テータ関数を用いた超特別$(2,2)$-同種写像グラフ計算

Computation of the superspecial $(2,2)$-isogeny graph using theta functions

東京大学大学院情報理工学系研究科　　大橋 亮 [*1]
Ryo Ohashi
Graduate School of Information Science and Technology, The University of Tokyo

東京大学大学院情報理工学系研究科　　小貫 啓史
Hiroshi Onuki
Graduate School of Information Science and Technology, The University of Tokyo

福岡工業大学　　工藤 桃成
Momonari Kudo
Fukuoka Institute of Technology

九州大学マス・フォア・イノベーション連係学府　　吉住 崚
Ryo Yoshizumi
Joint Graduate Program of Mathematics for Innovation, Kyushu University

九州大学マス・フォア・インダストリ研究所 / 産業技術総合研究所　　縫田 光司
Koji Nuida
Joint Graduate Program of Mathematics for Innovation, Kyushu University / AIST

Abstract

It is known that the $(2,2)$-isogeny graph of superspecial abelian surfaces in characteristics $p \geq 5$ can be computed by using the *Richelot correspondence*. In this report, we propose another algorithm for computing this graph by using the *theta functions*. Our algorithm seems to be slightly faster than conventional algorithms, and is useful in computing the $(2,2,2)$-isogeny graph of superspecial abelian threefolds (see [21] for details).

1　はじめに

超特別アーベル曲面間の (ℓ,ℓ)-同種写像グラフは, 数論や代数幾何学における重要な研究対象であり, また暗号学的ハッシュ関数の構成に利用される (e.g. [4], [3]) 等の応用もある. 特に $\ell = 2$ ならば Richelot 対応を用いてこのグラフは計算でき, その構造は高島 [22] や Florit-Smith [10] により理論的な解析が行われている.

本稿では, テータ関数を用いて超特別アーベル曲面間の $(2,2)$-同種写像グラフを計算するアルゴリズムを紹介する. これは [21, Remark 3.16] において, 超特別 3 次元アーベル多様体間の $(2,2,2)$-同種写像グラフを計算するためのサブルーチンとして利用されるが, 紙面の都合により詳細を省略したものである. 第 3 章でその方法を明示的に与えることとし, また全ての計算が素体の二次拡大体上で実行できることの証明も行う. また第 4 章でこのアルゴリズムを Magma で実装して, 既存の方法と比較する実験を行う. この実験結果はテータ関数を用いた方法がより効率的であることを示唆している.

[*1] E-mail: ryo-ohashi@g.ecc.u-tokyo.ac.jp

謝辞　本研究は, 総務省の「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」 の成果の一部である. また, 本研究では九州大学マス・フォア・イノベーション卓越大学院プログラムの支援および科研費「計算代数幾何手法による超特異曲線とそのモジュライ空間の研究と暗号応用への展開 (23K12949)」の助成を受けた.

2　アーベル曲面とテータ関数

この節では主に, 複素数体上で定義されたアーベル曲面とその間の $(2,2)$-同種写像がテータ関数を用いてどのように計算できるのかを復習する.

2.1　楕円曲線に付随するテータ関数

体 K 上で定義された種数 1 の非特異射影曲線 E と, その上の 1 点 $O \in E$ の組を K 上の**楕円曲線**という. 体 K の標数が 2 でなければ, そのような曲線はルジャンドル形式

$$E : y^2 = x(x-1)(x-t), \quad t \in \overline{K},\ t \neq 0, 1 \tag{2.1}$$

と, 無限遠点 $O \in E$ の組として表される. よく知られているように, 楕円曲線 E 上の点全体の集合 $E(\overline{K})$ は点 O を単位元として可換群をなす. 以降では, 特に $K = \mathbb{C}$ の場合を考える.

定義 1 (次元 1 のテータ関数)
指標 $a, b \in \{0, 1/2\}$ に対応するテータ関数を, 点 $z \in \mathbb{C}$ および $\tau \in \mathbb{H}$ に対して

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau) \coloneqq \sum_{n \in \mathbb{Z}} \exp\bigl(\pi i (n+a)^2 \tau + 2\pi i (n+a)(z+b)\bigr)$$

と定義する.

ここで (2.1) で与えられた $\mathbb{C}$ 上の楕円曲線に対して, ある $\tau \in \mathbb{H}$ が定める複素トーラスへの同型写像

$$\begin{array}{ccc} E & \xrightarrow{\ \cong\ } & \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \\ (0,0),\ (1,0),\ (t,0) & \longmapsto & 1/2,\ \tau/2,\ (1+\tau)/2 \end{array}$$

が存在する. このとき斉次座標

$$[\theta_0^2 : \theta_1^2 : \theta_2^2 : \theta_3^2] \coloneqq \left[\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\tau)^2 : \theta\left[\begin{smallmatrix} 0 \\ 1/2 \end{smallmatrix}\right](0,\tau)^2 : \theta\left[\begin{smallmatrix} 1/2 \\ 0 \end{smallmatrix}\right](0,\tau)^2 : \theta\left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right](0,\tau)^2\right] \in \mathbb{P}^3$$

を, 楕円曲線 E に付随するテータ零点とよぶことにする.

命題 2
上の状況において, 楕円曲線 E のテータ零点は $\left[1 : \sqrt{t} : \sqrt{1-t} : 0\right] \in \mathbb{P}^3$ で与えられる.

証明　トマエの公式 (cf. [19, Theorem 8.1]) を $g = 1$ の場合に適用して得られる. ∎

2.2　アーベル曲面と同種写像

簡単に言えば, アーベル曲面とは楕円曲線の 2 次元版にあたる.

定義 3 (アーベル曲面)
体 K 上の滑らかな射影代数多様体であって, 次元 2 でかつ群構造をもつものを K 上の**アーベル曲面**という. アーベル曲面 A の単位元を 0_A と書くとき, 自然数 ℓ に対して

$$A[\ell] \coloneqq \{P \in A \mid \ell P = 0_A\}$$

を A の ℓ-**ねじれ部分群**という.

任意のアーベル曲面 A は, 次のいずれかに同型である:

- ある種数 2 曲線 C の**ヤコビ多様体** (i.e. 次数 0 の因子類がなす可換群).
- ある楕円曲線 E_1, E_2 の直積.

特に前者である場合, アーベル曲面 A は**単純**であるという.

