $m\mathrm{A}i'$ のみである. 但し ε は基本単数で, $m = 77, 133, 157$ の時は $\omega = (1 + \sqrt{m})/2$ とおいた. また $'$ は共役を意味する. どの m に対しても, $\mathbb{Q}(\sqrt{m})$ 上の isogeny class は 1 つだけである.

Code	a_1	a_2	a_3	a_4	a_6	Δ	j	tors.
22A1	$\sqrt{22}$	1	$1+\sqrt{22}$	$-79-18\sqrt{22}$	$185+38\sqrt{22}$	ε^3	20^3	$\mathbb{Z}/2\mathbb{Z}$
22A1′	$-\sqrt{22}$	1	$1-\sqrt{22}$	$-79+18\sqrt{22}$	$185-38\sqrt{22}$	ε'^3	20^3	$\mathbb{Z}/2\mathbb{Z}$
77A1	ω	$-1-\omega$	0	$7-2\omega$	$7-\omega$	$-\varepsilon^3$	-15^3	$\mathbb{Z}/2\mathbb{Z}$
77A1′	$1-\omega$	$-2+\omega$	0	$5+2\omega$	$6+\omega$	$-\varepsilon'^3$	-15^3	$\mathbb{Z}/2\mathbb{Z}$
77A2	ω	$-1-\omega$	0	$-13-7\omega$	$60+13\omega$	ε^3	255^3	$\mathbb{Z}/2\mathbb{Z}$
77A2′	$1-\omega$	$-2+\omega$	0	$-20+7\omega$	$73-13\omega$	ε'^3	255^3	$\mathbb{Z}/2\mathbb{Z}$
133A1	0	0	1	$-158-30\omega$	$1132+215\omega$	$-\varepsilon^3$	-96^3	$\{O\}$
133A1′	0	0	1	$-188+30\omega$	$1347-215\omega$	$-\varepsilon'^3$	-96^3	$\{O\}$
157A1	$1+\omega$	0	$1+\omega$	$-5633-977\omega$	$-350775-60846\omega$	$-\varepsilon^6$	-13^3	$\{O\}$

表 1: Elliptic curves

注. 講演時には $\mathbb{Q}(\sqrt{77})$ 上の曲線の決定は出来ていなかったが, その後出来た. これにより判別式が 101 以下の 31 個の実二次体に対し, その上で自明な導手を持つ楕円曲線の決定が出来たことになる.

* 現在の所属は立命館大学理工学部
この研究は早稲田大学特定課題研究助成費 (98A-634) の援助を受けています.

2 Some criteria

k を実二次体, E を k 上自明な導手を持つ楕円曲線とする.

実二次体上導手が自明で, しかもその体上定義された位数 2 の有理点を持つ楕円曲線は, [2] で詳しく調べられている. 例えば, そのような曲線の存在, 非存在の条件, 存在する場合に何本あるか, などが得られている. また $1 < m < 100$ の時に $\mathbb{Q}(\sqrt{m})$ の上のそのような曲線全ての表が与えられている. それらを用いて, 定理 2 にある体に対しては, 位数 2 の有理点を持つ曲線は, $\mathbb{Q}(\sqrt{22})$ の上に 2 本だけ, $\mathbb{Q}(\sqrt{77})$ の上に 4 本だけあること, 他の体の上には無いことが示せる. ($m = 101, 157, 197$ の時は [4] の Proposition 2.2 を使ってもよい.)

よって以下 E は位数 2 の k-有理点を持たないと仮定する. また k の類数が 1 であることも仮定する. $\Delta(E)$ を判別式, c_4, c_6 を Weierstrass 方程式に付随する通常通りのものとする. $\Delta(E) = \pm\varepsilon^n$, $n \in \mathbb{Z}$ (ε は k の基本単数) であるとしてよく ([15], Chapter VIII の Corollary 8.3), また変数変換の公式より $0 \leq n < 12$ としてよい. このとき $c_4^3 - c_6^2 = 1728\Delta(E) = \pm 1728\varepsilon^n$ だから,

$$E_n^{\pm} : y^2 = x^3 \pm 1728\varepsilon^n$$

の k-整数点の集合 $E_n^{\pm}(\mathcal{O}_k)$ を $0 \leq n < 12$ に対し決めれば c_4, c_6 の候補が出揃い, E の決定が出来る. 各 k に対し 24 個の $E_n^{\pm}(\mathcal{O}_k)$ を決める必要があり大変だが, 一対一対応

$$E_n^{\pm}(\mathcal{O}_k) \to E_{n+6}^{\pm}(\mathcal{O}_k), \quad (x, y) \mapsto (x\varepsilon^2, y\varepsilon^3)$$

があるので, 求めるものは半分くらいにはなる. また ε のノルムが -1 で n が奇数の時は,

$$E_n^{+}(\mathcal{O}_k) \to E_{6-n}^{-}(\mathcal{O}_k), \quad (x, y) \mapsto (x'\varepsilon^2, y'\varepsilon^3)$$

も一対一対応なので, さらに求めるものを減らせる.

