楕円曲線上の不変量の計算 II. (CREMONA の解説)

森田 知真

目的: Cremona [C] に従って, $\mathbb{Q}$ 上の楕円曲線 E の Mordell-Weil 群 $E(\mathbb{Q})$ についての様々な不変量を具体的に求めるアルゴリズムを紹介する. 特に, Mordell-Weil 群 $E(\mathbb{Q})$ の生成元やランクなどが明示的に計算できることを解説するのが目的である.

1. 導入

$\mathbb{Q}$ 上の楕円曲線 E に対して, その上に存在する有理点を求めることは, 整数論において最も重要かつ困難な問題のひとつである. この問題に関しての最初のブレーク・スルーは, Mordell-Weil 群 $E(\mathbb{Q})$ が $\mathbb{Z}$ 上有限生成であるという Mordell の定理である. この定理より

$$E(\mathbb{Q}) = T \times F$$

とあらわすことができる. 但し, ここで, T はトーション部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ をあらわし, F は有限階数 r の自由アーベル群 $E(\mathbb{Q})_{\mathrm{fr}} = E(\mathbb{Q})/T$ である. 以下, Mordell-Weil 群 $E(\mathbb{Q})$ のランクと言えば, この r を意味するものとする.

2. トーション $E(\mathbb{Q})_{\mathrm{tors}}$ の決定

この章では, トーション部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ の構造や生成元を明示的に計算する. この計算には完全なアルゴリズムが存在し, 有限時間で 確実 に計算を実行することが可能である.

2.1. **トーション $E(\mathbb{Q})_{\mathrm{tors}}$ についての基本的な性質.** まず, $E(\mathbb{R})$ の構造は S^1 または $S^1 \times C_2$ に同型であることがわかる ([Sil 3,p.420]). ここで, C_k によって位数 k の巡回群をあらわすものとする. また, S^1 のすべての有限部分群は巡回群だという事実を用いれば, $E(\mathbb{Q})_{\mathrm{tors}}$ の可能性としては, C_k 型または $C_k \times C_2$ 型のいずれかである. さらに強く, Mazur の定理より

$$E(\mathbb{Q})_{\mathrm{tors}} = \begin{cases} C_k & 1 \le k \le 10 \quad \text{or} \quad k = 12 \\ C_{2k} \times C_2 & 1 \le k \le 4 \end{cases}$$

となることが知られている ([Ma1], [Ma2]).

Date: May 27, 2012.
Key words and phrases. Elliptic curves, Mordell-Weil groups, L-functions.

2.2. **Lutz-Nagell の定理.** トーション $E(\mathbb{Q})_{\mathrm{tors}}$ を具体的に決定するのに本質的な役割を果たすのが, 次の Lutz-Nagell の定理である.

Theorem 2.1. *E を $\mathbb{Q}$ 上定義された楕円曲線で, その方程式は*

$$y^2 = f(x) = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{Z})$$

で与えられるとする. このとき, $P = (x_1, y_1) \in E(\mathbb{Q})_{\mathrm{tors}}$ ならば, $x_1, y_1 \in \mathbb{Z}$ である.

なお, 一般の楕円曲線 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ については, xy と y の項を平方完成させることで取り除き, 分母をはらうという変換を行うことで, 上の定理の形の楕円曲線にもっていくことができる. この定理を用いることで, 次のように, $P = (x_1, y_1) \in E(\mathbb{Q})_{\mathrm{tors}}$ の y_1 を評価することができ, 有限時間で $E(\mathbb{Q})_{\mathrm{tors}}$ の元を計算することができる.

Proposition 2.2. *上の定理の記号のもとで, $P = (x_1, y_1) \in E(\mathbb{Q})_{\mathrm{tors}}$ ならば*

$$y_1 = 0 \quad or \quad y_1^2 \mid \Delta_0$$

が成立する. 但し, $\Delta_0 = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 18abc$ であり, 判別式 Δ とは $\Delta = -16\Delta_0$ なる関係がある.

Proof. まず, $2P = 0$ となるときは, 明らかに, $y_1 = 0$ となる. $2P = (x_2, y_2)$ とおいたときに, 上の定理より, $x_2, y_2 \in \mathbb{Z}$ が分かり, 加法公式より

$$2x_1 + x_2 = m^2 - a$$

と書ける. 但し, ここで, $m = f'(x_1)/2y_1$ は P における接線の傾きである. よって, $m \in \mathbb{Z}$ が分かり, $y_1 \mid f'(x_1)$ となる. ここで

$$\Delta_0 = (-27f(x) + 54c + 4a^3 - 18ab)f(x) + (f'(x) + 3b - a^2)f'(x)^2$$

であることに注意すると, $y_1^2 \mid \Delta_0$ が従う. □

Example 2.3. 上の Proposition を用いることで, $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 - 43x + 166$$

に対するトーション部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ を具体的に求める. この楕円曲線 E に対して, Δ_0 を計算すると

$$\Delta_0 = 425984 = 2^{15} \cdot 13$$

となる. よって, 上の Proposition より, トーション部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ に含まれる元の y 座標の候補としては

$$\{0, \pm1, \pm2, \pm4, \pm8, \pm16, \pm32, \pm64, \pm128\}$$

のいずれかになる. 実際に代入し, さらには, Mazur の定理を利用することで, 無限位数の元を排除することを行い, トーション点は

$$\{(3, \pm8),\ (-5, \pm16),\ (11, \pm32)\}$$

と決定される. さらに計算すると, $E(\mathbb{Q})_{\mathrm{tors}}$ は $P = (3, 8)$ を生成元とする (もちろんどれでもよい), 位数 7 の巡回群であることが分かる.

2.3. **還元写像の利用.** 素数 p に対して, 楕円曲線 E の還元 $E(\mathbb{Z}/p\mathbb{Z})$ が good で $(m,p)=1$ なら, 還元写像 $E(\mathbb{Q})[m] \to E(\mathbb{Z}/p\mathbb{Z})$ は単射となる ([Sil 1,p.176]). このことを利用して, 上で行われた計算の速度をはやめることができるのを紹介したい.

Example 2.4. 還元写像を用いることによって, $\mathbb{Q}$ 上の楕円曲線

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

が非自明なトーション点を持たないことを示す. まず, 判別式は $\Delta = -3^5 \cdot 2^4$ と求まるので, 素数 $p \geq 5$ に対して, E は good な還元を持つことが分かる. また, 簡単な手計算により

$$\sharp E(\mathbb{Z}/5\mathbb{Z}) = 6, \quad \sharp E(\mathbb{Z}/7\mathbb{Z}) = 13$$

が得られる. よって, $\sharp E(\mathbb{Q})[m] = 1$ $(m \neq 5, 7)$, $\sharp E(\mathbb{Q})[5] \mid 13$ や $\sharp E(\mathbb{Q})[7] \mid 6$ が分かり, 自明なトーション点 O しか持たないことになる. Mazur の定理より, $m \leq 12$ のときに考えれば十分である.

Example 2.5. (Example 2.3. の続き.)

楕円曲線 $E : y^2 = x^3 - 43x + 166$ のトーション点は

$$\big\{(3, \pm 8),\ (-5, \pm 16),\ (11, \pm 32)\big\}$$

で与えられることを見た. 一方で, E は $p = 3, 5$ で good な還元を持ち, $\sharp E(\mathbb{Z}/3\mathbb{Z}) = \sharp E(\mathbb{Z}/5\mathbb{Z}) = 7$ と簡単に計算できる. よって, 非自明なトーション点が存在すれば, $E(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$ とすぐに決定されることが分かる.

Remark 2.6. これらの例から, 重み 2 の rational newform の q 展開の係数が分かれば, トーション $E(\mathbb{Q})_{\mathrm{tors}}$ の構造についての情報が得られるということが見てとれる.

♣ トーション $E(\mathbb{Q})_{\mathrm{tors}}$ の計算の仕方 (まとめ)

• まずは, 楕円曲線 E をうまく変換させて, Lutz-Nagell の定理が使える形

$$y^2 = f(x) = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{Z})$$

にする. 次に, Δ_0 を割り切る y 座標 (整数) をシラミ潰しで探すことによって, トーション点の候補を見つける (有限回の操作). また, 還元写像を使うことで計算の速度を上げることができる.

• コンピューターに命令すると, トーション $E(\mathbb{Q})_{\mathrm{tors}}$ の位数, 生成元, 構造をすぐに求めてくれる.

3. 自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成元の決定

この章では, Mordell-Weil 群 $E(\mathbb{Q})$ のランクがあらかじめ分かっているものとし, その生成元を決定する方法を解説する. この手法は, 高さ関数を使って, シラミ潰しで探すものであり, 有限時間で終了するという保証はない. しかし, 導手が 1000 くらいまでの楕円曲線なら, かなりの数の楕円曲線について, 手計算でも決定することができるということを紹介したい.

3.1. **高さ関数についての基本的性質.** Mordell-Weil 群 $E(\mathbb{Q})$ のランクや (トーションでない) 生成元を決定するのに, 中心的な役割を果たす高さ関数について簡単にまとめておく. 高さ関数にはふたつの種類のものがある, ナイーブ高さ関数と標準高さ関数である. 有理点 $P = (x, y) = (a/c^2, b/c^3) \in E(\mathbb{Q})$ $(a, b, c \in \mathbb{Z}$, $\gcd(a, c) = \gcd(b, c) = 1)$ に対して, ナイーブ高さ関数は

$$h(P) = \log \max\Big\{|\ a\ |, c^2\Big\}$$

と定義される. つまり, x 座標の分子と分母を比べているのである. 一方で, 標準高さ関数はナイーブ高さ関数を用いて

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

と定義される. これらの表示からも明らかなように, ナイーブ高さ関数は手計算でも可能なの対して, 標準高さ関数は実用的ではない. しかし, 標準高さ関数は以下のように, 理論的に良い性質を満たすことが分かっている ([Sil 1,p.229]).

a). $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$ $\quad (P, Q \in E(\mathbb{Q}))$

b). $\hat{h}(m \cdot P) = m^2 \hat{h}(P).$ $\quad (P \in E(\mathbb{Q}),\ m \in \mathbb{Z})$

c). $\hat{h}(P) = 0 \iff P \in E(\mathbb{Q})_{\mathrm{tors}}.$

Remark 3.1. Néron や Tate によって, 標準高さ関数 $\hat{h}$ は局所高さ関数の和で書けることが示されている. また, その各々の局所高さ関数は明示的に与えられ, 実際に (近似) 計算可能であり, しかも, 本稿の計算においても必要である. しかし, これらの計算は複雑で, 教育的でなく, コンピューターなしで実行することは困難なので, ここでは紹介しないことにした. 詳しくは [Sil 2,3] や [C] を参照されたい.

3.2. **生成元の決定.** この節では, Mordell-Weil 群 $E(\mathbb{Q})$ の (トーションでない) 生成元をふたつの高さ関数を使って, シラミ潰しで探すことを目的とする. なお, ここでは Mordell-Weil 群 $E(\mathbb{Q})$ のランク r はあらかじめ分かっているものとする. この手順は大まかに言って, 三つのパートに分かれる.