定義 4 (同種写像)
アーベル曲面間の全射準同型 $\phi : A \to B$ であって, その核が $A[\ell]$ の極大 ℓ-等方部分群であるようなものはアーベル曲面間の (ℓ,ℓ)-**同種写像**とよばれる. ここで, 核が等しい (ℓ,ℓ)-同種写像 $\phi, \phi' : A \to B$ は像 B での自己同型の差を除いて一致するため, これらを同一視する.

以降では A を複素数体 $\mathbb{C}$ 上で定義されたアーベル曲面とする. すると, ジーゲル上半平面

$$\mathcal{H}_2 \coloneqq \{\Omega \in \mathrm{Mat}_2(\mathbb{C}) \mid {}^t\Omega = \Omega,\ \mathrm{Im}\,\Omega > 0\}$$

に属するある行列 Ω により A は $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2)$ と同型になり, このような $\Omega \in \mathcal{H}_2$ はアーベル曲面 A の**周期行列**とよばれる. 一般に異なる行列 $\Omega \neq \Omega' \in \mathcal{H}_2$ であっても, それらを周期行列にもつアーベル曲面が同型になる場合があることに注意せよ.

定義 5 (シンプレクティック行列)
集合

$$\mathrm{Sp}_4(\mathbb{Z}) \coloneqq \left\{ M \in \mathrm{GL}_4(\mathbb{Z}) \;\middle|\; M\begin{pmatrix} 0 & \mathbf{1}_2 \\ -\mathbf{1}_2 & 0 \end{pmatrix} {}^tM = \begin{pmatrix} 0 & \mathbf{1}_2 \\ -\mathbf{1}_2 & 0 \end{pmatrix} \right\}$$

は群をなし, この元を 4 次**シンプレクティック行列**という.

補題 6 ([17, Lemma 8.2.1])
正方行列 $\alpha, \beta, \gamma, \delta \in \mathrm{Mat}_2(\mathbb{Z})$ に対して $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_4(\mathbb{Z})$ を仮定すると, 次の 3 条件は同値である:

(i) 行列 M は 4 次シンプレクティック行列である.
(ii) 行列 $\alpha\,{}^t\beta$, $\gamma\,{}^t\delta$ はともに対称であり, かつ $\alpha\,{}^t\delta - \beta\,{}^t\gamma = \mathbf{1}_2$ を満たす.
(iii) 行列 ${}^t\alpha\gamma$, ${}^t\beta\,\delta$ はともに対称であり, かつ ${}^t\alpha\delta - {}^t\beta\gamma = \mathbf{1}_2$ を満たす.

任意のシンプレクティック行列 $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ に対して, ジーゲル上半平面 $\mathcal{H}_2$ への作用

$$\begin{aligned} \mathrm{Sp}_4(\mathbb{Z}) \times \mathcal{H}_2 &\longrightarrow \mathcal{H}_2 \\ (M, \Omega) &\longmapsto (\alpha\Omega + \beta)(\gamma\Omega + \delta)^{-1} =: M.\Omega \end{aligned}$$

が矛盾なく定まり, 写像

$$\mathbb{C}^2 \longrightarrow \mathbb{C}^2\,;\, z \longmapsto {}^t(\gamma\Omega + \delta)^{-1} z =: M.z$$

は同型 $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2) \cong \mathbb{C}^2/(\mathbb{Z}^2 + M.\Omega\mathbb{Z}^2)$ を誘導する. 逆に, 同型なアーベル曲面を定義する周期行列は, あるシンプレクティック行列の作用により移り合うことが知られている.

定理 7 ([17, Theorem 8.3.1])
ジーゲル上半平面の行列 $\Omega, \Omega' \in \mathcal{H}_2$ に対して, 次の 2 条件は同値である:

(i) アーベル曲面間の同型 $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2) \cong \mathbb{C}^2/(\mathbb{Z}^2 + \Omega'\mathbb{Z}^2)$ が成立する.
(ii) あるシンプレクティック行列 $M \in \mathrm{Sp}_4(\mathbb{Z})$ が存在して $\Omega' = M.\Omega$ を満たす.

2.3 アーベル曲面に付随するテータ関数

ジーゲル上半平面の行列 $\Omega \in \mathcal{H}_2$ に対して, 次元 1 の場合と同様に次のような関数を考える.

定義 8 (次元 2 のテータ関数)
指標 $a, b \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ に対応するテータ関数を, 点 $z \in \mathbb{C}^2$ および $\Omega \in \mathcal{H}_2$ に対して

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) \coloneqq \sum_{n \in \mathbb{Z}^2} \exp\bigl(\pi i\,{}^t(n+a)\,\Omega\,(n+a) + 2\pi i\,{}^t(n+a)(z+b)\bigr)$$

と定義する.

もし $\Omega \in \mathcal{H}_2$ が対角行列

$$\Omega = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}, \quad \tau_1, \tau_2 \in \mathbb{H} \tag{2.2}$$

で与えられる場合は, これに付随するテータ関数を次の公式を用いて計算できる:

補題 9 ([7, Lemma F.3.1])
上の状況において, 任意の $z=(z_1,z_2)\in\mathbb{C}^2$ に対して

$$\theta\left[\begin{smallmatrix}a_1 & a_2\\ b_1 & b_2\end{smallmatrix}\right](z,\Omega)=\theta\left[\begin{smallmatrix}a_1\\ b_1\end{smallmatrix}\right](z_1,\tau_1)\theta\left[\begin{smallmatrix}a_2\\ b_2\end{smallmatrix}\right](z_2,\tau_2)$$

が成立する.

次に, 同型なアーベル曲面を与える周期行列 $\Omega,\Omega'\in\mathcal{H}_2$ に付随するテータ関数の間に成立する関係式を紹介する. そのような行列 Ω,Ω' に対しては, 定理 7 から $\Omega'=M.\Omega$ を満たす行列 $M=\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\in\mathrm{Sp}_4(\mathbb{Z})$ が存在する. このシンプレクティック行列 M の作用によって, 行列 Ω,Ω' に付随するテータ関数は次のように変化する: 各指標 $a,b\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ に対して

$$k(M,a,b):=(a\,{}^t\delta-b\,{}^t\gamma)\cdot{}^t(b\,{}^t\alpha-a\,{}^t\beta+(\alpha\,{}^t\beta)_0)-a\,{}^tb \tag{2.3}$$

および行ベクトル

$$M.a:=a\,{}^t\delta-b\,{}^t\gamma+\frac{1}{2}(\gamma\,{}^t\delta)_0,\quad M.b:=b\,{}^t\alpha-a\,{}^t\beta+\frac{1}{2}(\alpha\,{}^t\beta)_0, \tag{2.4}$$

を定義しておく. ここで, 行列 $\alpha\,{}^t\beta$, $\gamma\,{}^t\delta$ の対角成分を並べた行ベクトルをそれぞれ $(\alpha\,{}^t\beta)_0,(\gamma\,{}^t\delta)_0$ と表した. すると, 定理 10 のようにして Ω' に付随するテータ関数を計算できる.