さらに, 2 等分点の体, 3 等分点の体を見ることによりそれぞれ以下の命題 3, 4 が得られ, 実際に計算する $E_n^{\pm}(\mathcal{O}_k)$ の数を更に減らすことが出来る. (命題 3 の証明は容易であるし, 命題 4 の証明の本質的な部分は [5] で与えられているので, ここでは証明を省略する.)

命題 3. k を代数体, E を k 上自明な導手を持つ楕円曲線とする. E が位数 2 の k-有理点を持たなければ, $k(\sqrt{\Delta(E)})$ の ray class number modulo $\prod_{\mathfrak{p}|2} \mathfrak{p}$ は 3 で割り切れる. □

命題 4. k を実二次体, ε を k の基本単数とする. 以下の 5 条件が成り立つ時, k 上自明な導手を持つ楕円曲線の判別式は k の 3 乗数でなくてはならない :

(1) k の類数は 6 と素である;
(2) k において 3 は不分岐である;
(3) $k(\sqrt{-3})$ の類数は 3 で割れない;
(4) $k(\sqrt[3]{\varepsilon})$ の類数は 2 で割れない;
(5) 3 を割る k の素 ideal $\mathfrak{p}$ に対し, 合同式 $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^3}$ は解 $X \in \mathcal{O}_k$ を持たない. □

m を定理 2 にあるものとし, $k = \mathbb{Q}(\sqrt{m})$ とする. この時 $m \neq 77$ なら命題 4 の条件が満たされることが確かめられる. $m = 77$ の場合は, $k(\sqrt{-3})$ の類数が 6 なので不適だが, や

m	$K=k$	$K=k(\sqrt{-1})$	$K=k(\sqrt{\varepsilon})$	$K=k(\sqrt{-\varepsilon})$
11	1	**3**	1	2
19	1	**3**	1	**6**
22	1	2	1	**3**
23	1	**3**	1	4
31	1	**3**	1	8
53	1	**3**	1	1
61	1	**3**	1	1
77	1	4	1	**3**
89	1	**6**	1	1
101	**3**	**21**	**3**	**3**
133	1	2	1	**3**
157	1	**3**	1	1
197	**3**	**15**	**3**	**3**

表 2: Ray class number of K modulo $\prod_{\mathfrak{p}|2}\mathfrak{p}$

はり 3 等分点の体を用いた議論により, $\mathbb{Q}(\sqrt{77})$ 上自明な導手を持つ楕円曲線の判別式が $\mathbb{Q}(\sqrt{77})$ の 3 乗数でなくてはならないことが示される.

$K=k(\sqrt{\Delta(E)})$ は k, $k(\sqrt{-1})$, $k(\sqrt{\pm\varepsilon})$ のいずれかである. K の ray class number modulo $\prod_{\mathfrak{p}|2}\mathfrak{p}$ を表 2 にまとめておく (3 の倍数は太字にしておいた). 命題 3, 表 2, 及び上の一対一対応のことから, $m=11,23,31,53,61,89,157$ なら $E_0^+(\mathcal{O}_k)$ のみを, $m=22,77,133$ なら $E_3^+(\mathcal{O}_k)$ のみを, $m=19$ なら $E_0^+(\mathcal{O}_k)$, $E_3^+(\mathcal{O}_k)$ を, そして $m=101,197$ なら $E_0^\pm(\mathcal{O}_k)$, $E_3^+(\mathcal{O}_k)$ を決定すれば十分であることがわかる.

3 整数点の計算

楕円曲線の整数点を計算する方法はいくつか知られているが, ここでは elliptic logarithm の評価に基づく方法を用いる. 即ち Mordell–Weil 群 $E_n^\pm(k)$ の基底を求め, 整数点を基底の一次結合で書いた時の係数の上界を elliptic logarithm の評価を用いて得るのである. (但し $m=101,197$ の時の $E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{m})})$ の計算は除く. これらについては 5 節を見よ.)

3.1 $E_n^\pm(k)_{\mathrm{tors}}$ の計算

Torsion 部分 $E_n^\pm(k)_{\mathrm{tors}}$ の計算は good prime での reduction と, 等分多項式の分解を見ることで行う. 詳細は略すが, 次が得られる:

補題 5. (1) 二次体 $k=\mathbb{Q}(\sqrt{m})$ (m は square-free) に対し,

$$E_0^+(k)_{\mathrm{tors}}=\begin{cases}\left\langle(-12,0)\right\rangle\oplus\left\langle(-12\zeta_3,0)\right\rangle\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & (m=-3\text{ の時}),\\ \left\langle(24,72\sqrt{3})\right\rangle\cong\mathbb{Z}/6\mathbb{Z} & (m=3\text{ の時}),\\ \left\langle(-12,0)\right\rangle\cong\mathbb{Z}/2\mathbb{Z} & (m\neq\pm3\text{ の時});\end{cases}$$

$$E_0^-(k)_{\mathrm{tors}} = \begin{cases} \left\langle (12\zeta_3, 0) \right\rangle \oplus \left\langle (-24, 72\sqrt{-3}) \right\rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} & (m = -3 \text{ の時}), \\ \left\langle (12, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z} & (m \neq -3 \text{ の時}). \end{cases}$$

ここに $\zeta_3 = (1 + \sqrt{-3})/2$.