I. ナイーブ高さ関数 h による x 座標の分子と分母の評価 B に従って, とにかく有理点を探す.

II. 探してきた有理点が自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成に寄与するかどうかを調べる. 標準高さ関数 $\hat{h}$ を用いて得られる, 高さ対で判定を行うことになる.

III. r 個の独立な元が生成する $E(\mathbb{Q})_{\mathrm{fr}}$ の指数有限部分群 A を大きくして全体に一致させる. ナイーブ高さ関数 h と標準高さ関数 $\hat{h}$ の差を評価することが鍵になる.

========================

それでは, 各々の手順を詳しく見ていきたい.

I. このステップでは, ナイーブ高さ関数 h により与えられた範囲の中で, 有理点をシラミ潰しに探すということになる. つまり, $B \in \mathbb{N}$ という範囲が与えられ

たときに, x 座標 p/q $(-B \le p, q \le B)$ という $(2B+1)^2$ 個をすべて代入することで有理点を見つける. この作業は絶望的に思えるが, 添付した資料が示すように導手が 1000 以下なら, 生成元の x 座標に対する評価 $B \in \mathbb{N}$ は, ほとんどが 10 程度, 大きくて 30 ほどである. よって, ほとんどのケースは (運が悪くなければ), 手計算可能なものである.

Example 3.2. 導手が 100 以下の楕円曲線の自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成元を列記しておく. 但し, N は導手をあらわすものとする.

$$\begin{aligned}(x,y) \mid N = {}& (0,0) \mid 37, \quad (0,0) \mid 43, \quad (0,0) \mid 53, \quad (2,1) \mid 57, \quad (0,1) \mid 58, \\ & (1,0) \mid 61, \quad (1,0) \mid 65, \quad (2,3) \mid 77, \quad (0,0) \mid 79, \quad (0,0) \mid 82, \\ & (0,0) \mid 83, \quad (2,2) \mid 88, \quad (0,0) \mid 89, \quad (0,0) \mid 91, \quad (-1,3) \mid 91', \\ & (1,1) \mid 92, \quad (0,0) \mid 99.\end{aligned}$$

E の生成元の x 座標の分子と分母に対する評価 $B \in \mathbb{N}$ がかなり小さい様子が分かる. ここで, $91'$ は 91 と同種でない別の楕円曲線をあらわしている.

Remark 3.3. 実根による評価, 合同式を考えること, さらには, 有理点は $(x,y) = (a/c^2, b/c^3) \in E(\mathbb{Q})$ の形をしていることなどに注意すると, $(2B+1)^2$ 個をすべて代入するということの手間は大幅に省くことができる.

II. すでに $P_1 \sim P_k$ $(1 \le k \le r)$ なる独立な有理点が分かっているとし, I. で得られた有理点 $P_{k+1} = P$ が自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成に寄与するかどうかを調べる. まずは, 標準高さ関数を使って, <u>高さ対</u>を

$$\hat{h}(P,Q) = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$$

と定義する. この高さ対, つまり $E(\mathbb{Q}) \otimes \mathbb{R}$ 上のメトリックを使って定義される $(k+1) \times (k+1)$ 行列 $M = (\hat{h}(P_i, P_j))$ を考えることにする.

<u>ア). 行列式 $\det(M) \neq 0$ のとき</u> ([Sil 1,p.232])

このときは, 新たに探してきた有理点 $P = P_{k+1}$ が $P_1 \sim P_k$ たちと独立になっていることが分かり, 自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成に寄与する.

<u>イ). 行列式 $\det(M) = 0$ のとき</u>

一方で, このときは, 有理点 $P = P_{k+1}$ が $P_1 \sim P_k$ たちの $\mathbb{Z}$ 上の線型結合で書けることが分かり, 自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成に寄与しない.

Example 3.4. 導手 997 の楕円曲線

$$E : y^2 + y = x^3 - x^2 - 5x - 3$$

の Mordell-Weil 群 $E(\mathbb{Q})$ のランクは $r = 2$ であることが分かっている ([C]). このときに, 上の手順で二つの独立な元を求めたい.

I. 評価 $B = 5$ に対して, $x = p/q$ $(-5 \le p, q \le 5)$ としてシラミ潰しで有理点を探していくと

$$P_1 = (-1,0),\ P_2 = (3,-1),\ P_3 = (5,8)$$

などが見つかり, 非自明なトーション点が存在しないこともすぐに分かるので, いずれも無限位数の元である. 分母 q としては, $q = 1$ または $q = 2^2$ のときだけ調べればよい (17 個).

II. 高さ対を用いて, $P_1 \sim P_3$ の独立性を調べる.

a). $P_1 = (-1, 0)$ と $P_2 = (3, -1)$ は独立か?

Silverman のアルゴリズムによってコンピューターで, 高さ対を計算すると

$$\hat{h}(P_1, P_1) \sim 0.3456, \quad \hat{h}(P_1, P_2) = \hat{h}(P_2, P_1) \sim 0.6912, \quad \hat{h}(P_2, P_2) \sim 1.3823$$

と求まり, これらを成分に持つ 2×2 行列とその行列式は

$$M \sim \begin{pmatrix} 0.3456 & 0.6912 \\ 0.6912 & 1.3823 \end{pmatrix}, \quad \det(M) \sim -0.00003456$$

となる. このことから, P_1 と P_2 には従属関係があり, $P_1 = kP_2$ または $P_2 = kP_1$ $(k \in \mathbb{Z})$ と予想されるが, 実際には $P_2 = 2P_1$ である.

b). $P_1 = (-1, 0)$ と $P_3 = (5, 8)$ は独立か?

前と同様にコンピューターで, 高さ対を計算すると

$$\hat{h}(P_1, P_1) \sim 0.3456, \quad \hat{h}(P_1, P_3) = \hat{h}(P_3, P_1) \sim 0.2176, \quad \hat{h}(P_3, P_3) \sim 1.7893$$

と求まり, これらを成分に持つ 2×2 行列とその行列式は

$$N \sim \begin{pmatrix} 0.3456 & 0.2176 \\ 0.2176 & 1.7893 \end{pmatrix}, \quad \det(N) \sim 0.5710$$

となる. よって, P_1 と P_3 は独立な点であり, 実際にランク 2 の $E(\mathbb{Q})_{\mathrm{fr}}$ の生成元を与えている.

Remark 3.5. 標準高さ関数 $\hat{h}$ には, 正規化の方法が二つあり, ここでは, もう一方の正規化 ([Sil 1,2] など) の 2 倍になっている. L 関数の先頭項に対する BSD 予想における表示で, 2^r が登場することがあるが, これはこの正規化に起因している. ここでの標準高さ関数 $\hat{h}$ の正規化では登場しない.

III. r 個の独立な元が生成する $E(\mathbb{Q})_{\mathrm{fr}}$ の指数有限部分群 A を大きくして全体に一致させる. ここで鍵となるのが次の Silverman によるナイーブ高さ関数 h と標準高さ関数 $\hat{h}$ の差を評価した結果である. 記号として, $\gcd(a, b) = 1$ の整数 a, b に対して, $h(a/b) = \log \max\{|\, a \,|, |\, b \,|\}$ とし, 実数 x に対して $\log^+(x) = \log \max\{1, |\, x \,|\}$ とおく.

Proposition 3.6. 判別式 Δ, j-不変量 j を持つ $\mathbb{Z}$ 上の楕円曲線 E を考える. また, $b_2 = a_1^2 + 4a_2 \neq 0$ なら, $2^* = 2$ とおき, $b_2 = 0$ ならば, $2^* = 1$ とする. ここで, 不変量 $\mu(E)$ を

$$\mu(E) = \frac{1}{6}(\log |\, \Delta \,| + \log^+(j)) + \log^+(b_2/12) + \log(2^*)$$

と定義する. このとき, $Q \in E(\mathbb{Q})$ に対して, 次の評価が成り立つ

$$-\frac{1}{12}h(j) - \mu(E) - 1.922 \leq \hat{h}(Q) - h(Q) \leq \mu(E) + 2.14.$$

簡単のために, $r = 1$ のときを考えよう. I. の操作によって, 有理点 P を得られたとする. このとき, 一般には, P は $E(\mathbb{Q})_{\mathrm{fr}}$ の有限指数部分群を生成するのみで, $E(\mathbb{Q})_{\mathrm{fr}}$ のある生成元 Q によって, $P = kQ$ $(k \in \mathbb{N})$ と書ける. 実際に, $k \geq 2$ とすると

$$\hat{h}(Q) \leq \frac{1}{4}\hat{h}(P)$$

となり, 生成元 Q の標準高さ $\hat{h}$ の評価が得られる. さらに, 上の Silverman による評価により, 生成元 Q のナイーブ高さ h の評価が得られることになる.

$$\underline{\text{手順}} \qquad \hat{h}(P) \text{ の値 } \Longrightarrow \hat{h}(Q) \text{ の評価 } \Longrightarrow h(Q) \text{ の評価.}$$

生成元 Q のナイーブ高さ h の評価により, x 座標の分子と分母に対する上限 $B \in \mathbb{N}$ が定まる. 再び, I. の操作に戻り, その範囲 B をシラミ潰しで探せば, 生成元が見つかる. 一般のランク r のときも同様の手順で実行される ([Ge-Zi], [Sik]).

Example 3.7. (Example 3.4. の復習.)

導手 997 の $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 + y = x^3 - x^2 - 5x - 3$$

の Mordell-Weil 群 $E(\mathbb{Q})$ のランクは $r = 2$ で, その生成元として

$$P_1 = (-1, 0),\ P_3 = (5, 8)$$

が求まった. 計算途中で $E(\mathbb{Q})_{\mathrm{fr}}$ の有限指数部分群 $A = \langle P_2 = (3, -1), P_3 = (5, 8)\rangle$ が得られたとしよう ($P_2 = 2P_1$). これを全体に拡張する操作は III. で述べたように, 次のように実行すればよい.

1). P_2 と P_3 の標準高さ $\hat{h}(P_i)$ $(i = 2, 3)$ を求める (コンピューターを使う).

2). 生成元 $Q \in E(\mathbb{Q})_{\mathrm{fr}}$ に対する $\hat{h}(Q)$ の評価を $\hat{h}(P_i)$ $(i = 2, 3)$ を使って求める ([Ge-Zi] や [Sik] を参照).

3). Silverman の命題により, ナイーブ高さ $h(Q)$ の評価が得られ, x 座標の分子と分母に対する上限 $B \in \mathbb{N}$ が分かる.

4). 手順 I. に戻って, 範囲 B をシラミ潰しに探せば, $P_1 = (-1, 0)$ が見つかる.