定理 10 (Theta transformation formula)
ある定数 $c\neq0$ が存在して, 任意の指標 $a,b\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ に対して

$$\theta\left[\begin{smallmatrix}M.a\\ M.b\end{smallmatrix}\right](M.z,M.\Omega)=c\cdot e^{\pi ik(M,a,b)}\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](z,\Omega)$$

が成立する.

証明 例えば [17, Theorem 8.6.1] を参照せよ. ∎

2.4 アーベル曲面の復元アルゴリズム

この小節では $\Omega\in\mathcal{H}_2$ を固定して, それを周期行列にもつアーベル曲面 A について考える. 表記を簡単にするため, 各 $a_1,a_2,b_1,b_2\in\{0,1/2\}$ に対して

$$\vartheta_i(z):=\theta\left[\begin{smallmatrix}a_1 & a_2\\ b_1 & b_2\end{smallmatrix}\right](z,\Omega),\quad i:=2b_1+4b_2+8a_1+16a_2$$

と定める. しばしば $\vartheta_i(0)$ は単に ϑ_i と書かれ, 斉次座標 $[\vartheta_i^2]_i\in\mathbb{P}^{15}$ をアーベル曲面 A の**テータ零点**とよぶ. いま, 集合 $\{0,\dots,15\}$ を

$$I_{\mathrm{even}}:=\{0,1,2,3,4,6,8,9,12,15\},\quad I_{\mathrm{odd}}:=\{5,7,10,11,13,14\}$$

と分割する.

補題 11
もし $i\in I_{\mathrm{odd}}$ ならば $\vartheta_i(z)$ は奇関数であり, そうでなければ $\vartheta_i(z)$ は偶関数である.

証明 任意の指標 $a,b\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ に対して

$$\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](-z,\Omega)=(-1)^{4a^tb}\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](z,\Omega)$$

が成立するので, 簡単な計算により主張がしたがう. ∎

この補題 11 によって直ちに $i\in I_{\mathrm{odd}}$ ならば $\vartheta_i=0$ が成立するが, 逆は一般に成立しない. より正確には, 命題 12 で示すように A が単純である場合に限ってこの性質が成立する.

命題 12
(a) もし A が単純ならば, 任意の $i\in I_{\mathrm{even}}$ に対して $\vartheta_i\neq0$ が成立する.
(b) もし A が単純でなければ $\vartheta_i=0$ を満たす $i\in I_{\mathrm{even}}$ がただ 1 つ存在する.

証明 例えば [8, Remark 5] よりしたがう. ∎

以降では, アーベル曲面 A のテータ零点 $[\vartheta_i^2]_i \in \mathbb{P}^{15}$ が与えられた場合に A を復元する方法を紹介する. まず A が単純である場合 (i.e. 命題 12 (a) に対応) の公式を与える.

命題 13 ([11, Section 7.5])
任意の $i \in I_{\mathrm{even}}$ に対して $\vartheta_i \neq 0$ を仮定する. このとき

$$C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \qquad \lambda \coloneqq \frac{\vartheta_0^2\vartheta_2^2}{\vartheta_1^2\vartheta_3^2},\ \mu \coloneqq \frac{\vartheta_2^2\vartheta_{12}^2}{\vartheta_1^2\vartheta_{15}^2},\ \nu \coloneqq \frac{\vartheta_0^2\vartheta_{12}^2}{\vartheta_3^2\vartheta_{15}^2}$$

と定めれば $A \cong \mathrm{Jac}(C)$ が成立する.

次に, 各 $i \in I_{\mathrm{even}}$ に対して $i = 2b_1 + 4b_2 + 8a_1 + 16a_2$ を満たす $a_1, a_2, b_1, b_2 \in \{0, 1/2\}$ をとり

- もし $i \neq 15$ ならば
$$\beta_i \coloneqq \begin{pmatrix} 2b_1 & 0 \\ 0 & 2b_2 \end{pmatrix}, \quad \gamma_i \coloneqq \begin{pmatrix} 2a_1 & 0 \\ 0 & 2a_2 \end{pmatrix}.$$
- そうでなければ
$$\beta_{15} \coloneqq \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad \gamma_{15} \coloneqq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

と定義する.

補題 14
任意の $i \in I_{\mathrm{even}}$ に対して

$$T_i \coloneqq \begin{pmatrix} \mathbf{1}_2 & \beta_i \\ \gamma_i & \mathbf{1}_2 \end{pmatrix}$$

と定めれば, これらは 4 次シンプレクティック行列である. もし $\vartheta_0 = 0$ ならば $\vartheta_i(0, T_i.\Omega) = 0$ である.

証明 各 $i \in I_{\mathrm{even}}$ に対して β_i, γ_i は対称行列で $\beta_i\gamma_i = \gamma_i\beta_i = \mathbf{0}_2$ を満たすから, 補題 6 により $T_i \in \mathrm{Sp}_4(\mathbb{Z})$. また $a = b = 0$ に対して, 式 (2.4) から

$$T_i.a = (a_1, a_2), \quad T_i.b = (b_1, b_2)$$

が確かめられるので, 定理 10 より主張を得る. ∎

いま A を単純でないアーベル曲面とすれば, 命題 12 (b) よりある $j \in I_{\mathrm{even}}$ が存在して $\vartheta_j = 0$ が成立する. このとき行列 $M \coloneqq T_{15}{T_j}^{-1} \in \mathrm{Sp}_4(\mathbb{Z})$ を作用させたテータ零点は, 補題 14 より $\vartheta_{15}(0, M.\Omega) = 0$ を満たす. すると [8, §4.1] の議論から $M.\Omega$ は対角行列となり, したがって $M.\Omega = \mathrm{diag}(\tau_1, \tau_2)$ を満たす $\tau_1, \tau_2 \in \mathbb{H}$ に対して, それらに付随するテータ零点

$$\left[\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\tau_k)^2 : \theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0,\tau_k)^2 : \theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0,\tau_k)^2 : \theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](0,\tau_k)^2\right] \in \mathbb{P}^3 \tag{2.5}$$