(2) 実二次体 k に対し

$$E_3^+(k)_{\mathrm{tors}} = \begin{cases} \left\langle (24\varepsilon, 72\varepsilon\sqrt{3\varepsilon}) \right\rangle \cong \mathbb{Z}/6\mathbb{Z} & (\sqrt{3\varepsilon} \in k \text{ の時}), \\ \left\langle (-12\varepsilon, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z} & (\text{そうでない時}). \end{cases}$$

(2) の条件 $\sqrt{3\varepsilon} \in k$ が成り立つには k で 3 が分岐しなくてはならない. よって我々が扱う体では $E_0^{\pm}(k)_{\mathrm{tors}} = \left\langle (\mp 12, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$, $E_3^+(k)_{\mathrm{tors}} = \left\langle (-12\varepsilon, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$ が成り立つ.

3.2 $E_n^+(k)/2E_n^+(k)$ の計算

以下 m を定理 2 にあるものの 101, 197 以外のものとし, $k = \mathbb{Q}(\sqrt{m})$ とおく.

$E_0^{\pm}$ は $\mathbb{Q}$ 上定義されているから, $\operatorname{rank} E_0^{\pm}(k)$ の計算だけなら

$$\operatorname{rank} E_0^{\pm}(k) = \operatorname{rank} E_0^{\pm}(\mathbb{Q}) + \operatorname{rank}(E_0^{\pm})^{(m)}(\mathbb{Q}) \tag{1}$$

を用いれば出来る. ここに $(E_0^{\pm})^{(m)} : y^2 = x^3 \pm 1728m^3$. $m = 53, 89$ ならこれと補題 5 より $E_0^+(k) = \left\langle (-12, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$ がわかる.

さて, $\operatorname{rank} E_0^+(k) \geq 1$ の場合の $E_0^+(k)$ の計算, 及び $E_3^+(k)$ の計算にうつる. まず, Mordell–Weil の定理の証明と同じように $E_n^+(k)/2E_n^+(k)$ を求めるが, 我々が扱っている二次体は類数が 1 なので, 有理数体の場合とほとんど同じ方法で求めることが出来る (Serf [12] を参照). ここでは Serf が作ったプログラム (今は SIMATH に組み込まれている) を使ったが, そのプログラムは位数 2 の k-有理点を持たない場合は, k の判別式が小さくないとどれくらい時間がかかるかわからない. 実際 Serf は, その場合は $m = 2, 3, 5, 13$ 以外では cpu time が arbitrarily large になる, と書いている. よって現状では $E_{3n}^{\pm}(\mathcal{O}_k)$ しか計算できない. 2 節の 3 等分点の体を用いた議論は, 計算量を減らす以外にも必要だったのである.

3.3 $E_n^+(k)/2E_n^+(k)$ から $E_n^+(k)$ を求める

$x \in \overline{k}$ ($\overline{k}$ は k の代数的閉包) に対し, $H(x)$ を absolute height とする. また $P \in E_n^+(\overline{k})$ に対し $h(P) = \log H(x(P))$ ($x(P)$ は P の x 座標) を absolute logarithmic height とし, $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P)$ を canonical height とする. ([15], [16], [17] 等ではこの $1/2$ を定義としていることに注意.)

$E_n^+(k)$ を求めるには次の補題が有益である (証明は例えば [14], [18] 参照):

補題 6. E を代数体 K 上定義された楕円曲線とする. 正の実数 λ に対し, $E(K)$ は $\hat{h}(Q) \leq \lambda$ なる無限位数の点 Q を含まないとする. また $r = \operatorname{rank} E(K)$ とし, $P_1, \ldots, P_r \in E(K)$ が独

立であるとする. この時 $\hat{E}(K) := E(K)/E(K)_{\mathrm{tors}}$ ($\cong \mathbb{Z}^{\oplus r}$) の中での sublattice $\langle P_1, \ldots, P_r \rangle$ の指数は

$$\left[\hat{E}(K) : \langle P_1, \ldots, P_r \rangle\right] \leq \sqrt{R(P_1, \ldots, P_r)} \left(\frac{\gamma_r}{\lambda}\right)^{r/2} \tag{2}$$