Example 3.8. $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 + 9$$

上の有理点 $P = (6, 15)$ を考える. このとき, 二倍公式を用いると

- $P = (6, 15) \Longrightarrow h(P) = 6$
- $2P = (\frac{24}{25}, \frac{395}{125}) \Longrightarrow h(2P) = 25$
- $4P = (-\frac{740784}{429025}, -\frac{551537139}{281011375}) \Longrightarrow h(4P) = 740784$

- $8P = (\frac{125360522428103195662176}{14500721596011932260225}, \frac{446935677515088044280958971345432999}{174616155304581912609214216585337 5})$
  $\Longrightarrow h(8P) = 125360522428103195662176$

が得られ, ナイーブ高さが爆発的に増大することが分かる. 一般に, 高さは指数的に大きさを増すので, 生成元を見つけたければ, 小さい高さからコツコツと探すのが最善と言え, はじめに見つけたものが生成元を与える可能性が高い.

♣ <u>自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成元の計算の仕方 (まとめ)</u>

- ここでは Mordell-Weil 群 $E(\mathbb{Q})$ のランク r はあらかじめ分かっているものとする. 手法は, 高さ関数を使って, シラミ潰しで探すものであり, 有限時間で終了するという保証はなかった. しかし, 導手が 1000 くらいまでの楕円曲線なら, かなりの数の楕円曲線について, 手計算でも決定できることを見た. 詳しい手順は以下の通りである.

I. ナイーブ高さ関数 h による x 座標の分子と分母の上限 B に従って, とにかく有理点を探す.

II. 探してきた有理点が自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ の生成に寄与するかどうかを調べる. 標準高さ関数 $\hat{h}$ を用いて得られる, 高さ対で判定を行うことになる.

III. r 個の独立な元が生成する $E(\mathbb{Q})_{\mathrm{fr}}$ の指数有限部分群 A を大きくして全体に一致させる. 生成元が満たすべきナイーブ高さの評価を, Silverman によるナイーブ高さ h と標準高さ $\hat{h}$ の差を比べた結果から求める. そして, その範囲を再び, シラミ潰しで探す.

- 標準高さ $\hat{h}$ の計算は複雑なので紹介しなかったが, コンピューターに命令すると, すぐに近似値を求めてくれる.

- 一般に, 高さは指数的に大きさを増すので, 生成元を見つけたければ, 小さい高さからコツコツと探すのが最善と言え, はじめに見つけたものが生成元を与える可能性が高い (Example 3.2. と 3.8. を参照).

4. Mordell-Weil 群 $E(\mathbb{Q})$ のランクの決定

ここでは, Mordell-Weil 群のランクを求める方法を紹介したい. 主に, 楕円曲線 E が位数 2 のトーション点を持つときを考える. このときは, Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ を $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ の有限部分群 $\mathbb{Q}(S,2)$ に埋め込んで計算を行えるという利点がある (記号は後に紹介する). 最後に, 位数 2 のトーション点を持つとは限らないときの一般の手法について簡単にコメントしたい.

4.1. 等質空間について. 上記の両方の方法に共通するのは, 楕円曲線 E 上の等質空間 H を分類することである. また, このとき, H は E のツイストである. つまり, 滑らかな曲線で, $\overline{\mathbb{Q}}$ 上 E と同型になっている. 等質空間やツイストについては, [Sil 1,X-§2,3] に簡潔に書かれている. この等質空間は

$$H : y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e \quad (a,b,c,d,e \in \mathbb{Q})$$

なる形をしており, H たち全体がなす集合を各方程式がどの体上で解を持つか否かで分類することを考える. 大まかに言えば, 次のようになる.

1). 有理数体 $\mathbb{Q}$ に大域的な解を持つ H は, Mordell-Weil 群の元を与える.

2). $\mathbb{Q}$ の完備化 $\mathbb{R}$ かつ $\mathbb{Q}_p$ (全ての素数 p) に局所的な解を持つ H は, Selmer 群の元を与える.

3). Hasse 原理が成立しない, つまり, $\mathbb{Q}$ に大域的な解を持たないが, 完備化 $\mathbb{R}$ かつ $\mathbb{Q}_p$ に局所的な解を持つ H は, Tate-Shafarevich 群の元を与える.

次の短完全列が存在することは §4.2. で示すことになる

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

つまり, Mordell-Weil 群 $E(\mathbb{Q})$ のランクを決定するという問題は, E 上の等質空間 H を上の 1).~3). に従って分類するという問題に帰着される. 上の 1).~3). について, コメントをしておく.

4.1.1. 大域的な解を持つ等質空間 H. ここでは, H 上の有理数解を探さなければならないが, これは以前と同様に, コツコツとシラミ潰しで探すほかはなく, 有限時間で終了するという保証はない. しかし, 被覆写像 $H \to E$ を使うことによって, 以下の例が示すように, E 上で計算するより H を導入して計算した方が手間が省ける可能性がある.

Example 4.1. $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 - 673$$

の自由 Mordell-Weil 群 $E(\mathbb{Q})_{\mathrm{fr}}$ はランクが 2 で, その生成元として

$$P_1 = (29, 541), \ P_2 = (33989323537/61761^2, -1384230292401340/61761^3)$$

を持つが, 二つ目の生成元 P_2 は, $(a, b, c, d, e) = (-2, 4, -24, 164, -58)$ を係数に持つ等質空間 H 上の点

$$(x, y) = (191/97, 123522/97^2)$$

から被覆写像 $H \to E$ を通して得られる. このことから, E 上よりも, H 上で計算した方が有理点の高さが小さくなる傾向にあり, 簡単になるという可能性がある.

4.1.2. 局所的な解を持つ等質空間 H. ここでは, $\mathbb{Q}$ の完備化 $\mathbb{R}$ かつ $\mathbb{Q}_p$ に局所的な解を持つかどうかをどのようにして調べるかということについて紹介したい. なお, 原論文 [B,S-D] にあるように, 有限時間で判定できることが分かっている.

a: 等質空間 H が $\mathbb{R}$ で, 局所的な解を持つかどうかは簡単に調べられる. まず, $g(x) = 0$ が解を持つかどうかを見る. 持たないときは $g(x)$ の符号は一定より, a の符号さえ調べれば, 解の有る無しが分かる. よって, 有限時間で判定できる.

b: $\mathbb{Z}_p$ における局所的な解を探せばよい. まずは, mod p で解けるかどうかを調べ, $\mathbb{Z}_p$ に持ち上がるか否かが問題である.

i). 奇素数 p で good な還元を持つときは, mod p で解が存在すれば, $\mathbb{Z}_p$ に持ち上がる (Hensel の補題). mod p では解が必ず存在するので, このステップは結局は無視できる. よって, 非アルキメデス的な局所解は, $p=2$ または素数 p で bad な還元を持つときの, 有限個の場合のみを調べればよいということになる.

Example 4.2. (楕円曲線に対する Hensel の補題の例.)

導手 92 の $\mathbb{Q}$ 上の楕円曲線

$$E: y^2 = x^3 - x + 1$$

を考える. $p=3$ で good な還元を持ち, mod 3 で例えば, $(x,y)=(2,1)$ を解に持つ. このとき, mod 3^2 に持ち上がることを見る.

$$(x,y) = (2+3m, 1+3n), \quad m,n \in \mathbb{Z}$$

とおける. 代入して, mod 3^2 で考えると

$$1+6n+9n^2 = 8+36m+54m^2+27m^3-2-3m+1 \Longrightarrow 1+6n = 7-3m$$

となり, 簡単に解くことができる. 例えば, $(m,n)=(0,1)$ とすると

$$(x,y) = (2,4) \bmod 3^2$$

を得ることになる. 同様にすれば, $\mathbb{Z}_p$ まで持ち上がることが分かる. 一般に, 奇素数 p で good な還元を持ち, mod p で解が存在すれば, $\mathbb{Z}_p$ に持ち上げるのは, この例と同様に, 簡単な不定一次方程式を解くことに帰着されるからである.

ii). $p=2$ や素数 p で bad な還元を持つときに, mod p で解が存在すれば, $\mathbb{Z}_p$ に持ち上がるかどうかを有限時間で判定するアルゴリズムが存在する ([B,S-D] や [C] を参照せよ).

4.1.3. *Hasse* 原理が成立しない等質空間 H. このような等質空間 H が実際に存在し, 楕円曲線 E の Tate-Shafarevich 群の非自明な元を与えるが, 導手 1000 以下の楕円曲線で非自明な Tate-Shafarevich 群を持つのは, 導手 571, 681, 960, $960'$ の四つのみである. 具体例は Example 4.15. で与える.

♡ <u>等質空間の分類の仕方 (まとめ)</u>

等質空間 H が局所解を持つかどうかは, <u>a</u>: $\mathbb{R}$ に持つか, <u>b</u>: $p=2$ または p で bad な還元を持つ素数に対して持つかのみを調べればよく, 有限時間で導出が終わることが知られている. 一方で, 大域解については, 小さい高さからコツコツとシラミ潰しに探すしかない.

4.1.4. 等質空間の定義と基本的な性質. ここでは, 等質空間の定義と簡単な性質について, まとめておく.

Definition 4.3. E を $\mathbb{Q}$ 上の楕円曲線とする. このとき, $E/\mathbb{Q}$ に対する等質空間とは $\mathbb{Q}$ 上の滑らかな曲線 H と次をみたす射 $\mu: H\times E \to H$ の対 (H,μ) のことである:

(1) $\forall p \in H$ に対して, $\mu(p, O) = p$ が成り立つ.

(2) $\forall p \in H$ and $P, Q \in E$ に対して, $\mu(\mu(p, P), Q) = \mu(p, P+Q)$ が成り立つ.

(3) $\forall p, q \in H$ に対して, $\mu(p, P) = q$ となる $P \in H$ が唯一つ, 存在する.

つまり, $E/\mathbb{Q}$ に対する等質空間とは, E 上に単純推移的な代数群の作用を持つ $\mathbb{Q}$ 上の滑らかな曲線 H のことである.

Remark 4.4. 上記の記号のもとで, さらに, 点 $p_0 \in H$ を固定し, 射

$$\theta : E \to H \quad (P \mapsto \mu(p_0, P))$$

を考える. このとき, θ は $\mathbb{Q}(p_0)$ 上で同型になり, H は E の $\mathbb{Q}$ 上のツイストであると言える ([Sil 1,X-(3.2)]).

Definition 4.5. E を $\mathbb{Q}$ 上の楕円曲線とする. このとき, $E/\mathbb{Q}$ に対するふたつの等質空間 $H/\mathbb{Q}$ と $H'/\mathbb{Q}$ が同値であるとは, $\mathbb{Q}$ 上定義された同型 $\theta : H \simeq H'$ で E 上への作用が両立しているものが存在することと定義する. また, E が含まれている同値類を自明な同値類と呼ぶ. これらの等質空間たちのなす同値類の集合を $E/\mathbb{Q}$ に対する Weil-Châtelet 群と呼び, $WC(E/\mathbb{Q})$ と書くことにする.

Remark 4.6. $H/\mathbb{Q}$ に対して, $H(\mathbb{Q})$ が空集合でないことと $H/\mathbb{Q}$ が自明な同値類に含まれることが同値であり ([Sil 1,X-(3.3)]), 前の小節でも述べたように, 等質空間がどの体上 (global or local) で点を持つかによって, $WC(E/\mathbb{Q})$ を分類し, Mordell-Weil 群 $E(\mathbb{Q})$ のランクを計算していく.