を補題 9 を用いて計算できる. 最後に, 命題 2 より楕円曲線 $E_k \cong \mathbb{C}/(\mathbb{Z} + \tau_k\mathbb{Z})$ の定義方程式を復元すれば, 求めるアーベル曲面 $A \cong E_1 \times E_2$ が得られた. 以上をまとめた結果が, 次のアルゴリズム 15 である:

アルゴリズム 15
入力: アーベル曲面 A のテータ零点 $[\vartheta_i^2]_i \in \mathbb{P}^{15}$.
出力: アーベル曲面 A の同型類.

1. もし任意の $i \in I_{\mathrm{even}}$ に対して $\vartheta_i^2 \neq 0$ ならば, 命題 13 を用いて C を復元して $A' = \mathrm{Jac}(C)$ とする.
2. そうでない場合 $\vartheta_j^2 = 0$ を満たす $j \in I_{\mathrm{even}}$ がただ 1 つ存在する.
   2-1. 補題 14 で定義された行列 T_j に対して $M \coloneqq T_{15}{T_j}^{-1} \in \mathrm{Sp}_4(\mathbb{Z})$ とする.
   2-2. 各 $i \in \{0, \ldots, 15\}$ に対して $\vartheta_i(0, M.\Omega)^2$ の値を, 定理 10 を用いて求める.
   2-3. 補題 9 により $M.\Omega = \mathrm{diag}(\tau_1, \tau_2)$ を満たす $\tau_k \in \mathbb{H}$ に付随するテータ零点 (2.5) を計算する.
   2-4. 命題 2 を用いて楕円曲線 E_k の定義方程式を復元して $A' = E_1 \times E_2$ とする.
3. アーベル曲面 A' を出力する.

2.5 アーベル曲面間の $(2,2)$-同種写像計算アルゴリズム

任意の行列 $\Omega \in \mathcal{H}_2$ に対して

$$\begin{aligned} \mathbb{C}^2/(\mathbb{Z}^2+\Omega\mathbb{Z}^2) &\longrightarrow \mathbb{C}^2/(\mathbb{Z}^2+\ell\Omega\mathbb{Z}^2) \\ z &\longmapsto \ell z \end{aligned}$$

は (ℓ,ℓ)-同種写像であり, その核は $\frac{1}{\ell}\mathbb{Z}^2/\mathbb{Z}^2$ に一致する. したがって $\Omega, 2\Omega$ を周期行列にもつアーベル曲面は互いに $(2,2)$-同種であり, それらに対応するテータ関数は次のような関係式を満たす:

定理 16 (Duplication formula)
任意の指標 $a,b \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ に対して

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,2\Omega)^2 = \frac{1}{4}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} (-1)^{4^t a\beta}\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](z,\Omega)\theta\left[\begin{smallmatrix} 0 \\ b+\beta \end{smallmatrix}\right](z,\Omega)$$

が成立する.

証明 例えば [13, Chapter IV, Theorem 2] を $m_1 = m_2$ および $z_1 = z_2 = z$ として適用すればよい. ∎

以降では Ω を周期行列にもつアーベル曲面を A として, そのテータ零点 $[\vartheta_i^2]_i \in \mathbb{P}^{15}$ が与えられたとする. 定理 16 を用いれば, 各 $i \in \{0,\dots,15\}$ に対して $\vartheta_i(0,2\Omega)^2$ の値を計算できる. ここで右辺の値を得るために各 $\vartheta_0^2, \vartheta_1^2, \vartheta_2^2, \vartheta_3^2$ の平方根を外す必要があるが, これは [6, §5.1] の議論により任意に外して良い. したがって, 次のようなアルゴリズム 17 が得られる:

アルゴリズム 17
入力: アーベル曲面 A のテータ零点 $[\vartheta_i^2]_i \in \mathbb{P}^{15}$.
出力: アーベル曲面 A に $(2,2)$-同種なある A' のテータ零点 $[\vartheta_i'^2]_i \in \mathbb{P}^{15}$.

1. 命題 12 から $\vartheta_j^2 \neq 0$ を満たす $j \in \{0,\dots,3\}$ が存在する. そこで $[\vartheta_i^2]_i$ を正規化して $\vartheta_j^2 = 1$ にする.
2. 各 $k \in \{0,1,2,3\}\setminus\{j\}$ に対して ϑ_k^2 の平方根を任意に外すことで ϑ_k の値を求める.
3. 各 $i \in \{0,\dots,15\}$ に対して $\vartheta_i'^2 := \vartheta_i(0,2\Omega)^2$ の値を, 定理 16 を用いて求める.
4. テータ零点 $[\vartheta_i'^2]_i \in \mathbb{P}^{15}$ を出力する.

3 超特別 $(2,2)$-同種写像グラフ計算

この節を通して標数 $p \geq 5$ の体上でのアーベル曲面について考える. まず超特別 $(2,2)$-同種写像グラフを定義した後に, それを計算するアルゴリズムを与える.

3.1 超特別同種写像グラフ

楕円曲線 E に対して, その p-ねじれ部分群が自明になる (i.e. $E[p] = \{O\}$) ものを**超特異楕円曲線**とよぶ. 超特別アーベル曲面は, 超特異楕円曲線の 2 次元版と見なせる.

定義 18 (超特別アーベル曲面)
アーベル曲面 A が**超特別的**とは, ある超特異楕円曲線 E に対して (主偏極を無視して) $A \cong E^2$ が成立するときをいう. ヤコビ多様体 $\mathrm{Jac}(C)$ が超特別アーベル曲面となる種数 2 曲線 C も超特別的という.