を満たす. ここに $R(P_1, \ldots, P_r)$ は regulator, γ_r は Hermite 定数である. ($\gamma_1 = 1$, $\gamma_2 = \sqrt{4/3}$, $\gamma_3 = \sqrt[3]{2}, \ldots$ γ_r の値は [14], [18] を参照.) □

(2) の右辺が 2 未満になる λ を探すわけだが, 補題 6 の仮定「$\hat{h}(Q) \leq \lambda$ なる無限位数の点 Q を含まないとする」をどうやって確かめようか? それには

$$h(P) - \hat{h}(P) < \delta \tag{3}$$

なる $P \in E(K)$ に依存しない δ がわかっていればよい. そうすれば $H(x(Q))$ は定数 $C := \exp(\lambda + \delta)$ で上から押えられる. こういう Q なら以下のようにして決定できる. その後改めて $\hat{h}(Q) \leq \lambda$ でないことを確かめればよい. (なお, 二次体上の楕円曲線の canonical height は SIMATH で計算できる. 計算方法は [16] の方法に従っているようだ.)

$x = n/d \in \mathbb{Q}$, $n \in \mathbb{Z}$, $d \in \mathbb{N}$, $(n, d) = 1$ なら $H(x) = \max\{|n|, d\}$ であるから, $H(x) \leq C$ なる $x \in \mathbb{Q}$ を全て見付けるのは容易である. $x \in k \backslash \mathbb{Q}$ とし, x を根とする $\mathbb{Z}$ 係数の原始多項式を $aX^2 + bX + c$ とする. この時 $H(x) \leq C$ ならば $\max\{|a|, |b|, |c|\} \leq 2C^2$ である ([15], Chapter VIII 参照). よってこのような x も決められる (時間は掛かるが).

(3) のような δ の計算方法は [14], [17] などで与えられている. [17] の方法で δ を計算するのは容易だが, 評価があまりよくない. [14] の方法では, bad prime $\mathfrak{p}$ での Tamagawa index $c_{\mathfrak{p}}$ が必要で, Tate のアルゴリズムに従った計算をする必要があり面倒であるが, 評価が良い. (但し [17] は $P \in E(\overline{k})$ に対する評価, [14] は $P \in E(k)$ に対する評価であることを言っておかないと公正さを欠くであろう).

例 7. k を判別式が 3 と素な実二次体, E を $y^2 = x^3 + 27$ で定義される楕円曲線とする. (E は E_0^+ の k 上の global minimal model.) [14] の評価だと, 2 が k で不分岐ならば,

$$h(P) - \hat{h}(P) \leq 1.8515333\ldots$$

が全ての $P \in E(k)$ に対して成り立つ. $2 = \mathfrak{p}^2$ の時は,

$$h(P) - \hat{h}(P) \leq \begin{cases} 1.8515333\ldots & (c_{\mathfrak{p}} = 1 \text{ の時}), \\ 2.0248201\ldots & (c_{\mathfrak{p}} = 2 \text{ の時}), \\ 2.0825823\ldots & (c_{\mathfrak{p}} = 3 \text{ の時}) \end{cases}$$

が全ての $P \in E(k)$ に対して成り立つ. ($c_{\mathfrak{p}}$ は $1, 2, 3$ のいずれかであることが示せる.) 一方 [17] の評価だと

$$h(P) - \hat{h}(P) \leq 4.0560165\ldots$$

が全ての $P \in E(\overline{k})$ に対して成り立つ.

二次体上の Tate のアルゴリズムは SIMATH で実行できるが, バグが多くうまくいかない場合が多い. SIMATH でうまくいかない場合でも, 今までは梅垣氏のプログラム (cf. [20]) で全てうまくいった.

以下に $E_0^+(k), E_3^+(k)$ (の free-part) の基底を表にしておく. (但し E_0^+ は rank が正の場合のみ.)

m	rank r	生成元 $P_1, \ldots, P_r$
11	1	$(32, 56\sqrt{11})$
19	1	$(-8, 8\sqrt{19})$
23	1	$(42935/6084, 4512263\sqrt{23}/474552)$
31	1	$(484/25, 2128\sqrt{31}/125)$
61	2	$(14 - 2\sqrt{61}, 104 - 8\sqrt{61})$, $(853/9, 3193\sqrt{61}/27)$
157	2	$(13, 5\sqrt{157})$, $((7142 - 698\sqrt{157})/289, (1103440 - 72592\sqrt{157})/4913)$

表 3: $E_0^+(k)$ の基底

m	rank r	生成元 $P_1, \ldots, P_r$
19	2	$((-1700 - 390\sqrt{19})/9, (3516786 + 806806\sqrt{19})/27)$, $((-37400 - 8580\sqrt{19})/19, (14994648 + 3440008\sqrt{19})/361)$
22	1	$(6304 + 1344\sqrt{22}, 726264 + 154840\sqrt{22})$
77	2	$(18 + 2\sqrt{77}, 560 + 64\sqrt{77})$, $(144 + 16\sqrt{77}, 2464 + 280\sqrt{77})$
133	2	$(-692 - 60\sqrt{133}, 39672 + 3440\sqrt{133})$, $((3416 + 296\sqrt{133})/9, (1307704 + 113392\sqrt{133})/27)$