Proposition 4.7. 次の自然な全単射が存在する

$$WC(E/\mathbb{Q}) \simeq H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E).$$

具体的には, $\mathbb{Q}$ 上の楕円曲線 E の等質空間 H に対して, 点 $p_0 \in H$ を選んだときに, 上の全単射は

$$\{H/\mathbb{Q}\} \to \{\sigma \mapsto p_0^\sigma - p_0\}$$

によって定義される *([Sil 1,X-(3.6)])*.

4.2. **Selmer 群と Tate-Shafarevich 群について.** この節では, 標記のことについての基本的な性質について簡単にまとめておく. $\mathbb{Q}$ 上の楕円曲線 E に対して, 同種写像 $\phi : E \to E'$ を考える. このとき, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-加群の短完全列

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

を得ることができる. 但し, $E[\phi]$ は同種写像 ϕ の kernel をあらわすものとする. ここでガロア・コホモロジーを考えると, 長完全列

$$\begin{array}{l} 0 \to \quad E(\mathbb{Q})[\phi] \quad \to \quad E(\mathbb{Q}) \quad \xrightarrow{\phi} \quad E'(\mathbb{Q}) \\ \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E[\phi]) \to H^1(G_{\mathbb{Q}}, E) \to H^1(G_{\mathbb{Q}}, E') \to; \end{array}$$

が得られ, 次の短完全列を形成することができる

$$(*)\quad 0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E[\phi]) \to H^1(G_{\mathbb{Q}}, E)[\phi] \to 0.$$

前節で述べたことから, 三つ目の項は Weil-Châtelet 群 $WC(E/\mathbb{Q})$ の ϕ -トーション・パートと同一視できることを注意しておく. ここで, $(*)$ の局所版を考えることにより, 次の可換図式が得られることになる

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(\mathbb{Q})/\phi(E(\mathbb{Q})) & \xrightarrow{\delta} & H^1(G_{\mathbb{Q}}, E[\phi]) & \longrightarrow & WC(E/\mathbb{Q})[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod E'(\mathbb{Q}_v)/\phi(E(\mathbb{Q}_v)) & \xrightarrow{\delta} & \prod H^1(G_{\mathbb{Q}_v}, E[\phi]) & \longrightarrow & \prod WC(E/\mathbb{Q}_v)[\phi] & \longrightarrow & 0.
\end{array}$$

ここで, v は素数全体と無限素点を走るものとし, $G_{\mathbb{Q}_v} = \mathrm{Gal}(\overline{\mathbb{Q}_v}/\mathbb{Q}_v)$ とおいた.

Definition 4.8. 上記の記号のもとで, $\phi : E \to E'$ に対する, ϕ-Selmer 群を

$$S^{(\phi)}(E/\mathbb{Q}) = \ker\left\{H^1(G_{\mathbb{Q}}, E[\phi]) \to \prod WC(E/\mathbb{Q}_v)\right\}$$

とし, Tate-Shafarevich 群を

$$Ш\,(E/\mathbb{Q}) = \ker\left\{WC(E/\mathbb{Q}) \to \prod WC(E/\mathbb{Q}_v)\right\}$$

と定義する. Шの元は, $\mathbb{Q}$ に大域的な解を持たないが, 完備化 $\mathbb{R}$ と $\mathbb{Q}_p$ に局所的な解を持つ等質空間 H によって定まるということができる.

これらの定義より, 次の短完全列

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E/\mathbb{Q}) \to Ш\,(E/\mathbb{Q})[\phi] \to 0$$

が存在することが分かった. 各項に対する等質空間による解釈は §4.1 の冒頭で述べた通りである.

4.3. **位数 2 の元が存在するときのランクの決定.** この節では, $\mathbb{Q}$ 上の楕円曲線 E が位数 2 のトーション点を持つときに, その Moderll-Weil 群 $E(\mathbb{Q})$ のランクを計算する方法を紹介する. 位数 2 のトーション点が存在するときは, 一般のときと比べて, $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ を $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ の有限部分群 $\mathbb{Q}(S, 2)$ (この節で定義する) に埋め込んで計算を行えるという利点がある. なお, 導手 1000 以下の楕円曲線で位数 2 のトーション点を持つものと持たないものはおよそ半々くらいである.

4.3.1. 設定と記号. $\mathbb{Q}$ 上の楕円曲線 E が位数 2 のトーション点 P を持つとする. このとき, 座標変換により

$$E : y^2 = x(x^2 + ax + b) \quad (a, b \in \mathbb{Z})$$

なる方程式を持ち, $P = (0, 0)$ と仮定してよい. さらに, E' として次の楕円曲線を考える

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

このとき, $\phi : E \to E'$ を

$$\phi(x, y) = (y^2/x^2, y(b - x^2)/x^2)$$

で定義すると, ϕ は次数 2 の同種写像を与え, その kernel は $E[\phi] = \{O, P\}$ となることが分かる. よって, $E[\phi]$ と μ_2 を同一視すれば, $H^1(G_{\mathbb{Q}}, E[\phi]) \simeq \mathbb{Q}^*/(\mathbb{Q}^*)^2$ となり, Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ が $\mathbb{Q}^*/\mathbb{Q}^{*2}$ に埋め込まれることが分かる.

Proposition 4.9. *$m \in \mathbb{N}$ に対して, S を $\mathbb{Q}$ の素点の部分集合で, 1). 無限素点, 2). E が bad な還元を持つ素点, 3). m を割る素数たちで構成されるものとする. さらに, $\mathbb{Q}^*/(\mathbb{Q}^*)^m$ の部分集合 $\mathbb{Q}(S, m)$ を*

$$\mathbb{Q}(S, m) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^m \mid \mathrm{ord}_p(b) \equiv 0 \pmod m \text{ for all } p \notin S\}$$

と定義する. このとき, $\delta : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow H^1(G_{\mathbb{Q}}, E[\phi])$ を通して, $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ は $\mathbb{Q}(S, 2)$ に

$$O \mapsto 1, \quad (0, 0) \mapsto a^2 - 4b, \quad (X, Y) \mapsto X \ (X \neq 0, \infty)$$

で埋め込まれる ([Sil 1,X-(1.1),(4.9)]).

Example 4.10. (以後, この例を中心に計算していく.)

導手 544 の $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 - 6x^2 + 17x$$

に対して, 判別式は $\Delta = -147968 = -2^9 \cdot 17^2$ で与えられ, $S = \{\infty, 2, 17\}$ となる. よって, 定義より

$$\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm 17, \pm 34\}$$

となることが分かる. 一方で, 上で定義した E と同種な楕円曲線 E' は

$$E' : Y^2 = X^3 + 12X^2 - 32X$$

なる方程式で与えられ, 同種写像は $\phi(x, y) = (y^2/x^2, y(17 - x^2)/x^2)$ となる. このとき, 上の Proposition より, $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ は有限群 $\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm 17, \pm 34\}$ に埋め込まれることが分かる.

有限群 $\mathbb{Q}(S, 2)$ は $H^1(G_{\mathbb{Q}}, E[\phi]) \simeq \mathbb{Q}^*/(\mathbb{Q}^*)^2$ の部分群で, $d \in \mathbb{Q}(S, 2)$ に対応する 1-コサイクル ξ_d が存在する. さらに, この 1-コサイクル ξ_d に対応する $E : y^2 = x^3 + ax^2 + bx$ の等質空間 H_d の方程式は

$$z = \sqrt{d}x/y, \quad w = \sqrt{d}(x - b/x)(x/y)^2$$

を用いて, 次の式で与えられる (詳しくは [Sil 1,X-(3.7)] を参照)

$$H_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

このとき, 対応 $(x, y) \mapsto (z, w)$ により, $\mathbb{Q}(\sqrt{d})$ での同型 $E \simeq H_d$ を与えているのが分かり, H_d は E の $\mathbb{Q}$ 上のツイストとなる. ここで考えた 1-コサイクルと等質空間との対応は次の写像にまとめられる

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}(S, 2) \hookrightarrow H^1(G_{\mathbb{Q}}, E[\phi]) \twoheadrightarrow WC(E/\mathbb{Q})[\phi].$$

また, これらの対応のもとで, Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ は

$$S^{(\phi)}(E/\mathbb{Q}) \simeq \{d \in \mathbb{Q}(S, 2) \mid H_d(\mathbb{Q}_v) \neq \varnothing \text{ for all } v \in S\}$$

と同一視できることにも注意しておく (等質空間の節のまとめを参照). Selmer 群のこの表示からも明らかなように, この群の計算は有限個 $\sharp\mathbb{Q}(S,2)\times\sharp S$ の $H_d(\mathbb{Q}_v)$ について調べればよく, 有限時間で決定できる.

4.3.2. *Selmer*群 $S^{(\phi)}(E/\mathbb{Q})$ の決定. これらの準備の下に, まずはSelmer群 $S^{(\phi)}(E/\mathbb{Q})$ の計算の仕方について紹介する.

Example 4.11. (Example 4.10. の続き.)

導手 544 の $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 - 6x^2 + 17x$$

に対して, $\mathbb{Q}(S,2) = \{\pm1, \pm2, \pm17, \pm34\}$ と計算された. 一方で, 上で定義した E と同種な楕円曲線 E' は

$$E' : Y^2 = X^3 + 12X^2 - 32X$$

なる方程式で与えられていた. Selmer 群

$$S^{(\phi)}(E/\mathbb{Q}) \simeq \Big\{d \in \{\pm1, \pm2, \pm17, \pm34\} \mid H_d(\mathbb{Q}_v) \neq \varnothing \text{ for all } v \in \{\infty, 2, 17\}\Big\}$$

を決定するには, どの $d \in \mathbb{Q}(S,2)$ に対して, H_d が局所的に解を持つか持たないかを調べればよい. 前にも述べたように, この Selmer 群の計算は有限時間で導出が終わる.

- $\underline{d = 17 \text{ のとき}}$ $\qquad H_{17} : 17w^2 = 17^2 + 12\cdot17z^2 - 32z^4$

ここで, $H_{17}(\mathbb{Q}_{17}) = \varnothing$ であることを示そう. まず

$$w = 17^m a, \quad z = 17^n b \qquad (m, n \in \mathbb{Z}, a, b \in \mathbb{Z}_p^*)$$

とおく. このとき, 左辺の 17 進付値は $2m+1$, 右辺の 17 進付値は $\min\{2, 2n+1, 4n\}$ となるので, $2m+1 = 2n+1$, $2n+1 \leq 2, 4n$ が必要になる. しかし, これを満たすのは $n = \frac{1}{2}$ のみとなり矛盾. よって, 局所的な解が存在せず, $17 \notin S^{(\phi)}(E/\mathbb{Q})$ となる. mod 17 の解が mod 17^3 に持ち上がらなくなることを示してもよい.

- $\underline{d = 2 \text{ のとき}}$ $\qquad H_2 : 2w^2 = 4 + 24z^2 - 32z^4$

係数を簡約するために, $z = Z/2$ とおくと

$$H_2 : w^2 = 2 + 3Z^2 - Z^4$$

と変形される. すべての $v \in S$ に対して, $H_2(\mathbb{Q}_v) \neq \varnothing$ を示してもよいが, 高さの小さいものから順に, シラミ潰しで有理点を探すと, $(Z, w) = (1, 2)$ が見つかる. よって, $2 \in S^{(\phi)}(E/\mathbb{Q})$ が分かり, しかも, 大域解であるので, Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ にも寄与する.