ここで超特異楕円曲線の同型類は

$$N_{1,p} = \frac{p-1}{12} + \frac{1-\left(\frac{-1}{p}\right)}{4} + \frac{1-\left(\frac{-3}{p}\right)}{3}$$

個存在して, また $p > 5$ ならば超特別種数 2 曲線の同型類は

$$N_{2,p} = \frac{p^3+24p^2+141p-166}{2880} - \frac{1-\left(\frac{-1}{p}\right)}{32} + \frac{1-\left(\frac{-2}{p}\right)}{8} + \frac{1-\left(\frac{-3}{p}\right)}{18} + \epsilon, \quad \epsilon := \begin{cases} 4/5 & \text{if } p \equiv 4 \pmod 5, \\ 0 & \text{otherwise} \end{cases}$$

個存在することが知られている (cf. [12, Theorem 3.3]).

定義 19 (超特別同種写像グラフ)
素数 $\ell \neq p$ に対して, 次のように定義される有向グラフ $\mathcal{G}_2(\ell, p)$ を**超特別同種写像グラフ**という:

- グラフ $\mathcal{G}_2(\ell, p)$ の頂点は, 超特別アーベル曲面の同型類とする.
- グラフ $\mathcal{G}_2(\ell, p)$ の辺は, 頂点間の (ℓ, ℓ)-同種写像とする.

このグラフは $(\ell+1)(\ell^2+1)$-正則 (多重) グラフになる. また, 次の重要な事実が知られている:

定理 20 ([14, Section 7.2])
任意の素数 $\ell \neq p$ に対して, 超特別同種写像グラフ $\mathcal{G}_2(\ell, p)$ は連結である.

この小節の最後に, 同種写像グラフ $\mathcal{G}_2(\ell, p)$ の辺 $\phi_1 : A_0 \to A_1$ および $\phi_2 : A_1 \to A_2$ に対して

- もし $\ker \phi_2 = \phi_1(A_0[\ell])$ ならば, 同種写像 ϕ_2 を ϕ_1 の**双対拡大**とよぶ.
- もし $\ker \phi_2 \cap \phi_1(A_0[\ell]) = 0$ ならば, 同種写像 ϕ_2 を ϕ_1 の**良い拡大**とよぶ.
- それ以外であれば, 同種写像 ϕ_2 を ϕ_1 の**悪い拡大**とよぶ.

任意の辺 $\phi_1 : A_0 \to A_1$ に対して, その良い拡大は ℓ^3 個存在することが知られている (cf. [3, Lemma 2]).

3.2 超特別アーベル曲面のテータ零点

第 2 節では簡単のため複素数体上のテータ関数のみを定義したが, 実際には Mumford の理論 [18] により標数が 2 でない任意の体上で各種公式が成立する (アルゴリズム 15 とアルゴリズム 17 も正常に機能する). さて, この小節では, 超特別アーベル曲面間の $(2,2)$-同種写像計算は $\mathbb{F}_{p^2}$ 上で行えることを証明する.

命題 21
超特異楕円曲線のテータ零点 $[\theta_i^2] \in \mathbb{P}^3$ に対して, 比 θ_j/θ_k $(\theta_k \neq 0)$ は有限体 $\mathbb{F}_{p^2}$ の元である.

証明 任意に超特異楕円曲線 $E : y^2 = x(x-1)(x-t)$ をとれば, 命題 2 よりそのテータ零点は

$$[\theta_0^2 : \theta_1^2 : \theta_2^2 : \theta_3^2] = \left[1 : \sqrt{t} : \sqrt{1-t} : 0\right] \in \mathbb{P}^3$$

で与えられる. ここで [1, Proposition 3.1] より $t, 1-t \in \mathbb{F}_{p^2}$ は有限体 $\mathbb{F}_{p^2}$ 上の 4 乗元であり, したがって

$$\frac{\theta_1}{\theta_0} = \sqrt[4]{t}, \quad \frac{\theta_2}{\theta_0} = \sqrt[4]{1-t}, \quad \frac{\theta_3}{\theta_0} = 0$$

やこれらの商は $\mathbb{F}_{p^2}$ に属する. ∎

定理 22
超特別アーベル曲面のテータ零点 $[\vartheta_i^2] \in \mathbb{P}^{15}$ に対して, 比 ϑ_j/ϑ_k $(\vartheta_k \neq 0)$ は有限体 $\mathbb{F}_{p^2}$ の元である.

証明 任意に超特別アーベル曲面 A をとる. 以降では A が単純かそうでないかで場合分けして考える.

- アーベル曲面 A が単純でない場合, ある超特異楕円曲線 E_1, E_2 が存在して $A \cong E_1 \times E_2$ が成立する. このとき E_1, E_2 のテータ零点をそれぞれ $[\alpha_i^2], [\beta_i^2] \in \mathbb{P}^3$ とすれば, 命題 21 によりこれらの成分の比は有限体 $\mathbb{F}_{p^2}$ の元である. 補題 9 より $E_1 \times E_2$ のテータ零点 $[\vartheta_i'^2] \in \mathbb{P}^{15}$ は

$$\begin{aligned} &\vartheta'_0 = \alpha_0\beta_0, \quad \vartheta'_1 = \alpha_1\beta_0, \quad \vartheta'_2 = \alpha_0\beta_1, \quad \vartheta'_3 = \alpha_1\beta_1, \quad \vartheta'_4 = \alpha_2\beta_0, \quad \vartheta'_6 = \alpha_2\beta_1, \\ &\vartheta'_8 = \alpha_0\beta_2, \quad \vartheta'_9 = \alpha_1\beta_2, \quad \vartheta'_{12} = \alpha_2\beta_2, \quad \vartheta'_5 = \vartheta'_7 = \vartheta'_{10} = \vartheta'_{11} = \vartheta'_{13} = \vartheta'_{14} = 0 \end{aligned}$$

  として計算できて, これらの比 $\vartheta'_j/\vartheta'_k$ $(\vartheta'_k \neq 0)$ もまた $\mathbb{F}_{p^2}$ の元である. いま $A \cong E_1 \times E_2$ だったから, 定理 7 により $E_1 \times E_2$ のテータ零点 $[\vartheta_i'^2] \in \mathbb{P}^{15}$ に対してある $M \in \mathrm{Sp}_4(\mathbb{Z})$ を作用させたものが A のテータ零点 $[\vartheta_i^2] \in \mathbb{P}^{15}$ になる. 定理 10 から, ある置換 $\sigma : \{0, \ldots, 15\} \to \{0, \ldots, 15\}$ が存在して

$$\frac{\vartheta_{\sigma(j)}}{\vartheta_{\sigma(0)}} = \frac{\vartheta'_j}{\vartheta'_0} \cdot (\sqrt{-1})^k, \quad j \in \{0, \ldots, 15\}, \ k \in \{0, 1, 2, 3\}$$

  が成立する. すると $\sqrt{-1} \in \mathbb{F}_{p^2}$ に注意すれば, これらの比 ϑ_j/ϑ_k $(\vartheta_k \neq 0)$ も有限体 $\mathbb{F}_{p^2}$ の元となる.