表 4: $E_3^+(k)$ の基底

3.4 Elliptic logarithm の方法 (概略)

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ を代数体 K 上定義された楕円曲線とし, $b_2 = a_1^2 + 4a_2$ とおく. よく知られているように, Weierstrass $\wp$ 関数による同型対応

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}), \quad z + \Lambda \to (x, y) = \Big(\wp(z) - b_2/12, (\wp'(z) - a_1x - a_3)/2\Big)$$

がある (Λ は格子). この逆写像 ψ を elliptic logarithm と言う. 以下 $\mathbb{C}/\Lambda$ の基本領域における $\psi(z)$ の代表元も $\psi(z)$ と書く. $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ とし, $\omega_1 \in \mathbb{R}$ に取っておく. $E(\mathbb{R})$ が一個の連結成分しか持たない場合 (例えば $E = E_n^{\pm}$), $P \in E(\mathbb{R})$ に対し $\psi(P)$ は ω_1 の実数倍である. 特に $T \in E(\mathbb{R})$ が位数 2 の場合 $\psi(T) = \omega_1/2$. 一般に $\psi(P)$ は楕円積分

$$\psi(P) = \int_{\infty}^{x(P)+b_2/12} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}} \quad (g_2 = c_4/12,\ g_3 = c_6/216)$$

で与えられる. $\psi(P)$ の実際的な計算方法 (算術幾何平均を用いる) は [1], [18] に出ていて, PARI/GP に実装されている.

$P = m_1P_1 + \cdots + m_rP_r + T$ $(m_1, \ldots, m_r \in \mathbb{Z},\ T \in E(K)_{\mathrm{tors}})$ を E の K-整数点とする. $M = \max\Big\{|m_1|, \ldots, |m_r|\Big\}$ とおく. $|\cdot|_{\mathfrak{p}_\infty}$ を K の無限素点 $\mathfrak{p}_\infty$ に対応する絶対値とすると, [19] の方法により,

$$|\psi(P)|_{\mathfrak{p}_\infty} \leq K_1 \exp(-K_2 M^2) \tag{4}$$

の形の評価が得られる. また $\psi(P)$ は elliptic logarithm の linear form だから, David [3] の結果より $\log|\psi(P)|_{\mathfrak{p}_\infty}$ の下からの評価

$$\log|\psi(P)|_{\mathfrak{p}_\infty} \geq -K_3(\log M + K_4)(\log\log M + K_5)^{r+2} \tag{5}$$

が得られる. ここに K_1, K_2, K_3, K_4, K_5 は, rank, 生成系の点の canonical height と elliptic logarithm, period ω_1, ω_2, 係数の height, $[k : \mathbb{Q}]$ などで explicit に書ける正の数である. (4) と (5) から M の upper bound が得られる.

例 8. $E_0^+(\mathcal{O}_{\mathbb{Q}(\sqrt{11})})$, $E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{133})})$ を決める時に最初に得られる評価はそれぞれ $M < 6.0293 \times 10^{24}$, $M < 1.3166 \times 10^{40}$ である. このように二次体上の楕円曲線に対しては, rank 1 の時は 10^{25} 程度, rank 2 の時は 10^{40} 程度の upper bound が得られる.

例 8 で述べたように, 最初の上界は非常に大きく, とても $m_1P_1 + \cdots + m_rP_r + T$ が整数点となっているか直接調べるのは無理である. しかし (4) を満たす M の upper bound を lattice の LLL-redued basis を用いて下げる方法がある ([18] に詳しく出ている). それを用いると, 元々の upper bound が H なら, 新しい bound は $\sqrt{\log H}$ くらいのサイズになる. よってその方法を数回適用すれば十分小さな bound が得られる. もちろんどこかで打ち止めになるわけだが, 今回の結果では, 一番悪い場合でも最終的な bound は 8 だった. これなら直接 $m_1P_1 + \cdots + m_rP_r + T$ が整数点になっているかどうか見るのは容易であろう.

例 9. $E_0^+(\mathcal{O}_{\mathbb{Q}(\sqrt{11})})$ を求める場合の upper bound の変化は $M < 6.0293 \times 10^{24}$, $M \leq 8$, $M \leq 3$ であり, $E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{133})})$ の場合は $M < 1.3166 \times 10^{40}$, $M \leq 27$, $M \leq 9$, $M \leq 8$ であった.