他にも, Proposition 4.9. の $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ を $\mathbb{Q}(S,2)$ に埋め込む方法により, E' 上の自明な点 $(X, Y) = (0, 0)$ は $d = -2$ に写されるので, $-2 \in S^{(\phi)}(E/\mathbb{Q})$ となる. $S^{(\phi)}(E/\mathbb{Q})$ が群構造を持つことを考慮すると

$$S^{(\phi)}(E/\mathbb{Q}) = \{\pm1, \pm2\}$$

と決定されることが分かる.

♡ Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ の計算の仕方 (まとめ)

A). 判別式 Δ より, 素点の集合 S と $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ の有限部分群 $\mathbb{Q}(S,2)$ を求める.

B). Selmer 群は $S^{(\phi)}(E/\mathbb{Q}) \simeq \left\{d \in \mathbb{Q}(S,2) \mid H_d(\mathbb{Q}_v) \neq \varnothing \text{ for all } v \in S\right\}$ と書けるので, $d \in \mathbb{Q}(S,2)$ に対応する等質空間 H_d に対して, $H_d(\mathbb{Q}_v) \neq \varnothing$ $(v \in S)$ かを調べる.

1). $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ を $\mathbb{Q}(S,2)$ に埋め込む方法より, E' 上の自明な点 $(X,Y) = (0,0)$ がどれと対応するのかを調べる. Selmer 群の元を与えることになる.

2). 大域解をコツコツと調べてみる. すぐに見つかれば, 局所的な計算はする必要なし.

3). 正道として, $H_d(\mathbb{Q}_v) \neq \varnothing$ $(v \in S)$ かを調べる. また, 群構造などを使って, 計算の省略なども考えてみる. 有限時間で終了することが保証されている.

4.3.3. *Tate-Shafarevich* 群 Ш $(E/\mathbb{Q})$ の決定.

A). Ш $(E/\mathbb{Q})$ が自明なとき

前にも述べたように, 導手 1000 以下の楕円曲線で Ш $(E/\mathbb{Q})$ が非自明なものは四つしかなかった. よって, ほとんどの場合は, 短完全列

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E/\mathbb{Q}) \to Ш\,(E/\mathbb{Q})[\phi] \to 0$$

において, Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ と Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ が一致することになる. つまり, Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ の元 d と対応するすべての等質空間 H_d が $\mathbb{Q}$ 上に大域解を持つのである. 等質空間 H_d 上の大域解 P と Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ の元 d との関係を数式で書くと次のようになる ([Sil 1,X-(4.9)]).

Proposition 4.12. 上記の記号のもとで, 写像 ψ を

$$\psi : H_d \to E', \quad \psi(z,w) = (d/z^2, -dw/z^3)$$

と定義し, $\delta : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}(S,2)$ と書く. このとき, 大域解 $P \in H_d(\mathbb{Q})$ が存在すれば, 次の式が成立する *(P に依存せずに)*

$$\delta(\psi(P)) \equiv d \pmod{(\mathbb{Q}^*)^2}.$$

♠ 疑問

Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ の元 d は大域解を持つ等質空間 H_d と対応していた. ランク 1 のときに, 等質空間 H_d と Heegner 点とは関係がないのか?

Example 4.13. (Example 4.11. の復習.)

導手 544 の $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 - 6x^2 + 17x$ に対して, 同種な楕円曲線 E' は $Y^2 = X^3 + 12X^2 - 32X$ なる方程式で与えられていた. また, Selmer 群

は $S^{(\phi)}(E/\mathbb{Q}) = \{\pm1, \pm2\}$ と与えられることが分かった．ここでは, 等質空間 H_d $(d = \pm1, \pm2)$ が大域解を持つことをシラミ潰しの方法で探し, $\text{Ш}(E/\mathbb{Q})[\phi] = 0$ を示す．群構造を考えれば, H_2 と H_{-2} が大域解を持つことを示せば十分である．

• $d = -2$ のとき

このときは, E' 上の自明な点 $(0,0)$ が $\delta : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}(S,2)$ を通して, $\delta(0,0) = -32 \equiv -2 \pmod{(\mathbb{Q}^*)^2}$ と写され, Selmer 群 $S^{(\phi)}(E/\mathbb{Q}) = \{\pm1, \pm2\}$ の元 $d = -2$ と対応する (Proposition 4.9. を参照).

• $d = 2$ のとき

等質空間 $H_2 : 2w^2 = 4 + 24z^2 - 32z^4$ の係数を簡約するために, $z = Z/2$ とおくと, $H_2 : w^2 = 2 + 3Z^2 - Z^4$ と変形された．高さの小さいものから順に, シラミ潰しで有理点を探すと, $(Z, w) = (1, 2)$, つまり, $(z, w) = (\frac{1}{2}, 2)$ が見つかる．上の Proposition の記号のもとで,

$$\psi(\frac{1}{2}, 2) = (8, -32) \in E'(\mathbb{Q}), \quad \delta(\psi(\frac{1}{2}, 2)) = 2 \pmod{(\mathbb{Q}^*)^2}$$

が確かめられる．

Remark 4.14. 前にも述べたように, 等質空間による被覆写像 $H \to E'$ を使えば, E' 上で有理点を探し, Selmer 群の元と対応するかを調べるより, H 上で有理点を探す方がシラミ潰しの範囲が小さくて済むことが多い．今の例だと, $(8, -32) \in E'(\mathbb{Q})$ に対して, $(z, w) = (\frac{1}{2}, 2) \in H_2(\mathbb{Q})$ だった．

B). $\text{Ш}(E/\mathbb{Q})$ が非自明な例

Example 4.15. 導手 18496 の $\mathbb{Q}$ 上の楕円曲線

$$E : y^2 = x^3 + 17x$$

に対して, $\text{Ш}(E/\mathbb{Q})$ が非自明になることを具体的に示す．まず, 上で定義した E と同種な楕円曲線 E' は $Y^2 = X^3 - 68X$ なる方程式で与えられる．また, $\mathbb{Q}(S, 2) = \{\pm1, \pm2, \pm17, \pm34\}$ と計算される．よって, Selmer 群は

$$S^{(\phi)}(E/\mathbb{Q}) \simeq \Big\{ d \in \{\pm1, \pm2, \pm17, \pm34\} \mid H_d(\mathbb{Q}_v) \neq \varnothing \text{ for all } v \in \{\infty, 2, 17\} \Big\}$$

と書ける．これを決定するには, どの $d \in \mathbb{Q}(S, 2)$ に対して, H_d が局所的に解を持つか持たないかを調べればよい (有限時間で終了)．実際に計算を行うと

$$S^{(\phi)}(E/\mathbb{Q}) \simeq \{\pm1, \pm2, \pm17, \pm34\}$$

のようになる ([Sil 1,p.312-314])．ここでは, $2 \in S^{(\phi)}(E/\mathbb{Q})$ に対応する等質空間

$$H_2 : w^2 = 2 - 34z^4$$

が $\mathbb{Q}$ 上に大域解を持たないことを初等的に示す．但し, $S^{(\phi)}(E/\mathbb{Q})$ の元に対応するので, 局所的には解を持っている．

Proof. まず, $(z,w)=(r/t,2s/t^2)$ $(r,s,t\in\mathbb{Z})$ の形をしており, 次を満たさなければならないことが分かる

$$(*)\quad 2s^2=t^4-17r^4,\quad \gcd(r,s,t)=1.$$

左辺の s^2 が mod 17 で 4 乗になっていること, つまり, $X^4\equiv s^2 \pmod{17}$ となる $X\in\mathbb{Z}$ が存在することを示す. まず, ルジャンドル記号 $(\frac{q}{p})=1$ で $Y^2\equiv q \pmod p$ となる $Y\in\mathbb{Z}$ が存在するということをあらわしていたのを思い出そう. 平方剰余法則を使うことによって

$$(\frac{2}{17})=1,\quad (\frac{q}{17})=1\quad (q\mid s \text{ なる奇素数})$$

を示せば, 左辺の s^2 が mod 17 で 4 乗になっていることが分かる.

(1) $(\frac{2}{17})=1$ について
これは, $6^2\equiv 2 \pmod{17}$ からもすぐに分かる.

(2) $(\frac{q}{17})=1$ について
$(*)$ の両辺を mod q で考えれば, $(\frac{17}{q})=1$ が分かる. 平方剰余法則 $(\frac{p}{q})\cdot(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ を使うことで, $(\frac{q}{17})=1$ を得る.

よって, 左辺の s^2 が mod 17 で 4 乗になっていることが分かった. $(*)$ の両辺を mod 17 すると, 2 も mod 17 で 4 乗とならないといけないが, これは矛盾である. 従って, H_2 に大域解が存在しないことが分かる. □

Remark 4.16. Tate-Shafarevich 群 Ш $(E/\mathbb{Q})$ は有限群であることが予想されており, さらには, Cassels によって, その予想の下で, 位数が perfect square であることが示されている. また, Ш $(E/\mathbb{Q})$ が有限群であれば, 原理的には, 有限時間で Mordell-Weil 群が決定できる ([Sil 1, p.304-306]).

4.3.4. *Mordell-Weil* 群 $E(\mathbb{Q})$ のランクの決定. 今までのことを総合して, Mordell-Weil 群 $E(\mathbb{Q})$ のランクを決定しよう.

Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ の決定や E に対する等質空間 H_d の大域解を地道に調べることで, $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ の位数が $n'=2^{e'}$ と分かったとする. また, E と E' の役割を入れ替えて計算することで, $E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))$ の位数が $n=2^e$ と決定できたとする. 但し, ここで, $\phi':E'\to E$ は $\phi:E\to E'$ の双対同種とする. このとき, この ϕ' を使うことで, $E(\mathbb{Q})/2E(\mathbb{Q})$ 上に, 重複度を込めて, nn' 個の有理点を構成できる.

r を Mordell-Weil 群 $E(\mathbb{Q})$ のランクとしたとき, 以下が成立する.

- $\sharp E(\mathbb{Q})[2]=4$ のとき (このときは重複度なし)

$$nn'=\sharp E(\mathbb{Q})/2E(\mathbb{Q})=2^{r+2}.$$

• $\sharp E(\mathbb{Q})[2]=2$ のとき (このときは重複度 2)

$$\frac{nn'}{2}=\sharp E(\mathbb{Q})/2E(\mathbb{Q})=2^{r+1}.$$

Example 4.17. (Example 4.13. の続き.)