- アーベル曲面 A が単純である場合, ある超特別的な種数 2 曲線 C が存在して $A \cong \mathrm{Jac}(C)$ が成立する. 標数 $p \geq 5$ だったから, そのような C は

$$C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \quad \#\{0, 1, \lambda, \mu, \nu\} = 5$$

と表示できて, このヤコビ多様体 $\mathrm{Jac}(C)$ のテータ零点 $[\vartheta_i'^2] \in \mathbb{P}^{15}$ が

$$\left(\frac{\vartheta_2'}{\vartheta_0'}\right)^4 = \frac{\mu(\nu-1)(\lambda-\mu)}{\nu(\mu-1)(\lambda-\nu)}, \quad \left(\frac{\vartheta_3'}{\vartheta_0'}\right)^4 = \frac{\mu}{\lambda\nu}, \quad \left(\frac{\vartheta_4'}{\vartheta_0'}\right)^4 = \frac{\mu(\nu-1)(\lambda-1)}{\lambda\nu(\mu-1)}, \quad \left(\frac{\vartheta_{12}'}{\vartheta_0'}\right)^4 = \frac{\mu(\nu-1)(\lambda-\mu)}{\nu(\mu-1)(\lambda-\nu)}$$

を満たすようにとれる (cf. [6, §7.5]). すると [20, Main Theorem A] で示した結果から, これらの元は有限体 $\mathbb{F}_{p^2}$ 上の 4 乗元である. すなわち $\vartheta_2'/\vartheta_0', \vartheta_3'/\vartheta_0', \vartheta_4'/\vartheta_0', \vartheta_{12}'/\vartheta_0'$ は $\mathbb{F}_{p^2}$ に属する. また

$$\frac{\vartheta_1'}{\vartheta_0'} = \frac{1}{\sqrt{\lambda}}\frac{\vartheta_2'}{\vartheta_3'}, \quad \frac{\vartheta_6'}{\vartheta_0'} = \sqrt{\frac{\lambda-1}{\lambda}}\frac{\vartheta_2'}{\vartheta_4'}, \quad \frac{\vartheta_8'}{\vartheta_0'} = \sqrt{\frac{\nu-1}{\nu}}\frac{\vartheta_{12}'}{\vartheta_4'}, \quad \frac{\vartheta_9'}{\vartheta_0'} = \sqrt{\frac{\nu-\lambda}{\nu\lambda}}\frac{\vartheta_2'\vartheta_{12}'}{\vartheta_3'\vartheta_4'}, \quad \frac{\vartheta_{15}'}{\vartheta_0'} = \frac{1}{\sqrt{\nu}}\frac{\vartheta_{12}'}{\vartheta_3'}$$

と表せるので, これらの比 $\vartheta_j'/\vartheta_k'$ $(\vartheta_k' \neq 0)$ はすべて $\mathbb{F}_{p^2}$ に属している. いま $A \cong \mathrm{Jac}(C)$ だったから, 前段と同様の議論によって比 ϑ_j/ϑ_k $(\vartheta_k \neq 0)$ も有限体 $\mathbb{F}_{p^2}$ の元となる. ∎

3.3 同種写像グラフ計算アルゴリズム

アルゴリズム 17 は, アーベル曲面 A のテータ零点 $[\vartheta_i^2] \in \mathbb{P}^{15}$ を入力として $(2,2)$-同種写像 $\phi : A \to B$ の像を 1 つ計算できるが, 別の $(2,2)$-同種写像 $\phi' : A \to B'$ による像を計算する場合には $[\vartheta_i^2] \in \mathbb{P}^{15}$ に適切なシンプレクティック行列 $M \in \mathrm{Sp}_4(\mathbb{Z})$ を作用させてから再度アルゴリズム 17 を実行する必要がある. そこで次のような 15 個の行列を定義する:

$$M_1 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_2 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_3 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad M_4 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

$$M_5 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad M_6 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad M_7 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad M_8 \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix},$$

$$M_9 \coloneqq \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_{10} \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad M_{11} \coloneqq \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad M_{12} \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$M_{13} \coloneqq \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad M_{14} \coloneqq \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad M_{15} \coloneqq \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

各 $j \in \{1, \ldots, 15\}$ に対して, テータ零点 $[\vartheta_i^2] \in \mathbb{P}^{15}$ に行列 M_j を作用させた後アルゴリズム 17 を実行して得られる $(2,2)$-同種写像を $\phi_j : A \to B_j$ と書けば, 次の命題が得られる:

命題 23
上の状況において, 各 ϕ_j は相異なる $(2,2)$-同種写像に対応する.

証明 各 M_j が 4 次シンプレティック行列であることは補題 6 よりしたがう. ここで, ある $M \in \mathrm{Sp}_4(\mathbb{Z})$ をテータ関数 $[\vartheta_i^2] \in \mathbb{P}^{15}$ に作用させた後アルゴリズム 17 を実行して得られる $(2,2)$-同種写像が ϕ と一致する必要十分条件は, 行列 M が $\mathrm{Sp}_4(\mathbb{Z})$ の部分群

$$\Gamma_0(2) \coloneqq \left\{ M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) \;\middle|\; \gamma \equiv \mathbf{0}_2 \pmod 2 \right\}$$

に属することである (cf. [5, §2.3.2]). したがって相異なる $(2,2)$-同種写像を得るためには $\mathrm{Sp}_4(\mathbb{Z})/\Gamma_0(2)$ の相異なる元をテータ零点 $[\vartheta_i^2] \in \mathbb{P}^{15}$ に作用させればよい. この剰余群 $\mathrm{Sp}_4(\mathbb{Z})/\Gamma_0(2)$ の位数は 15 であって, それらの代表元が $M_1, \ldots, M_{15}$ で与えられることを計算機により確認できる. ∎

超特別同種写像グラフ $\mathcal{G}_2(2,p)$ は定義 19 でも述べたように 15-正則であり, 上で定義した 15 個の行列を用いることで次のアルゴリズム 24 のように計算することができる:

アルゴリズム 24

入力: 素数 $p \geq 5$.