4 整数点一覧

今までの方法で $E_0^+(\mathcal{O}_k), E_3^+(\mathcal{O}_k)$ を計算してみた. 結果を以下に書いておく. (但し E_0^+ は rank が正の場合のみ. また E_3^+ は $k \neq \mathbb{Q}(\sqrt{101}), \mathbb{Q}(\sqrt{197})$ の場合.)

m	$\operatorname{rank} r$	$nT + m_1P_1 + \cdots + m_rP_r$	$(n, m_1, \ldots, m_r)$
11	1	$(32, -56\sqrt{11})$	$(0, -1)$
		$(-12, 0)$	$(1, 0)$
		$(32, 56\sqrt{11})$	$(0, 1)$
19	1	$(-8, -8\sqrt{19})$	$(0, -1)$
		$(96, 216\sqrt{19})$	$(1, -1)$
		$(-12, 0)$	$(1, 0)$
		$(96, -216\sqrt{19})$	$(1, 1)$
		$(-8, 8\sqrt{19})$	$(0, 1)$
23	1	$(-12, 0)$	$(1, 0)$
31	1	$(-12, 0)$	$(1, 0)$
61	2	$(14 - 2\sqrt{61}, -104 + 8\sqrt{61})$	$(0, -1, 0)$
		$(14 + 2\sqrt{61}, \quad 104 + 8\sqrt{61})$	$(1, -1, 0)$
		$(-12, 0)$	$(1, 0, 0)$
		$(14 + 2\sqrt{61}, -104 - 8\sqrt{61})$	$(1, 1, 0)$
		$(14 - 2\sqrt{61}, \quad 104 - 8\sqrt{61})$	$(0, 1, 0)$
157	2	$(13, -5\sqrt{157})$	$(0, -1, 0)$
		$(-12, 0)$	$(1, 0, 0)$
		$(13, 5\sqrt{157})$	$(0, 1, 0)$

表 5: $E_0^+(\mathcal{O}_k)$ $(T = (-12, 0))$

m	$\operatorname{rank} r$	$nT + m_1P_1 + \cdots + m_rP_r$	$(n, m_1, \ldots, m_r)$
19	2	$(3400 + 780\sqrt{19}, 309168 + 70928\sqrt{19})$	$(0, -1, -1)$
		$(172380 + 39546\sqrt{19}, 101213874 + 23220045\sqrt{19})$	$(1, 0, -1)$
		$(-2048 - 468\sqrt{19}, 0)$	$(1, 0, 0)$
		$(172380 + 39546\sqrt{19}, -101213874 - 23220045\sqrt{19})$	$(1, 0, 1)$
		$(3400 + 780\sqrt{19}, -309168 - 70928\sqrt{19})$	$(0, 1, 1)$
22	1	$(6304 + 1344\sqrt{22}, -726264 - 154840\sqrt{22})$	$(0, -1)$
		$(-2364 - 504\sqrt{22}, 0)$	$(1, 0)$
		$(6304 + 1344\sqrt{22}, 726264 + 154840\sqrt{22})$	$(0, 1)$
77	2	$(18 + 2\sqrt{77}, -560 - 64\sqrt{77})$	$(0, -1, 0)$
		$((135 + 15\sqrt{77})/2, 945 + 108\sqrt{77})$	$(1, -1, 0)$
		$(144 + 16\sqrt{77}, -2464 - 280\sqrt{77})$	$(0, 0, -1)$
		$(-54 - 6\sqrt{77}, 0)$	$(1, 0, 0)$
		$(144 + 16\sqrt{77}, 2464 + 280\sqrt{77})$	$(0, 0, 1)$
		$((135 + 15\sqrt{77})/2, -945 - 108\sqrt{77})$	$(1, 1, 0)$
		$(18 + 2\sqrt{77}, 560 + 64\sqrt{77})$	$(0, 1, 0)$
133	2	$(-692 - 60\sqrt{133}, -39672 - 3440\sqrt{133})$	$(0, -1, 0)$
		$(8304 + 720\sqrt{133}, 1071144 + 92880\sqrt{133})$	$(1, -1, 0)$
		$(346 + 30\sqrt{133}, 48160 + 4176\sqrt{133})$	$(0, -1, -1)$
		$((2595 + 225\sqrt{133})/2, -81270 - 7047\sqrt{133})$	$(1, -1, -1)$
		$(-1038 - 90\sqrt{133}, 0)$	$(1, 0, 0)$
		$((2595 + 225\sqrt{133})/2, 81270 + 7047\sqrt{133})$	$(1, 1, 1)$
		$(346 + 30\sqrt{133}, -48160 - 4176\sqrt{133})$	$(0, 1, 1)$
		$(8304 + 720\sqrt{133}, -1071144 - 92880\sqrt{133})$	$(1, 1, 0)$
		$(-692 - 60\sqrt{133}, 39672 + 3440\sqrt{133})$	$(0, 1, 0)$

表 6: $E_3^+(\mathcal{O}_k)$ $(T = (-12\varepsilon, 0))$

5 $\mathbb{Q}(\sqrt{101})$, $\mathbb{Q}(\sqrt{197})$ の場合

$k = \mathbb{Q}(\sqrt{101})$ または $\mathbb{Q}(\sqrt{197})$ とする. この時補題 5 と (1) より $E_0^{\pm}(k) = \left\langle (\mp 12, 0) \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$ がわかる.