導手 544 の $\mathbb{Q}$ 上の楕円曲線 $E: y^2=x^3-6x^2+17x$ に対して, 同種な楕円曲線 E' は $Y^2=X^3+12X^2-32X$ なる方程式で与えられていた. また, Selmer 群は $S^{(\phi)}(E/\mathbb{Q})=\{\pm1,\pm2\}$ と与えられることが分かった. さらには, $Ш(E/\mathbb{Q})[\phi]=0$ より, $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ は Selmer 群 $S^{(\phi)}(E/\mathbb{Q})=\{\pm1,\pm2\}$ と同型になり

$$\sharp E'(\mathbb{Q})/\phi(E(\mathbb{Q}))=2^2$$

となる. 一方で, E と E' の役割を入れ替えて同様の計算をすることで, $S^{(\phi')}(E/\mathbb{Q})=\{1,17\}$ かつ $Ш(E/\mathbb{Q})[\phi']=0$ となり

$$\sharp E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))=2$$

が分かる. 簡単に $\sharp E(\mathbb{Q})[2]=2$ と計算できるので, 上の式より,

$$E(\mathbb{Q})\simeq E'(\mathbb{Q})\simeq \mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

を得ることができた.

Remark 4.18. ここでは, 位数 2 の元が存在するときのランクの決定について紹介した. 一般に, 位数 2 の元が存在しないときの方法について述べておく. 位数 2 の元が存在するときは有限群 $\mathbb{Q}(S,2)$ を使って, E に対する等質空間 H_d を分類すればよかった. (Cremona の本における) 一般のときには, そのような有限群がなく, どのくらい E 上に等質空間 H_d が存在するかを求めなければならない. これは有限時間で求めることができるものの, 非常に厄介である.

♣ Mordell-Weil 群 $E(\mathbb{Q})$ のランクの決定の仕方 (まとめ)

ここでは, 位数 2 の元が存在すると仮定する.

1). 有限群 $\mathbb{Q}(S,2)$ を使って, E 上の等質空間を求める. そして, Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ を等質空間の局所解が存在するかどうかを見ることで計算を行う. 有限時間で実行できることが保障されている.

2). Mordell-Weil 群 $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ と Selmer 群 $S^{(\phi)}(E/\mathbb{Q})$ の差である Tate-Shafarevich 群 $Ш(E/\mathbb{Q})$ が自明か非自明かを見る. このためには, Mordell-Weil 群の生成元をコツコツと探さなければならないが, 導手 1000 以下なら, 生成元の高さも小さいし, $Ш(E/\mathbb{Q})$ が非自明なものも四つしかないので, 多くの場合が計算可能と言える. ただ, 有限時間で実行できるとは保障されていない.

3). E と E' の役割を入れ替えて同様の計算をすることで, Mordell-Weil 群 $E(\mathbb{Q})$ のランクが決定される.

References

[B-SD] Birch, B. J.; Swinnerton-Dyer, H. P. F.: *Notes on elliptic curves. I.* J. Reine Angew. Math. 212. 1963. 7-25.

[C] Cremona, J.E.: *Algorithms for modular elliptic curves. Second edition.* Cambridge University Press, Cambridge, 1997. vi+376 pp.

[Ge-Zi] Gebel, Josef.; Zimmer, Horst G.: *Computing the Mordell-Weil group of an elliptic curve over* $\mathbb{Q}$. Elliptic curves and related topics, 61-83, CRM Proc. Lecture Notes, 4, 1994.

[Ma 1] Mazur, B.:*Rational points on modular curves.* Modular functions of one variable, V, pp. 107-148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

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

[Sik] Siksek, S.: *Infinite descent on elliptic curves.* Rocky Mountain J. Math. 25 (1995), no. 4, 1501-1538.

[Sil 1] Silverman, Joseph H.:*The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986. xii+400 pp.

[Sil 2] Silverman, Joseph H.: *Computing heights on elliptic curves.* Math. Comp. 51 (1988), no. 183, 339-358.

[Sil 3] Silverman, Joseph H.:*Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp.

Department of Mathematics, Hokkaido University, Sapporo 060-0810, Japan

E-mail address: `morita@math.sci.hokudai.ac.jp`

TABLE 2

MORDELL–WEIL GENERATORS

This table contains an entry for the strong Weil curve in each isogeny class[1] of positive rank. For each we give the (x, y) coordinates of generators of the Mordell–Weil group (modulo torsion) with respect to the minimal equation of Table 1. In a few cases the coordinates are not integral, in which case we give them in the form $(a/c^2, b/c^3)$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.

[1] This is the first curve in the class except for class 990H, where we give a generator for the curve 990H3.

Curve	x	y
37 A1 (A)	0	0
43 A1 (A)	0	0
53 A1 (A)	0	0
57 A1 (E)	2	1
58 A1 (A)	0	1
61 A1 (A)	1	0
65 A1 (A)	1	0
77 A1 (F)	2	3
79 A1 (A)	0	0
82 A1 (A)	0	0
83 A1 (A)	0	0
88 A1 (A)	2	2
89 A1 (C)	0	0
91 A1 (A)	0	0
91 B1 (B)	−1	3
92 B1 (C)	1	1
99 A1 (A)	0	0
101 A1 (A)	−1	0
102 A1 (E)	−1	2
106 B1 (A)	2	1
112 A1 (K)	0	2
117 A1 (A)	0	2
118 A1 (A)	0	1
121 B1 (D)	4	5
122 A1 (A)	1	1
123 A1 (A)	1	1
123 B1 (C)	1	0
124 A1 (B)	1	1
128 A1 (C)	0	1
129 A1 (E)	1	4
130 A1 (E)	2	2
131 A1 (A)	0	0
135 A1 (A)	4	7
136 A1 (A)	−2	2
138 A1 (E)	0	1
141 A1 (E)	−3	4
141 D1 (I)	0	0
142 A1 (F)	1	1
142 B1 (E)	−1	1
143 A1 (A)	4	6
145 A1 (A)	0	1
148 A1 (A)	−1	2
152 A1 (A)	−1	2
153 A1 (C)	0	1
153 B1 (A)	5	13
154 A1 (C)	2	3
155 A1 (D)	2	5
155 C1 (C)	1	0

Curve	x	y
156 A1 (E)	1	1
158 A1 (E)	−1	4
158 B1 (D)	0	1
160 A1 (D)	0	2
162 A1 (K)	2	0
163 A1 (A)	1	0
166 A1 (A)	0	2
170 A1 (A)	0	2
171 B1 (A)	2	4
172 A1 (A)	2	1
175 A1 (B)	2	−3
175 B1 (C)	−3	12
176 C1 (A)	1	2
184 A1 (C)	0	1
184 B1 (B)	2	1
185 A1 (D)	4	12
185 B1 (A)	0	2
185 C1 (B)	3	2
189 A1 (A)	−1	1
189 B1 (C)	−3	9
190 A1 (D)	13	33
190 B1 (C)	1	2
192 A1 (Q)	3	2
196 A1 (A)	0	1
197 A1 (A)	1	0
198 A1 (I)	−1	5
200 B1 (C)	−1	1
201 A1	1	1
201 B1	−1	2
201 C1	16	−7
203 B1	2	2
205 A1	−1	8
207 A1	0	4
208 A1	4	8
208 B1	4	4
209 A1	−5	9
210 D1	−1	1
212 A1	2	2
214 A1	0	4
214 B1	0	0
214 C1	11	10
215 A1	6	12
216 A1	−2	6
218 A1	−2	2
219 A1	2	0
219 B1	2	4
219 C1	−6	7
220 A1	3	1

Curve	x	y
224 A1	1	2
225 A1	1	1
225 E1	−5	22
226 A1	0	1
228 B1	3	6
229 A1	−1	1
232 A1	2	4
234 C1	1	1
235 A1	−2	3
236 A1	1	1
238 A1	24	100
238 B1	1	1
240 C1	1	2
242 A1	0	1
243 A1	1	0
244 A1	−1	2
245 A1	7	17
245 C1	12	24
246 D1	3	3
248 A1	0	1
248 C1	1	1
249 A1	4	−2
249 B1	0	1
252 B1	−2	9
254 A1	2	0
254 C1	−1	1
256 A1	0	1
256 B1	−1	1
258 A1	2	3
258 C1	5	6
262 A1	−2	5
262 B1	1	0
265 A1	8	0
269 A1	−1	0
272 A1	0	2
272 B1	−1	2
273 A1	11	31
274 A1	2	1
274 B1	31	−15
274 C1	−1	1
275 A1	8	21
277 A1	1	0
278 A1	2	3
280 A1	1	2
280 B1	−18	70
282 B1	3	2
285 A1	1	4
285 B1	6	13

Curve	x	y
286 B1	19	78
286 C1	1	5
288 A1	1	2
288 B1	−3	4
289 A1	−12	38
290 A1	−5	4
291 C1	0	0
294 G1	1	5
296 A1	1	2
296 B1	3	2
297 A1	15	49
297 B1	0	0
297 C1	4	7
298 A1	2	1
298 B1	1	0
300 D1	1	3
302 A1	7	3
302 C1	1	1
303 A1	−2	13
303 B1	0	1
304 A1	10	32
304 C1	0	4
304 F1	3	2
306 B1	−2	5
308 A1	7	14
309 A1	3	3
310 B1	6	0
312 B1	−1	1
312 F1	−1	3
314 A1	6	13
315 B1	−2	1
316 B1	−1	2
318 C1	5	11
318 D1	1	5
320 B1	1	1
320 F1	−2	1
322 A1	−2	8
322 D1	0	2
324 C1	1	1
325 A1	2	9
325 B1	1	0
326 A1	−5	3
326 B1	0	2
327 A1	1	1
328 A1	−2	2
330 E1	−3	4
331 A1	1	0
333 A1	−3	0

Curve	x	y
333 B1	2	7
333 C1	2	1
335 A1	2	2
336 E1	2	6
338 A1	0	1
338 E1	5	10
338 F1	23	73
339 A1	18	40
339 C1	1	1
340 A1	4	3
342 C1	−3	15
342 E1	0	1
344 A1	0	2
345 B1	−1	1
345 F1	5	7
346 B1	−1	2
347 A1	0	0
348 A1	0	1
348 D1	10	27
350 C1	1	3
350 F1	−1	35
352 B1	1	4
352 C1	3	4
352 D1	3	4
352 F1	12	44
354 C1	13	7
354 F1	3	4
356 A1	2	2
357 B1	4	3
357 D1	0	10
359 A1	3	−1
359 B1	2	−1
360 E1	−2	1
361 A1	0	9
362 A1	1	0
362 B1	1	3
364 A1	−8	98
364 B1	1	2
366 F1	3	4
366 G1	−3	13
368 A1	3	6
368 D1	1	1
368 E1	1	1
368 G1	4	1
369 A1	1	4
370 A1	1	0
371 A1	14	42
372 A1	0	3

Curve	x	y
372 D1	−2	3
373 A1	−1	0
374 A1	−1	6
377 A1	−2	5
378 D1	2	2
378 F1	4	11
380 A1	−1	2
381 A1	−2	1
384 D1	2	1
384 H1	4	3
385 A1	2	−9
385 B1	−1	3
387 B1	10	22
387 C1	0	1
389 A1	{ 0 { 1	0 } 0 }
390 A1	1	1
392 A1	9	22
392 C1	−2	7
392 F1	1	1
396 B1	2	9
399 A1	−10	33
399 B1	−2	1
400 A1	15	50
400 C1	12	40
400 H1	1	4
402 A1	4	6
402 D1	7	2
404 A1	0	2
405 B1	1	3
405 C1	0	1
405 D1	4	2
405 F1	−1	0
406 A1	9	10
406 B1	3	12
406 C1	7	3
408 D1	7	18
410 A1	1	2
410 D1	8	16
414 C1	5	11
414 D1	1	17
416 B1	0	2
418 B1	5	19
422 A1	2	1
423 A1	−2	4
423 C1	18	63
423 F1	8	4
423 G1	1	1