出力: 同種写像グラフ $\mathcal{G}_2(2,p)$ の頂点集合 $\mathcal{V}$ および辺集合 $\mathcal{E}$.

1. 標数 p での超特異楕円曲線の同型類全体の集合を $\{E_1, \ldots, E_n\}$ として, リスト $\mathcal{S} \leftarrow \emptyset$ を用意する.
   - *1-1.* リスト $\mathcal{V} \leftarrow \{E_i \times E_j \mid 1 \leq i \leq j \leq n\}$ を作成する.
   - *1-2.* リスト $\mathcal{V}$ の各要素に対して, そのテータ零点を命題 2 と補題 9 により計算して $\mathcal{S}$ に追加する.
2. リスト $\mathcal{E} \leftarrow \emptyset$ と初期化して, また $k \leftarrow 1$ とする.
3. リスト $\mathcal{S}$ の第 k 番目の要素を $[\vartheta_i^2] \in \mathbb{P}^{15}$ として, また $j \leftarrow 1$ とする.
   - *3-1.* 定理 10 より $[\vartheta_i^2] \in \mathbb{P}^{15}$ に行列 M_j を作用させて $[\vartheta_i'^2] \in \mathbb{P}^{15}$ とする.
   - *3-2.* アルゴリズム 17 に $[\vartheta_i'^2]$ を入力して得られたテータ零点を新たに $[\vartheta_i'^2] \in \mathbb{P}^{15}$ とする.
   - *3-3.* アルゴリズム 15 に $[\vartheta_i'^2]$ を入力して得られたアーベル曲面を A' とする.
   - *3-4.* もし A' が $\mathcal{V}$ のどの要素とも同型でなければ A' を $\mathcal{V}$ に追加して, また $[\vartheta_i'^2]$ を $\mathcal{S}$ に追加する.
   - *3-5.* リスト $\mathcal{V}$ の第 k' 番目が A' と同型であるとして, 組 (k,k') を $\mathcal{E}$ に追加する.
   - *3-6.* もし $j < 15$ ならば $j \leftarrow j+1$ としてステップ *3-1* に戻る.
4. もし $k < \#\mathcal{S}$ ならば $k \leftarrow k+1$ としてステップ *3* に戻る.
5. リスト $\mathcal{V}$ およびリスト $\mathcal{E}$ を出力する.

注意 25

グラフ $\mathcal{G}_2(2,p)$ 上の頂点 (= 超特別アーベル曲面) を, その**不変量**と同一視することでステップ *3-4* と *3-5* における同型判定を効率的に行うことができる. 例えば, 不変量として

- アーベル曲面 $A = E_1 \times E_2$ が単純でない場合は, 楕円曲線 E_1, E_2 それぞれの j-不変量の集合.
- アーベル曲面 $A = \mathrm{Jac}(C)$ が単純である場合は, 種数 2 曲線 C の井草不変量.

を採用することができる.

3.4 計算機による実験

アルゴリズム 24 を計算代数システム Magma [2] により実装の上で, 既存の方法 (cf. [9, Appendix B]) と実行時間を比較する. 実験は Intel Xeon Gold 6130 CPU で, メモリが 768GB 搭載の計算機上で実行した.

標数	既存	今回	標数	既存	今回	標数	既存	今回	標数	既存	今回
5	0.36	0.02	43	1.70	1.04	97	13.97	8.88	151	56.62	36.40
7	0.40	0.32	47	2.19	1.33	101	16.76	10.01	157	61.98	41.32
11	0.16	0.11	53	2.93	1.78	103	17.60	10.85	163	68.24	42.24
13	0.12	0.11	59	3.91	2.39	107	20.08	12.16	167	77.12	43.53
17	0.21	0.16	61	4.18	2.51	109	19.41	12.49	173	89.22	46.54
19	0.27	0.17	67	5.39	3.26	113	22.53	13.93	179	97.27	51.65
23	0.42	0.26	71	6.21	3.90	127	32.15	19.35	181	102.30	53.38
29	0.71	0.42	73	6.89	4.07	131	36.33	21.24	191	122.32	62.49
31	0.76	0.47	79	7.93	5.12	137	39.71	23.53	193	129.74	64.11
37	1.18	0.69	83	7.34	5.88	139	41.39	24.88	197	134.90	68.22
41	1.54	0.93	89	11.85	7.10	149	54.02	33.03	199	159.59	70.06

表: グラフ $\mathcal{G}_2(2,p)$ の計算に要した時間

また, 今回の方法を用いてグラフ $\mathcal{G}_2(2,997)$ の計算は 9556.86 秒で完了した (頂点数は 355925 個).

4 超特別種数 2 曲線リストアップへの応用

第 3.1 節で述べたように, 超特別種数 2 曲線の同型類は $N_{2,p}$ 個存在する. この節では, それらの具体的な定義方程式を求めるアルゴリズムを提示する. ここで, グラフ $\mathcal{G}_2(2,p)$ の連結性よりも強い主張を紹介する.

定理 26 ([9, Theorem 7.2])
超特別同種写像グラフ $\mathcal{G}_2(2,p)$ の部分グラフ $\mathcal{J}_2(2,p)$ を次のように定義する:

- グラフ $\mathcal{J}_2(2,p)$ の頂点は, 超特別種数 2 曲線のヤコビ多様体の同型類とする.
- グラフ $\mathcal{J}_2(2,p)$ の辺は, 頂点間の $(2,2)$-同種写像とする.

このとき, グラフ $\mathcal{J}_2(2,p)$ は連結である.

種数 2 超特別曲線をリストアップする上では $\mathcal{G}_2(p)$ の部分グラフ $\mathcal{J}_2(p)$ を探索すれば十分である. そこでアルゴリズム 24 を少し変形して, 次のようなアルゴリズム 27 を得る (これは [16, Algorithm 5.1] の改良と見なすことがができる).

アルゴリズム 27
入力: 素数 $p \geq 5$.
出力: 標数 p での超特別種数 2 曲線の同型類全体の集合 $\mathcal{L}$.