一方これらの体に対し, $E_3^+(k)$ が求まらなかった. $\operatorname{rank} E_3^+(k) \leq 1$ はわかり, Tate–Shafarevich 群が有限であると仮定すると $\operatorname{rank} E_3^+(k) = 1$ であることもわかった. しかし存在するであろう生成元の height が大きいらしく, 見付からなかった.

しかし実は以前, [5] の Proposition 4 で

$$E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{37})}) = \left\{(-12\varepsilon, 0), (17640 - 1740\sqrt{37}, \pm(2074464 - 438480\sqrt{37}))\right\}$$

を証明したのと同じく, 古典的な方法である分解 $x^3 = (y - 24\varepsilon\sqrt{3\varepsilon})(y + 24\varepsilon\sqrt{3\varepsilon})$ を用いて $E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{m})})$ $(m = 101, 197)$ を求めたことがあった. 結果は次のものであった (詳細は略す. [2] の Proposition 2, [4] の Lemma 2.1, [8] の Theorem 1 が大事な役割を果たすことだけ注意しておく):

命題 10. $m = 101, 197$ ならば $E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = \left\{(-12\varepsilon, 0)\right\}$.

6 Q.E.D.

各 $(x, y) \in E_n^{\pm}(\mathcal{O}_k)$ が c_4, c_6 の候補であったことを思い出そう. 前節までの議論で候補が出揃ったわけだが, これらが実際に c_4, c_6 に成れるかを調べる必要がある. まず次の結果がある (Setzer [13]):

命題 11. 二次体上自明な導手を持つ楕円曲線の j-invariant は 0 でも 1728 でもない. □

よって $y = 0$ の時は考慮からはずしてよい. 他の (x, y) に対しては, Tate のアルゴリズムを用いて楕円曲線 $Y^2 = X^3 - 27xX - 54y$ の k 上の導手が自明かどうか調べる. 結局 c_4, c_6 に成れるのは

$$\begin{aligned}
\left((135 + 15\sqrt{77})/2, -945 - 108\sqrt{77}\right) &\in E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{77})}) \quad (77\text{A1 に対応}),\\
\left(\varepsilon^2(135 + 15\sqrt{77})/2, \varepsilon^3(945 + 108\sqrt{77})\right) &\in E_9^+(\mathcal{O}_{\mathbb{Q}(\sqrt{77})}) \quad (77\text{A1}' \text{ に対応}),\\
(8304 + 720\sqrt{133}, -1071144 - 92880\sqrt{133}) &\in E_3^+(\mathcal{O}_{\mathbb{Q}(\sqrt{133})}) \quad (133\text{A1 に対応}),\\
\left((8304 + 720\sqrt{133})\varepsilon^2, (1071144 + 92880\sqrt{133})\varepsilon^3\right) &\in E_9^+(\mathcal{O}_{\mathbb{Q}(\sqrt{133})}) \quad (133\text{A1}' \text{ に対応}),\\
(13\varepsilon^2, 5\sqrt{157}\varepsilon^3) &\in E_6^+(\mathcal{O}_{\mathbb{Q}(\sqrt{157})}) \quad (157\text{A1 に対応})
\end{aligned}$$

のみであることがわかる. (22A1, 22A1′, 77A2, 77A2′ は位数 2 の k-有理点を持つので, 今までの議論で得られなくても何の問題も無い. 77A1, 77A1′ に対応するものが出てきたのはたまたまである.)