Curve	x	y
425 A1	0	4
425 B1	10	20
425 C1	1	0
425 D1	−9	5
426 A1	7	10
427 B1	1	0
427 C1	−3	1
428 B1	1	1
429 A1	0	1
429 B1	6	−15
430 A1	3	−1
430 B1	1	2
430 C1	−2	0
430 D1	−26	213
431 A1	1	0
432 B1	2	2
432 D1	5	12
432 F1	5	16
433 A1	$\{-1$	$0\}$
	$\{0$	$1\}$
434 A1	−1	2
434 D1	0	7
437 A1	10	34
438 C1	−1	2
438 D1	24	−20
438 F1	1	0
438 G1	0	1
440 A1	−4	1
440 B1	2	3
441 B1	2	4
441 C1	30	−211
441 D1	2	2
441 F1	4	4
442 B1	−9	21
443 A1	−1	0
443 B1	−1	1
444 B1	3	3
446 A1	4	2
446 B1	−5	10
446 D1	$\{0$	$2\}$
	$\{1$	$0\}$
448 A1	0	4
448 B1	4	8
448 G1	1	4
450 C1	9	18
450 F1	−1	38
451 A1	7	20
455 A1	2	−5

Curve	x	y
455 B1	14	36
456 C1	3	6
456 D1	23	114
458 A1	2	1
458 B1	−3	5
459 A1	2	1
459 B1	4	8
459 H1	−2	5
460 C1	−6	25
460 D1	4	5
462 A1	4	7
462 C1	1	2
462 E1	−17	92
464 A1	0	2
464 B1	6	2
465 A1	0	−4
465 B1	7	13
467 A1	1	0
468 C1	0	9
469 A1	−5	4
469 B1	2	−1
470 A1	1	7
470 C1	−8	29
470 E1	1	0
470 F1	−9	24
471 A1	0	1
472 A1	0	1
472 E1	0	2
473 A1	15	21
474 A1	14	57
474 B1	1	2
475 B1	10	31
475 C1	0	1
477 A1	2	0
480 A1	−1	2
480 F1	−1	10
481 A1	$87/2^2$	$63/2^3$
482 A1	17	55
484 A1	18	121
485 B1	0	0
486 A1	2	3
486 B1	−1	1
486 F1	1	2
490 A1	1	12
490 D1	0	1
490 G1	−2	21
492 A1	3	2
492 B1	−7	18

Curve	x	y
493 B1	40	226
494 A1	3	8
494 D1	45	224
495 A1	2	2
496 A1	0	1
496 E1	2	1
496 F1	7	14
497 A1	2	6
498 B1	−1	6
503 A1	7	4
504 A1	0	3
504 E1	2	1
504 F1	6	5
505 A1	6	9
506 A1	−4	2
506 D1	17	−3
506 E1	−1	1
506 F1	4	2
507 A1	70	472
507 B1	2	0
507 C1	$94/3^2$	$913/3^3$
510 D1	3	4
513 A1	8	−3
513 B1	2	−3
514 A1	−7	6
514 B1	2	0
516 B1	7	−18
517 C1	$85/2^2$	$513/2^3$
520 A1	−1	8
522 A1	7	10
522 E1	−1	14
522 F1	6	13
522 I1	1	2
522 J1	11	−24
524 A1	10	1
525 A1	6	3
525 C1	14	1
525 D1	3	0
528 A1	−2	2
528 G1	−6	2
528 H1	−2	24
530 B1	−1	2
530 C1	156	1922
530 D1	1	4
534 A1	3	−5
539 C1	123	1310
539 D1	9	−25
540 B1	0	1

Curve	x	y
540 C1	16	10
540 D1	1	1
542 B1	1	1
544 A1	0	2
545 A1	6	17
546 C1	-4	3
549 A1	4	6
549 B1	2	4
550 A1	5	10
550 F1	52	286
550 G1	1	1
550 I1	-35	-258
550 J1	-1	10
551 A1	7	15
551 B1	5	7
551 C1	$509/2^2$	$10465/2^3$
551 D1	9	14
552 A1	18	64
552 D1	17	5
552 E1	-1	6
556 A1	2	1
557 A1	0	1
558 A1	1	1
558 D1	9	-45
558 F1	-3	7
558 G1	9	4
560 D1	-1	10
560 E1	6	14
560 F1	5	10
561 B1	34	181
561 C1	1	1
563 A1	$\{$ 2 4	-1 4 $\}$
564 A1	-8	1
564 B1	1	6
566 A1	0	2
567 A1	4	5
567 B1	10	26
570 A1	4	-10
570 C1	-2	11
570 E1	2	3
571 B1	$\{$ 0 1	1 0 $\}$
573 C1	-1	1
574 A1	-1	1
574 B1	17	65
574 F1	-2	19
574 G1	-1	4

Curve	x	y
574 H1	1	2
574 I1	61	18
575 A1	0	1
575 B1	45	312
575 D1	-6	15
575 E1	3	-3
576 A1	1	3
576 H1	4	10
576 I1	1	9
579 B1	-1	2
580 A1	-2	1
580 B1	-2	5
582 A1	-3	3
582 C1	1	3
585 A1	8	8
585 D1	5	4
585 F1	238	3513
585 G1	-1	4
585 H1	4	2
585 I1	8	-68
586 B1	-7	19
586 C1	1	0
588 B1	5	49
588 C1	-1	1
590 C1	1	2
590 D1	10	-10
591 A1	0	1
592 A1	-2	1
592 D1	-1	2
592 E1	-4	1
593 A1	1	0
594 A1	0	6
594 D1	18	79
598 A1	1	19
598 B1	-5	14
598 D1	21	-103
600 A1	11	3
600 B1	1	2
600 E1	43	270
603 E1	6	6
603 F1	5	4
605 A1	212	2919
605 B1	$84/5^2$	$563/5^3$
605 C1	6	9
606 B1	0	1
606 E1	0	24
608 A1	4	4
608 D1	0	4

Curve	x	y
608 E1	128	1444
608 F1	1	2
609 A1	$-1/2^2$	$15/2^3$
609 B1	$211/2^2$	$2529/2^3$
610 B1	7	-1
612 B1	8	6
612 C1	-4	18
614 A1	5	-2
614 B1	0	1
615 A1	-2	2
615 B1	22	112
616 A1	10	44
616 D1	29	154
616 E1	6	3
618 A1	0	2
618 B1	61	-1
618 C1	$11/2^2$	$-9/2^3$
618 D1	15	28
618 E1	-1	2
618 F1	10	19
620 A1	2	13
620 B1	18	5
620 C1	0	2
621 B1	-2	1
622 A1	1	1
623 A1	12	43
624 A1	2	2
624 B1	6	14
624 F1	12	36
624 G1	0	2
626 A1	1	1
629 A1	2	2
629 C1	-6	8
629 D1	16	47
630 D1	12	50
630 E1	2	9
632 A1	0	4
633 A1	12	34
635 A1	$-3/2^2$	$9/2^3$
635 B1	2	0
637 A1	6	-2
637 C1	$4776/7^2$	$158761/7^3$
637 D1	7	24
639 A1	6	10
640 A1	$17/2^2$	$15/2^3$
640 B1	-2	6
640 G1	0	2
640 H1	0	5

Curve	x	y
642 C1	15	64
643 A1	1 2	0 1
644 A1	13	49
644 B1	4	7
645 E1	51	607
645 F1	1	7
646 D1	9	11
648 A1	-1	4
648 B1	-1	1
648 D1	-3	9
649 A1	3	4
650 A1	-2	9
650 B1	84	726
650 C1	5	4
650 G1	3	-1
650 K1	25	117
651 C1	$11/2^2$	$27/2^3$
651 D1	$15/2^2$	$69/2^3$
654 A1	17	45
654 B1	-3	37
655 A1	1 3	2 2
656 A1	3	2
657 C1	2	4
657 D1	4	2
658 D1	5	13
658 E1	5	165
658 F1	3	-1
659 A1	$-50/3^2$	$76/3^3$
660 B1	1	3
660 C1	-3	15
662 A1	25	115
663 B1	$51/2^2$	$-43/2^3$
663 C1	-3	3
664 A1	2 1	2 2
664 B1	-1	1
664 C1	1	1
665 A1	4	22
665 B1	$-119/8^2$	$527/8^3$
665 C1	0	1
665 D1	-18	66
666 C1	3	12
666 D1	5	3
666 E1	27	130
669 A1	2	2
670 A1	31	47

Curve	x	y
670 B1	$-5/2^2$	$11/2^3$
670 C1	3	0
670 D1	8	12
672 A1	0	2
672 B1	0	42
672 E1	-1	6
672 F1	6	12
674 A1	0	0
674 B1	3	1
674 C1	157	1969
675 A1	5	12
675 B1	0	1
675 I1	-6	28
677 A1	0	0
678 A1	2	0
678 B1	5	9
678 C1	29	129
680 A1	6	4
681 A1	4	4
681 C1	-1 0	0 1
681 E1	7	4
682 A1	-6	11
682 B1	15	36
684 A1	4	18
684 B1	10	27
685 A1	2	0
688 A1	1	1
688 C1	4	3
689 A1	3	1
690 A1	11	32
690 E1	-14	11
690 H1	-1	5
693 B1	1	3
696 A1	6	1
696 C1	0	3
696 F1	12	29
696 G1	2	3
700 C1	1	1
700 D1	180	2450
700 E1	-26	7
700 F1	0	25
700 G1	0	10
702 A1	5	4
702 B1	-1	1
702 H1	$7/2^2$	$151/2^3$
702 K1	-1	12
702 L1	25	104

Curve	x	y
702 M1	-29	86
703 B1	7	18
704 A1	0	1
704 B1	0	1
704 J1	2	1
704 K1	2	1
704 L1	5	11
705 A1	120	1093
705 B1	312	5366
705 D1	1	2
705 E1	3	-3
706 A1	1	1
706 B1	41	-277
706 C1	7	12
706 D1	0	2
707 A1	3 0	3 3
709 A1	0 -1	0 0
710 A1	-3	4
710 B1	-11	85
710 C1	3	3
711 A1	2	2
711 B1	4	-16
713 A1	-1	1
714 A1	13	196
714 D1	2	3
714 F1	-1	10
715 A1	-2	3
715 B1	87	812
718 B1	0 -1	0 2
718 C1	13	-5
720 A1	1	4
720 E1	5	16
720 G1	7	-30
720 H1	-1	18
722 A1	$27444/13^2$	$4423160/13^3$
722 B1	5	-12
722 E1	93	314
722 F1	-1	1
723 A1	2	0
723 B1	2	1
725 A1	8	8
726 A1	-2	5
726 D1	3	1
726 E1	-34	198
726 G1	17	-108