1. 標数 p での超特異楕円曲線 E を適当に 1 つ生成して, リスト $\mathcal{S} \leftarrow \emptyset$ を用意する.
   1-1. 積 $E \times E$ のテータ零点を命題 2 と補題 9 により計算して $\mathcal{S}$ に追加する.
2. リスト $\mathcal{L} \leftarrow \emptyset$ と初期化して, また $k \leftarrow 1$ とする.
3. リスト $\mathcal{S}$ の第 k 番目の要素を $[\vartheta_i^2] \in \mathbb{P}^{15}$ として, また $j \leftarrow 1$ とする.
   3-1. 定理 10 より $[\vartheta_i^2] \in \mathbb{P}^{15}$ に行列 M_j を作用させて $[\vartheta_i'^2] \in \mathbb{P}^{15}$ とする.
   3-2. アルゴリズム 17 に $[\vartheta_i'^2]$ を入力して得られたテータ零点を新たに $[\vartheta_i'^2] \in \mathbb{P}^{15}$ とする.
   3-3. アルゴリズム 15 に $[\vartheta_i'^2]$ を入力して得られたアーベル曲面を A' とする.
   3.4. もし A' が単純でなければ, ステップ *3-6* に飛ぶ. そうでなければ $A' = \mathrm{Jac}(C')$ とする.
   3-5. もし C' が $\mathcal{L}$ のどの要素とも同型でなければ C' を $\mathcal{L}$ に追加して, また $[\vartheta_i'^2]$ を $\mathcal{S}$ に追加する.
   3-6. もし $j < 14$ ならば $j \leftarrow j+1$ としてステップ *3-1* に戻る.
4. リスト $\mathcal{L}$ の要素数が $N_{2,p}$ 未満ならば $\mathcal{L}$ を出力, そうでなければ $k \leftarrow k+1$ としてステップ *3* に戻る.

注意 28
ここでは証明を省略するが, 行列 $M_1, \ldots, M_8$ は良い拡大に, 行列 $M_9, \ldots, M_{14}$ は悪い拡大に, 行列 M_{15} は双対拡大に対応している. したがって, アルゴリズム 27 で行列 M_{15} は無駄なグラフ探索を引き起こすため, ステップ *3-6* では $j = 15$ を排除している.

5 おわりに

本稿では超特別同種写像グラフ $\mathcal{G}_2(2,p)$ をテータ関数により計算するアルゴリズム (アルゴリズム 24) を紹介して, これが Richelot 対応を用いる既存の方法と比較して効率的なことを計算機実験により確認した. また第 4 節では, 種数 2 超特別曲線を効率的にリストアップするアルゴリズム (アルゴリズム 27) も与えた. これらを計算代数システム Magma [2] で実装したコードは

`https://github.com/Ryo-Ohashi/richelot_graph`

から利用可能である. 今後の展望としては, アルゴリズム 27 で良い拡大のみを利用することでより効率的な超特別種数 2 曲線のリストアップが行えないかを検討していきたい.

参 考 文 献

[1] R. Auer and J. Top: *Legendre elliptic curves over finite fields*, J. Number Theory **95**, 303–312, 2002.

[2] W. Bosma, J. J. Cannon, C. Fieker and A. Steel: *Handbook of Magma functions*, Version 2.27, 2024.

[3] W. Castryck and T. Decru: *Multiradical isogenies*, preprint, `https://ia.cr/2021/1133`.

[4] W. Castryck, T. Decru and B. Smith: *Hash functions from superspecial genus-2 curves using Richelot isogenies*, J. Math. Cryptol. **14**, 268–292, 2020.

[5] R. Cosset: *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*, Thesis (Ph.D.)-Université Henri Poincaré, 2011.

[6] R. Cosset and D. Robert: *Computing (ℓ,ℓ)-isogneies in polynomial time on Jacobians of genus 2 curves*, Math. Comput. **84**, 1953–1975, 2014.

[7] P. Dartois, A. Leroux, D. Robert and B. Wesolowski: *SQISignHD: New dimensions in cryptography*, preprint, `https://ia.cr/2023/436`.

[8] P. Dartois, L. Maino, G. Pope and D. Robert: *An algorithmic approach to $(2,2)$-isogenies in the theta model and applications to isogeny-based cryptography*, preprint, `https://ia.cr/2023/1747`.

[9] E. Florit and B. Smith: *Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph*, Contemp. Math. **779**, 103-132, 2022.

[10] E. Florit and B. Smith: *An atlas of the Richelot isogeny graph*, RIMS Kôkyûroku Bessatsu **B90**, 195–219, 2022.

[11] P. Gaudry: *Fast genus 2 arithmetic based on Theta functions*, J. Math. Crypt. **1**, 243–265, 2007.

[12] T. Ibukiyama, T. Katsura and F. Oort: *Supersingular curves of genus two and class numbers*, Compositio Math. **57**(2), 127–152, 1986.

[13] J. Igusa: *Theta functions*, Grundlehren der mathematischen Wissenschaften **194**, Springer–Verlag, 1972.

[14] B.W. Jordan and Y. Zaytman: *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, preprint, arXiv: 2005.09031.

[15] S. Karati and P. Sarkar: *Kummer for genus one over prime-order fields*, J. Cryptology **33**, 97–129, 2020.

[16] M. Kudo, S. Harashita and E. W. Howe: *Algorithms to enumerate superspecial Howe curves of genus 4*, The Open Book Series **4** (1), 301–316, 2020.

[17] H. Lange and C. Birkenhake: *Complex Abelian Varieties*, Grundlehren der mathematischen Wissenschaften **302**, Springer–Verlag, 2004.

[18] D. Mumford: *On the equations defining abelian varieties. I*, Invent. math. **1**, 287–354, 1966.

[19] D. Mumford: *Tata Lectures on Theta II*, Progress in Mathematics **43**, Birkhäuser, 1984.

[20] R. Ohashi: *On the Rosenhain forms of superspeial curves of genus two*, preprint, arXiv: 2308.11963.

[21] R. Ohashi, H. Onuki, M. Kudo, R. Yoshizumi and K. Nuida: *Computing Richelot isogeny graph of superspecial abelian threefolds*, preprint, arXiv: 2401.10500.

[22] K. Takashima: *Counting superspecial Richelot isogenies by reduced automorphism groups*, RIMS Kôkyûroku Bessatsu **B90**, 185–193, 2022.