7　アイデア求む

E を代数体 k 上定義された楕円曲線とする. 3.3 節の議論により, Mordell–Weil 群 $E(k)$ を求めるのには, ある正の数 C に対し有限集合 $S = \{P \in E(k) \mid H(P) \leq C\}$ を決定することが大事であるとわかっていただけたと思う. S を求めるには, $k = \mathbb{Q}$ の場合は $C = 10000$ くらいでも 1 分も掛からないが, k が二次体だとそうはいかない. 実際 3.3 節で述べたことから, C^6 に比例した時間が掛かってしまい, $C = 100$ でも相当な時間を要する. しかし次のことに注意すれば, C^5 に比例した時間で求まるように出来る: 我々は類数 1 の体 k しか扱っていないから, 楕円曲線の k-有理点の x 座標は $x = n/d^2$, $n, d \in \mathcal{O}_k$, $(n, d) = 1$ の形をしているので, $x \in k \backslash \mathbb{Q}$ の時は x を根とする $\mathbb{Z}$ 上の原始多項式は $a^2X^2 + bX + c$ の形をしている. さらに, この多項式の判別式が k の判別式の平方数倍であること, $a^2 = N_{k/\mathbb{Q}}(d)^2$ であることに注意するとさらなるスピードアップが出来る. しかしそれでも $\{P \in E_3^+(\mathbb{Q}(\sqrt{19})) \mid H(P) \leq C\}$ を決定するには, $C = 100$ なら 1 時間くらいで済むが, $C = 200$ なら 1 日半くらい掛かってしまう (C 言語で書いたプログラム (長桁計算や二次体の計算は SIMATH のサブルーチンを使った) を Pentium 200MHZ の CPU を積んだパソコンで実行させた). そういうわけで今回, 命題 4 の条件を満たしていて, $E_n^+(k)/2E_n^+(k)$ が求まっているような実二次体 k に対しても, $E_n^+(k)$ を求めるのを断念した場合がいくつかある. (例えば $k = \mathbb{Q}(\sqrt{46})$ で $n = 3$ の時. この場合 C が 2 万以上, 少々工夫しても 6000 以上になってしまい, S を求めるのに要する時間は $\cdots$ 考えたくない.)

上のような S を決定するための素晴らしいアルゴリズムを開発すること, もしくは速いプログラムを作ることは, 二次体上の楕円曲線の研究に大いに役立つはずである. アイデアを求む.

参考文献

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, 1986.

[2] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, *Pacific J. Math.* **144** (1990), 233–258.

[3] S. David, Minorations de formes linéaires de logarithmes elliptiques, *Mémoires de la Societé Mathématique de France*, Vol. 62, 1995.

[4] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, *Japan. J. Math.* **12** (1986), 45–52.

[5] T. Kagawa, Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$, *Acta Arith.* **83** (1998), 253–269.

[6] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields, *Arch. Math.*, to appear.

[7] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields $\mathbb{Q}(\sqrt{3p})$, *preprint*.

[8] T. Kagawa and N. Terai, Squares in Lucas sequences and some Diophantine equations, *Manuscripta Math.* **96** (1998), 195–202.

[9] M. Kida, Reduction of elliptic curves over real quadratic number fields, *Math. Comp.*, to appear.

[10] M. Kida and T. Kagawa, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, *J. Number Theory* **66** (1997), 201–210.
[11] R. G. E. Pinch, *Elliptic curves over number fields*, Ph. D. thesis, Oxford, 1982.
[12] P. Serf, *The rank of elliptic curves over real quadratic number fields of class number* 1, Ph. D. thesis, Universität des Saarlandes, Saarbrücken, 1995.
[13] B. Setzer, Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant, *Illinois J. Math.* **25** (1981), 233–245.
[14] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), 1501–1538.
[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.
[16] J. H. Silverman, Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339–358.
[17] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **51** (1988), 339–358.
[18] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Text **41**, 1998.
[19] N. P. Smart and N. M. Stephens, Integral points on elliptic curves over number fields, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 9–16.
[20] 梅垣敦紀「代数体上の楕円曲線の計算」, シンポジウム「代数学と計算」(報告集は `ftp://tnt.math.metro-u.ac.jp/pub/ac97/PROCEEDINGS/` より入手可能)

〒 525–8577　滋賀県草津市野路東 1–1–1
立命館大学理工学部数学物理学科
E-mail : kagawa@se.ritsumei.ac.jp

8　追記 (1999 年 8 月 7 日)

5 節で $E_3^+(k)$ $(k=\mathbb{Q}(\sqrt{101}), \mathbb{Q}(\sqrt{197}))$ の無限位数の点が見付からなかったと書いたが, その後見付け出すことに成功した. (方法は, E_3^+ と 3-isogeny な曲線 $y^2=x^3-\varepsilon^3$ 上の無限位数の点を見付け (Serf のプログラムでそれぞれ数分, 数秒), それを E_3^+ にうつしたのである.) その点を $P=(x,y)$ とすると, $k=\mathbb{Q}(\sqrt{101})$ の時は

$$x=\frac{126449730933319735654808 30+11293174148057446433386 26\sqrt{101}}{98500265336240645370025},$$
$$y=\frac{816109017096133902021448934818764731 52+826729889164067249551632751686590574 4\sqrt{101}}{309140639207533923437201413336311 25},$$

$k=\mathbb{Q}(\sqrt{197})$ の時は

$$x=-\frac{298542599728836713 22+213905508707292995 8\sqrt{197}}{385086590512437025},$$
$$y=\frac{699952218368385130216512269168+498708297148462696244743763 20\sqrt{197}}{238966814216663016333671375}$$

である. また (x,y) の canonical height はそれぞれ $33.6329\cdots$, $23.4789\cdots$ である. $E_3^+(k)=\langle(x,y)\rangle\oplus\langle(-12\varepsilon,0)\rangle\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ であることも確かめた.