Curve	x	y
728 C1	12	26
728 D1	5	14
730 F1	17	−1
730 G1	−1	1
730 I1	1	3
730 J1	−7	−22
731 A1	13	−5
732 B1	10	18
732 C1	1	−3
735 C1	0	2
735 E1	13	40
735 F1	−19	−53
737 A1	106	1105
738 A1	1	13
738 D1	41	101
738 E1	3	−8
738 F1	−7	75
740 B1	−3	10
740 C1	−5	10
741 E1	7	19
742 A1	3	2
742 E1	277	−4034
742 G1	9	23
744 A1	2	−3
744 C1	8	27
744 F1	44	279
744 G1	6	3
747 A1	−4	5
747 C1	26	−4
747 D1	0	2
747 E1	2	3
749 A1	3	2
752 A1	−1	6
753 C1	−1	1
754 B1	60	−16
754 C1	−2	1
754 D1	14	51
755 A1	1	1
755 B1	1	1
756 B1	−3	1
756 C1	−4	2
758 A1	3	−10
759 A1	10	11
759 B1	7	16
760 D1	1	5
760 E1	6	15
762 C1	−2	2
762 D1	1	2
762 E1	6	−15

Curve	x	y
763 A1	−2	3
765 C1	−4	24
768 A1	2	3
768 B1	1	2
768 G1	0	3
768 H1	3	6
770 D1	4	25
770 E1	19	64
770 F1	6	52
774 D1	66	−609
774 E1	−3	−3
774 F1	9	−2
774 G1	−1	9
775 A1	−2	12
776 A1	1	6
777 D1	4	5
777 E1	43	50
777 F1	0	1
777 G1	−6	10
780 A1	5	5
780 C1	−3	−15
781 B1	14	16
782 A1	0	2
784 A1	−3	1
784 B1	0	49
784 H1	1	8
784 I1	−1	1
784 J1	−12	98
786 A1	1	0
786 B1	10	−1
786 C1	12085	1322560
786 G1	−6	4
786 H1	−3	−8
786 J1	−9	−124
786 K1	3	7
786 L1	0	6
790 A1	2	3
791 C1	68	522
792 A1	−5	8
792 C1	1	2
792 D1	5	2
793 A1	$82/3^2$	$497/3^3$
794 A1	$\left\{\begin{matrix}0\\1\end{matrix}\right.$	$\left.\begin{matrix}1\\0\end{matrix}\right\}$
794 B1	−8	15
794 C1	1	1
794 D1	6	3
795 A1	−2	5
797 A1	0	1

Curve	x	y
798 A1	0	2
798 C1	3	7
798 D1	−4	12
798 G1	−9	23
798 H1	8	−67
799 B1	−2	26
800 A1	−4	6
800 B1	2	2
800 C1	−8	2
800 H1	−1	2
800 I1	−8	50
801 C1	8	13
801 D1	6	8
804 B1	71	−486
804 C1	2	2
804 D1	12	54
805 A1	$181/2^2$	$15015/2^3$
806 A1	6	12
806 B1	5	13
806 C1	12	25
806 D1	137	1543
810 D1	4	4
810 H1	5	7
811 A1	2	1
812 B1	−6	14
813 B1	2	7
814 A1	−2	4
814 B1	3	−3
815 A1	3	3
816 A1	0	12
816 G1	1	−2
816 H1	−14	18
816 I1	−1	162
816 J1	−4	6
817 A1	$\left\{\begin{matrix}4\\2\end{matrix}\right.$	$\left.\begin{matrix}9\\4\end{matrix}\right\}$
817 B1	−2	924
819 A1	14	37
819 B1	2	−1
822 A1	3	3
822 D1	3	−14
825 A1	1	5
825 B1	−7	5
825 C1	14	16
827 A1	2	0
828 B1	−8	1
828 C1	4	1
829 A1	−1	0
830 B1	63	48

Curve	x	y
830 C1	7	16
831 A1	13	−47
832 A1	3	8
832 B1	5	8
832 C1	9	32
832 H1	1	3
832 I1	−1	16
832 J1	42	256
834 C1	−1	3
834 E1	1	1
834 F1	35	126
834 G1	2	14
836 A1	8	19
840 A1	54	368
840 E1	1	3
840 F1	17	51
840 H1	−5	3
842 A1	−2	1
842 B1	−2	−15
843 A1	0	2
846 B1	1	4
846 C1	−1	41
847 B1	55	423
847 C1	116	1212
848 F1	3	4
848 G1	6	32
849 A1	2	−6
850 C1	2	61
850 D1	21	567
850 E1	4	−12
850 K1	25	112
850 L1	5	7
851 A1	6	11
854 A1	13	9
854 B1	−15	309
854 C1	−1	4
854 D1	−19	−40
855 B1	2	21
856 A1	1	1
856 B1	4	8
856 C1	4	2
856 D1	137	1578
858 B1	−2	35
858 F1	−9	355
858 G1	5	3
861 B1	45	220
861 C1	−5	64
861 D1	−1	5
862 A1	1	0

Curve	x	y
862 B1	4	2
862 E1	−11	273
862 F1	1	3
864 A1	1	2
864 B1	4	4
864 C1	4	−12
864 J1	9	18
864 K1	0	4
864 L1	0	36
866 A1	4	8
867 A1	57	433
867 B1	0	4
867 C1	$301/6^2$	$4805/6^3$
869 A1	9	6
869 B1	11	39
869 D1	−4	81
870 A1	2	9
870 B1	−14	311
870 C1	0	7
870 E1	−1	2
870 F1	17	41
872 A1	0	4
873 B1	$275/2^2$	$3289/2^3$
873 C1	$227473/16^2$	$106817593/16^3$
873 D1	1	4
874 C1	3	−1
874 D1	−2	2
874 E1	−3	47
876 A1	128	1
876 B1	5	−6
880 A1	3	6
880 C1	103	660
880 D1	−3	−20
880 F1	8	16
880 G1	26	160
880 H1	−2	2
882 A1	39	−15
882 D1	3	3
882 E1	9	−225
882 G1	−1	6
882 H1	51	352
885 B1	58	411
885 C1	−2	1
885 D1	1	37
886 A1	2	0
886 B1	20	−10
886 D1	281	−77
886 E1	1	1
888 B1	−6	6

Curve	x	y
888 C1	5	7
890 A1	0	1
890 B1	−1	2
890 D1	2	−1
890 E1	−20	12
890 F1	5	−19
890 G1	−5	3
891 A1	2	−7
892 B1	−16	10
892 C1	−2	2
894 A1	81	0
894 B1	−5	3
894 D1	−2	2
894 E1	33	127
894 F1	3	−1
894 G1	2	17
895 A1	1	0
896 A1	6	12
896 B1	−2	2
896 D1	3	3
897 C1	6	7
897 D1	2987	−165762
897 E1	63	261
897 F1	3	3
898 A1	8	−4
898 D1	−1	1
899 A1	−1	1
900 C1	−4	6
900 D1	16	54
900 E1	−10	25
901 A1	−4	8
901 B1	90	106
901 E1	$-23/2^2$	$897/2^3$
901 F1	−1	0
902 A1	5	253
903 A1	4	10
904 A1	2	4
905 A1	$-1/2^2$	$43/2^3$
906 A1	$394/3^2$	$3505/3^3$
906 B1	−3	2
906 C1	−1	3
906 D1	12	85
906 G1	−3	2
906 H1	−8	−32
909 C1	−1	4
910 B1	6	14
910 C1	−5	51
910 D1	−3	4
910 F1	137	295

Curve	x	y
910 G1	5	−8
910 H1	9	−75
910 K1	10	35
912 A1	12	27
912 F1	36	243
912 G1	2	2
912 H1	20	18
912 I1	3	−6
914 A1	−1	2
915 B1	0	12
915 D1	−1	8
916 C1	0 −1	1 2
916 D1	8	14
916 E1	−1	1
918 A1	92	−38
918 B1	9	21
918 C1	53	285
918 E1	1	0
918 F1	4	12
918 H1	5	3
918 I1	5	14
918 J1	17	127
920 A1	302	5290
920 B1	7	−5
920 C1	2	5
920 D1	4	5
921 B1	−5	7
924 B1	24	121
924 C1	3	7
924 E1	2	3
924 H1	89	−231
925 A1	3	12
925 B1	2	12
927 A1	12	21
928 A1	3	4
928 B1	1	4
930 A1	−7	10
930 D1	−13	394
930 E1	0	3
930 H1	19	−130
930 M1	1	8
933 A1	−1	0
933 B1	−12	4
934 A1	0	0
935 A1	2	2
936 A1	2	6
936 E1	−4	9
936 G1	2	9

Curve	x	y
936 H1	−2	9
938 A1	−1	1
938 B1	3	110
938 C1	−5	−5
939 A1	29	66
939 B1	11	30
939 C1	1	4
940 C1	44	46
940 D1	2	2
942 C1	−28	122
942 D1	4	−5
944 A1	2	4
944 B1	10	4
944 C1	2	4
944 E1	3 1	2 −4
944 H1	66	512
944 I1	6	−16
944 J1	4	2
944 K1	2	8
946 B1	5	11
950 A1	2	11
950 E1	15	17
954 A1	13	7
954 D1	11	35
954 E1	166	1965
954 F1	3	3
954 H1	−1	6
954 I1	11	−15
954 J1	11	102
960 A1	3	6
960 B1	1	12
960 H1	21	30
960 K1	7	14
960 L1	11	24
960 M1	1	6
966 A1	11	98
966 C1	−121	992
966 D1	2	−8
966 E1	−2	11
966 G1	1	35
968 A1	7	22
968 D1	3	4
968 E1	44	242
972 C1	−2	1
972 D1	−3	3
973 B1	$74/5^2$	$2682/5^3$
974 E1	1	0
974 F1	3	6

Curve	x	y
974 G1	1	0
974 H1	−1	−8
975 A1	26	23
975 B1	7	12
975 F1	−8	62
975 H1	13	32
975 I1	273	4387
975 J1	3	7
975 K1	−3	9
976 C1	2	2
978 E1	0	1
978 F1	−1	24
978 G1	−6	−24
979 B1	1514	57983
980 C1	2	7
980 D1	−9	98
981 A1	0	9
981 B1	4	2
982 A1	5	5
984 C1	−13	82
984 D1	1	6
985 B1	1	2
986 B1	126	481
986 C1	−1	44
986 D1	6	14
986 E1	80	801
986 F1	−1	4
987 E1	−3	72
988 B1	18309	2476099
988 C1	8	26
990 A1	0	5
990 E1	15	51
990 H3	−35	97
990 J1	3	18
994 A1	−1	2
994 D1	65	503
994 F1	−1	1
994 G1	−16	42
995 B1	7	17
996 B1	20	54
996 C1	3	6
997 A1	3	0
997 B1	−1 5	0 8
997 C1	3 1	0 −6
999 A1	32	156
999 B1	2	−1